CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Volume 15

Soraya Weiner

Nachmarktpflichten für Software- und KI-Produkte

Produktsicherheitsrechtliche Anforderungen für Hersteller im Vergleich zwischen der Schweiz und der EU

EIZ Publishing

Nachmarktpflichten für Software- und KI-Produkte

Produktsicherheitsrechtliche Anforderungen für
Hersteller im Vergleich zwischen der Schweiz und der EU

Dissertation
der Rechtswissenschaftlichen Fakultät
der Universität Zürich

zur Erlangung der Würde einer Doktorin
der Rechtswissenschaft

vorgelegt von

Soraya Weiner
von Kloten, ZH

genehmigt auf Antrag von

Prof. Dr. Florent Thouvenin
und
Prof. Dr. Walter Fellmann

Die Rechtswissenschaftliche Fakultät der Universität Zürich gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 3. Dezember 2025

Der Dekan: Prof. Dr. Thomas Gächter

Verlag: EIZ Publishing (eizpublishing.ch), Bellerivestrasse 49, 8008 Zürich,
eizpublishing@europa-institut.ch
Autorin: Soraya Weiner
Abbildung Cover: Muhammad Raihan
ISBN:
978-3-03994-072-1 (Print – Softcover)
978-3-03994-073-8 (Print – Hardcover)
978-3-03994-074-5 (ePub)
DOI: https://doi.org/10.36862/6WSK-8E9M
Version: 1.00 – 20260220

Die Dissertation wurde publiziert mit Unterstützung des Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung.

Die vorliegende Dissertation wurde von Soraya Weiner eingereicht und am 3. Dezember 2025 von der Rechtswissenschaftlichen Fakultät der Universität Zürich auf Antrag von Herrn Professor Dr. Florent Thouvenin (erster Referent) und Herrn Professor Dr. Walter Fellmann (zweiter Referent) genehmigt.

Dieses Werk ist als gedrucktes Buch sowie als E-Book (open access) in verschiedenen Formaten verfügbar. Weitere Informationen finden Sie unter der URL: https://eizpublishing.ch/publikationen/nachmarktpflichten-fuer-software-und-ki-produkte/.

Vorwort

Diese Arbeit ist in den Jahren 2022 bis 2025 entstanden und beachtet Literatur, geltende Gesetzestexte sowie -entwürfe und Internetseiten bis zum 31.05.2025.

Alle Hervorhebungen (auch in Zitaten) stammen von der Autorin; fremde Hervorhebungen wurden nicht übernommen. Deutsche Schreibweisen wurden an die Schweizer Rechtschreibung angepasst (z.B. in Zitaten das ß durch ss ersetzt). Abbildungen und Tabellen ohne Quellenangabe wurden selbst erstellt.

Zugunsten einer einfacheren Lesbarkeit wird jeweils die kürzeste Form eines Wortes (z.B. der Hersteller, die Person) verwendet. Ausgenommen davon ist der Bezug auf reale Personen, für welche jeweils die Formulierung des gegen aussen gelebten Geschlechts gewählt wird.

Vorab danke ich Herrn Prof. Dr. Florent Thouvenin für seine Betreuung, die wertvollen Anregungen während der Ausarbeitung dieser Arbeit und für die grossen Freiheiten, welche er mir gewährt hat. Ebenso danke ich Herrn Prof. Dr. Walter Fellmann für die interessante Diskussion zum Produktsicherheitsrecht sowie für die Erstellung des Zweitgutachtens.

Bedanken möchte ich mich weiter bei den Herrn lic. iur. Hans-Joachim Hess, Peter Gyger der BFU und Severo Nicoli des ESTI für die gewinnbringenden Gespräche respektive die Beantwortung meiner Fragen zur Praxis. Die vorliegende Arbeit hat durch ihre Hinweise wesentlich an Qualität gewonnen.

Für die Denkanstösse und Durchsicht meiner Arbeit in den Bereichen ihrer jeweiligen Fachgebiete möchte ich mich bei Sven Fassbender, MLaw Jimmy Orucevic, MLaw Viviane Ammann und M.A. HSG Adrian Rakita bedanken. Bei Vivian möchte ich mich besonders für die vielen gemeinsamen Schreibstunden und Kaffeepausen in Zürich, Dänemark und München bedanken.

Ausserdem möchte ich mich herzlich bei meiner Arbeitgeberin, meinen Vorgesetzten und meinen Teamkolleginnen und -kollegen bedanken. Die gewährte Flexibilität und der stärkende sowie humorvolle Arbeitsalltag haben mir den nötigen Ausgleich ermöglicht.

Für die vielfältige Unterstützung durch meine Familie, Freundinnen und Freunde bin ich zutiefst dankbar. Ohne sie hätte ich diese Arbeit nicht verfasst. Besonders erwähnen möchte ich Maja und Helmi Studer sowie Michael und Marvin Weiner mit Rachel Hollinrake, die immer an mich geglaubt haben. Her-

vorheben möchte ich ausserdem Dario Bicker, Désirée Kaissl, Bettina Keller v/o Tschappa, Tatjana Subotic v/o Wallaby, Vibha Mohan, Danielle Naegeli v/o Pitschi, Andreas und Alexandra Reust, Nadine Schwendimann sowie Nadine Wyss. Mein grösster Dank gilt meinem Freund Mika Freitag, der mich mit viel Geduld, Verständnis und Zuversicht begleitet und unterstützt. Ihnen widme ich diese Arbeit.

Soraya Weiner
Bassersdorf, im September 2025

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

a.A.	andere Ansicht
a.M.	andere Meinung
AB	Amtliches Bulletin
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AcP	Archiv für die civilistische Praxis
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Attorney General
AGI	Artificial General Intelligence
AI	Artificial Intelligence
AJP	Aktuelle Juristische Praxis
API	Application Programming Interface
App	Applikation
Art.	Artikel
ASTRA	Bundesamt für Strassen
Aufl.	Auflage
B2B	Business-to-Business
B2C	Business-to-Consumer
BAKOM	Bundesamt für Kommunikation
BB	Betriebs-Berater
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BFK	Eidgenössisches Büro für Konsumentenfragen
BFS	Bundesamt für Statistik
BFU	Beratungsstelle für Unfallverhütung
BGE	Entscheidungen des Schweizerischen Bundesgerichts, Amtliche Sammlung
BGer	Bundesgericht
BJ	Bundesamt für Justiz
BKR	Zeitschrift für Bank- und Kapitalmarktrecht
BSK	Basler Kommentar

bspw.	beispielsweise
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
CASP	Coordinated Activities on the Safety of Products
CB	Compliance Berater, Betriebs-Berater Compliance
CE	Conformité Européenne
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CES	Consumer Electronics Show
CH	Schweiz
CHK	Handkommentar zum Schweizer Privatrecht
CNAI	Kompetenznetzwerk für Künstliche Intelligenz
COD	Ordinary Legislative Procedure
COM	Commission Document
CR	Computer und Recht
CRA	Cyber Resilience Act
CyRV	Cyberrisikenverordnung
d.h.	das heisst
DIN	Deutsches Institut für Normung
DSB	Datenschutz-Berater
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
E.	Erwägung
ECLI	European Case Law Identifier
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EFTA	Europäische Freihandelsassoziation
EG	Europäische Gemeinschaft
EKK	Eidgenössische Kommission für Konsumentenfragen
EleG	Bundesgesetz betreffend die elektrischen Schwach- und Starkstromanlagen

EMV-RL	Richtlinie über die elektromagnetische Verträglichkeit
EN	Europäische Norm
engl.	englisch
ErwG	Erwägungsgrund
ESTI	Eidgenössisches Starkstrominspektorat
et al.	et alia
etc.	et cetera
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
evtl.	eventuell
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
f./ff.	und folgende
FAQ	Frequently Asked Questions
FAV	Funkanlagenverordnung
FMG	Fernmeldegesetz
Fn.	Fussnote
FusG	Fusionsgesetz
gem.	gemäss
Gen-AI	Generative Artificial Intelligence
GesKR	Gesellschafts- und Kapitalmarktrecht
gl.M.	gleiche Meinung
GPAI	General Purpose AI
GPAIM	General Purpose AI Model
GPSR	General Product Safety Regulation
GPT	Generative Pre-trained Transformer
GTG	Gentechnikgesetz
h.L.	herrschende Lehre
HAVE	Haftung und Versicherung
HLEG AI	High-Level Expert Group on Artificial Intelligence

HMG	Heilmittelgesetz
Hrsg.	Herausgeber
i.d.R.	in der Regel
i.e.S.	im engeren Sinne
i.S.d.	im Sinne der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinne
IDG	Internetrecht und Digitale Gesellschaft (Schriftenreihe)
IEC	International Electrotechnical Commission
IK-EUDP	Interdepartementale Koordinationsgruppe EU-Digitalpolitik
inkl.	inklusive
InTeR	Zeitschrift zum Innovations- und Technikrecht
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Informationstechnologie
JZ	Juristenzeitung
Kap.	Kapitel
KI	Künstliche Intelligenz
KI-VO	Künstliche-Intelligenz-Verordnung
KIR	Künstliche Intelligenz und Recht
L	Legislation
LGV	Lebensmittel- und Gebrauchsgegenständeverordnung
LiDar SLAM	Light Detection and Ranging and Simultaneous Localisation and Mapping
lit.	litera
LLM	Large Language Model
LMG	Lebensmittelgesetz
LVD	Low Voltage Directive (Niederspannungsrichtlinie)
m.E.	meines Erachtens
m.w.H.	mit weiteren Hinweisen
MaschV	Maschinenverordnung

MDR	Medical Device Regulation
MepV	Medizinprodukteverordnung
MMR	Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT
MRA	Mutual Recognition Agreement
MRL	Maschinenrichtlinie
MVO	Maschinenverordnung
MÜVO	Marktüberwachungsverordnung
NEV	Niederspannungsverordnung
NHK	Nomos Handkommentar
NJW	Neue Juristische Wochenschrift
NLF	New Legislative Framework
NLP	Natural Language Processing
NP	Nomos Praxiskommentar
NR	Nationalrat
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OECD	Organisation for Economic Co-operation and Development
OFK	Orell Füssli Kommentar
OR	Obligationenrecht
PC	Personal Computer
PLD	Product Liability Directive
PrHG	Produktehaftpflichtgesetz
Proc. Des. Soc.	Proceedings of the Design Society
ProdHaftG	Produkthaftungsgesetz
ProdSG	Produktsicherheitsgesetz
PrSG	Produktesicherheitsgesetz
PrSV	Produktesicherheitsverordnung
RAPEX	Rapid Exchange of Information System
RDi	Recht Digital
RED	Radio Equipment Directive
RL	Richtlinie

Rn.	Randnummer
RTK GPS	Real-Time Kinematic Global Positioning System
S.	Seite
s. o.	siehe oben
s. u.	siehe unten
SaaS	Software as a Service
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SECO	Staatssekretariat für Wirtschaft
SGK	St. Galler Kommentar
SHK	Stämpflis Handkommentar
SJZ	Schweizerische Juristen-Zeitung
SN	Schweizer Norm
sog.	sogenannt
SR	Systematische Sammlung des Bundesrechts
STEG	Bundesgesetz über die Sicherheit von technischen Einrichtungen und Geräten
StGB	Strafgesetzbuch
SWD	Staff Working Document
THG	Bundesgesetz über die technischen Handelshemmnisse
u.a.	unter anderem
u.U.	unter Umständen
Uabs.	Unterabsatz
UE	Urteil des Obergerichts des Kantons Zürich
URG	Urheberrechtsgesetz
USG	Umweltschutzgesetz
usw.	und so weiter
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VEMV	Verordnung über die elektromagnetische Verträglichkeit
VersR	Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht
VO	Verordnung
v/o	vulgo

VSS	Spielzeugverordnung
VTS	Verordnung über die technischen Anforderungen an Strassenfahrzeuge
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung
WHO	Weltgesundheitsorganisation
Wi-Fi	Wireless Fidelity
WIREs	Wiley Interdisciplinary Reviews
z.B.	zum Beispiel
ZfPC	Zeitschrift für Product Compliance
ZGB	Zivilgesetzbuch
Ziff.	Ziffer
zit.	zitiert
ZUM	Zeitschrift für Urheber- und Medienrecht

Literaturverzeichnis

Ackermann Tobias/Golling Manuel, Entwurf einer neuen Produktsicherheits-Verordnung – Worauf sich Hersteller zukünftig einstellen müssen, ZfPC 2022, S. 67 ff.

Amstutz, Marc/Atamer, Yesim M. (Hrsg.), Handkommentar zum Schweizer Privatrecht, Wirtschaftsrechtliche Nebenerlasse: FusG, UWG, KKG, PauRG und PrHG, 4. Aufl., Zürich, 2023 (zit. CHK-Bearbeiter/in)

Areeb Qazi Mohammad/Nadeem Mohammad/Sohail Shahab Saquib/Imam Raza/Doctor Faiyaz/Himeur Yassine/Hussain Amir/Amira Abbes, Filter Bubbles in Recommender Systems: Fact or Fallacy – A Systematic Review, WIREs Data Mining and Knowledge Discovery 13/2023, S. 1 ff.

Arioli Martina, Risikomanagement nach der EU-Verordnung über Künstliche Intelligenz, Jusletter IT 04.07.2024

Asenger Hüveyda, Künstliche Intelligenz im Strafverfahren und Fairness: Ein Ausblick auf internationale und nationale KI-Systeme und Anwendungen, InTeR 2023, S. 134 ff.

Batache Djamila, Künstliche Intelligenz in der Medizin aus haftungsrechtlicher Perspektive, Dissertation, Basel, Schriften zum Recht der neuen Technologien Band 4, Zürich/St. Gallen, 2024

Bauer Matthias, Das Recht des technischen Produkts, Praxishandbuch für Unternehmensjuristen, Wiesbaden, 2018

Beck Susanne, Der rechtliche Status autonomer Maschinen, AJP 2017, S. 183 ff.

Bodewig Theo, Der Rückruf fehlerhafter Produkte, Eine Untersuchung der Rückrufpflichten und Rückrufansprüche nach dem Recht Deutschlands, der Europäischen Union und der USA, Habilitation, Tübingen, Jus privatum Band 36, 1999

Bomhard David/Merkle Marieke, Europäische KI-Verordnung, RDi 2021, S. 276 ff.

Bomhard, David/Schreiber, Kristina/Marly, Jochen/Bernzen, Anna K./Beurskens, Michael/Dovas, Maria-Urania (Hrsg.), Praxishandbuch Softwarerecht, Rechtsschutz und Vertragsgestaltung, 8. Aufl., München, 2024 (zit. Bearbeiter/in, in: Bomhard et al.)

Borges Georg, Der Begriff des KI-Systems – Tatbestandsmerkmale und Auslegungsansätze, CR 11/2023, S. 706 ff. (zit. Borges, Begriff)

Borges Georg, Die europäische KI-Verordnung (AI Act) – Teil 1, Überblick, Anwendungsbereich und erste Einschätzung, CR 8/2024, S. 497 ff. (zit. Borges, Teil 1)

Borio Beatrice, Haftungsrechtliche Herausforderungen bei autonomen Pflegerobotern, Pflegerecht – Pflegewissenschaft 2021, S. 223 ff.

Borkert Kristian/Nomerowskaja Anastasia, Regulation eats Innovation for Breakfast: KI-basierte SaaS-Lösung unter dem Regime des EU AI Acts in der Praxis, InTeR 2024, S. 166 ff.

Braun Binder Nadja/Burri Thomas/Lohmann Melinda Florina/Simmler Monika/Thouvenin Florent/Vokinger Kerstin Noëlle, Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, Jusletter 28.06.2021

Braun Binder Nadja/Egli Catherine, Umgang mit Hochrisiko-KI-Systemen in der KI-VO, MMR 2024, S. 626 ff. (zit. Braun Binder/Egli, Umgang)

Bräutigam, Peter/Kraul, Torsten/Bauer, Stefan (Hrsg.), Internet of Things, Rechtshandbuch, München, 2021 (zit. Bearbeiter/in, in: Bräutigam/Kraul/Bauer)

Buchalik Barbara/Gehrmann Mareike Christine, Von Nullen und Einsen zu Paragraphen: Der AI Act, ein Rechtscode für Künstliche Intelligenz, CR 3/2024, S. 145 ff.

Bühler Theodor, Auswirkungen des Produktsicherheitsgesetzes auf das Privatrecht, SJZ 108/2012, S. 45 ff. (zit. Bühler, Privatrecht)

Bühler Theodor, Die Produktsicherheit als Bestandteil der schweizerischen Rechtsordnung, Zürich/St. Gallen, 2012 (zit. Bühler, Bestandteil)

Bühler Theodor, Sicherheit von Non-Food-Produkten in der neuesten schweizerischen Gesetzgebung, Zürich/St. Gallen, 2015 (zit. Bühler, Sicherheit)

Bühler Theodor/Tobler Christa, Produktsicherheit in der EU und in der Schweiz, Zürich, 2011

Büyüksagis Erdem, Responsabilité pour les systèmes d'intelligence artificielle, HAVE 2021, S. 12 ff.

Canapa, Damiano/Richa, Alexandre (Hrsg.), Aspects juridiques de l'intelligence artificielle, Bern, 2024 (zit. Bearbeiter/in, in: Canapa/Richa)

Chappuis, Christine/Winiger, Bénédict/Campi, Arnaud (Hrsg.), La responsabilité du fait des produits, Journée de la responsabilité civile 2016, Zürich, 2018 (zit. Bearbeiter/in, in: Chappuis/Winiger/Campi)

Chibanguza Kuuya/Steege Hans, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, S. 1769 ff.

Costello Nancy/Sutton Rebecca/Jones Madeline/Almassian Mackenzie/Raffoul Amanda/Ojumu Oluwadunni/Salvia Meg/Santoso Monique/Kavanaugh Jill R./Austin S. Bryn, Algorithms, Addiction, And Adolescent Mental Health: An Interdisciplinary Study to Inform State-level Policy Action to Protect Youth from the Dangers of Social Media, American Journal of Law & Medicine 2-3/2023, S. 135 ff.

Dal Molin-Kränzlin Alexandra/Dal Molin Luca, Open Source Software in M&A-Transaktionen, GesKR 2020, S. 382 ff.

Denga Michael, Unternehmenshaftung für KI – zur Konformitätsbewertung in Permanenz, CR 5/2023, S. 277 ff.

Diebold Nicolas F./Rütsche Bernhard, Wettbewerbsrecht und Marktregulierung, Band 1 Grundlagen, Zürich, 2023

Drittenbass Joel, Regulierung von autonomen Robotern, Angewendet auf den Einsatz von autonomen Medizinrobotern: eine datenschutzrechtliche und medizinprodukterechtliche Untersuchung, Dissertation, Schriften zum Recht der neuen Technologien Band 1, Zürich/St. Gallen, 2021

Dürr, David/Lardi, Mauro/Rouiller, Nicolas (Hrsg.), Unternehmensführung und Recht/Droit et gestion d'entreprise, Regulatorisches Umfeld für KMU/Le cadre juridique et réglementaire de l'activité des entreprises, 2. Aufl., Zürich/St. Gallen, 2019 (zit. Bearbeiter/in, in: Dürr/Lardi/Rouiller)

Ebers Martin/Hoch Veronica R. S./Rosenkranz Frank/Ruschemeier Hannah/Steinrötter Björn, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, S. 528 ff.

Ehrenzeller, Bernhard/Egli, Patricia/Hettich, Peter/Hongler, Peter/Schindler, Benjamin/Schmid, Stefan G./Schweizer, Rainer J. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 4. Aufl., Zürich, 2023 (zit. SGK BV-Bearbeiter/in)

Errass Christoph, Technikregulierungen zur Gewährleistung von Sicherheit, Sicherheit & Recht 2/2016, S. 63 ff.

Etzkorn Philipp, Bedeutung der «Entwicklungslücke» bei selbstlernenden Systemen, MMR 2020, S. 360 ff.

Faeh Andrea, Die Rechte des Verbrauchers im Arzneimittelmarkt der Europäischen Union, Möglichkeiten und Grenzen des Individualrechtsschutzes im Binnenmarkt unter spezieller Berücksichtigung des Rechts auf Zugang, Sicherheit und Information, Dissertation, Freiburg, Arbeiten aus dem Iuristischen Seminar der Universität Freiburg Schweiz Band 304, Zürich, 2011

Feiler Lukas/Forgó Nikolaus, KI-VO, EU-Verordnung über Künstliche Intelligenz, Kommentar, Wien, 2024

Fellmann Walter, Haftpflichtrecht im Zeichen der Digitalisierung, HAVE 2021, S. 105 ff. (zit. Fellmann, Haftpflichtrecht)

Fellmann Walter, Inhalt und Tragweite des Produktesicherheitsgesetzes (PrSG) vom 12. Juni 2009, HAVE 2010, S. 3 ff. (zit. Fellmann, Tragweite)

Fellmann Walter, Nachmarktpflichten des Herstellers und des Importeurs nach dem PrSG, Jusletter 25.10.2010

Fellmann Walter/Büren-von Moos Gabrielle, Grundriss der Produktehaftpflicht, Bern, 1993

Fellmann, Walter (Hrsg.), Haftpflichtprozess 2021, Haftung für Künstliche Intelligenz, (teil-)automatisierte Fahrzeuge, Drohnen und Software, Entwicklungen im Dienstleistungs-, Privatversicherungs-, Prozess-, Staatshaftungs- und Haftpflichtrecht: Beiträge zur Tagung vom 2. und 3. November 2021, Zürich/Basel/Genf, 2021 (zit. Bearbeiter/in, in: Fellmann)

Fellmann, Walter/Furrer, Andreas (Hrsg.), Produktesicherheit und Produktehaftung – Die Schonzeit für Hersteller, Importeur und Händler ist vorbei!, Tagung vom 23. März 2012, Bern, 2012 (zit. Bearbeiter/in, in: Fellmann/Furrer, Schonzeit)

Fellmann, Walter/Furrer, Andreas (Hrsg.), Produktsicherheit und Produkthaftung – neue Herausforderungen für schweizerische Unternehmen, Tagung vom 31.03.2011 in Luzern, Bern, 2011 (zit. Bearbeiter/in, in: Fellmann/Furrer, Herausforderungen)

Fischer, Willi/Luterbacher, Thierry (Hrsg.), Haftpflichtkommentar, Kommentar zu den schweizerischen Haftpflichtbestimmungen, Zürich/St. Gallen, 2016 (zit. Haftpflichtkommentar-Bearbeiter/in)

Foerste, Ulrich/Westphalen, Friedrich (Hrsg.), Produkthaftungshandbuch, 4. Aufl., München, 2024 (zit. Bearbeiter/in, in: Foerste/Westphalen)

Fornage Anne-Christine, Sécurité des produits, respect des normes techniques et conformité aux exigences essentielles: les précisions du Tribunal fédéral, sui generis 2018, S. 109 ff. (zit. Fornage, Sécurité)

Freytag Urs, Die Industrie 4.0 im Spannungsfeld zwischen Safety, Security und Privacy, Sicherheit & Recht 1/2019, S. 23 ff.

Fröhlich-Bleuler Gianni, Softwareverträge, 2. Aufl., Bern, 2014

Gebhardt Nicolas/Bahns Tammo/Krause Dieter, An Example of Visually Supported Design of Modular Product Families, Procedia CIRP 21/2014, S. 75 ff.

Geiser, Thomas/Fountoulakis, Christiana (Hrsg.), Zivilgesetzbuch I, Art. 1-456 ZGB. Basler Kommentar, 7. Aufl., Basel, 2022 (zit. BSK ZGB I-Bearbeiter/in)

Gerster Alexander R., Bundesgesetz über die Produktesicherheit (PrSG), Grundlagen, Pflichten und Folgen einer Pflichtverletzung unter besonderer Berücksichtigung des zivilrechtlichen Haftungsrechts, Dissertation, Zürich, 2018

Graf Fabienne/Obrecht Liliane, Rechtliche Rahmenbedingungen für Künstliche Intelligenz in der Schweiz, Jusletter 29.11.2021

Graf Fabienne/Obrecht Liliane/Weiner Soraya, Erste Erkenntnisse zu Transparenz, Diskriminierung und Manipulation, Jusletter 12.12.2022

Guillod, Olivier/Müller, Christoph (Hrsg.), Pour un droit équitable, engagé et chaleureux, Mélanges en l'honneur de Pierre Wessner, Basel, 2011 (zit. Bearbeiter/in, in: Guillod/Müller)

Haas Peter/Leutwiler Sarah, Nachmarktpflichten im Fokus internationaler Produktrückrufe, HAVE 2018, S. 452 ff.

Hacker Philipp, Europäische und nationale Regulierung von Künstlicher Intelligenz, NJW 2020, S. 2142 ff.

Häner, Isabelle/Waldmann, Bernhard (Hrsg.), 7. Forum für Verwaltungsrecht, Staatliche Aufsicht über die Wirtschaft und ihre Akteure, Bern, 2019 (zit. Bearbeiter/in, in: Häner/Waldmann)

Hänsenberger Silvio, Die Haftung für Produkte mit lernfähigen Algorithmen, Jusletter 26.11.2018

Hänsenberger Silvio, Die zivilrechtliche Haftung für autonome Drohnen unter Einbezug von Zulassungs- und Betriebsvorschriften, Dissertation, St. Gallen, sui generis Band 3, Berlin, 2018 (zit. Hänsenberger, Drohnen)

Hartmann Christoph/Klindt Thomas, Kritisches zum Kommissions-Entwurf für eine Produktsicherheits-VO, ZfPC 2022, S. 73 ff.

Heiss, Helmut/Loacker, Leander D. (Hrsg.), Grundfragen des Konsumentenrechts, Zürich, 2020 (zit. Bearbeiter/in, in: Heiss/Loacker)

Hess Hans-Joachim, Haftungsverschärfung für Produkte in der EU, CB 01-02/2023, S. 27 ff. (zit. Hess, Haftungsverschärfung)

Hess Hans-Joachim, Produktehaftpflichtgesetz (PrHG), Bundesgesetz über die Produktehaftpflicht vom 18. Juni 1993, 3. Aufl., Bern, 2016 (zit. SHK PrHG-Hess)

Hess Hans-Joachim, Produktehaftung – Produktesicherheit, Zürich, 2021 (zit. Hess, Produktehaftung – Produktesicherheit)

Hess Hans-Joachim, Produktesicherheitsgesetz (PrSG), Bern, 2010 (zit. SHK PrSG-Hess)

Hildt Elisabeth, Artificial Intelligence: Does Consciousness Matter?, Frontiers in Psychology 10/2019, S. 1 ff.

Hilgendorf, Eric/Roth-Isigkeit, David (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, München, 2023 (zit. Bearbeiter/in, in: Hilgendorf/Roth-Isigkeit)

Hoi Steven C.H./Sahoo Doyen/Lu Jing/Zhao Peilin, Online learning: A comprehensive survey, Neurocomputing 2021, S. 249 ff.

Holliger-Hagmann Eugénie, Das Produktesicherheitsgesetz: Eine Büchse der Pandora – Das Produktesicherheitsgesetz (PrSG) trat am 1. Juli 2010 in Kraft und wirft mehr Fragen auf, als es löst, Sicherheit & Recht 3/2010, S. 186 ff. (zit. Holliger-Hagmann, Büchse der Pandora)

Holliger-Hagmann Eugénie, Produktesicherheitsgesetz (PrSG), Produktsicherheit und Haftpflicht, Zürich/St. Gallen, 2011 (zit. Holliger-Hagmann, Produktsicherheit und Haftpflicht)

Holliger-Hagmann Eugénie, Produktesicherheitsgesetz PrSG, Produktrisiken im Griff – rechtliche Fallstricke vermeiden, Zürich, 2010 (zit. Holliger-Hagmann, Fallstricke)

Honsell Heinrich/Isenring Bernhard/Kessler Martin A., Schweizerisches Haftpflichtrecht, 5. Aufl., Zürich, 2013

Huguenin Claire, Obligationenrecht, Allgemeiner und besonderer Teil, 3. Aufl., Zürich, 2019

Hürlimann-Kaup, Bettina/Eitel, Paul/Hartmann, Stephan/Haas, Raphaël (Hrsg.), Sachenrecht, Obligationenrecht und mehr, Liber amicorum für Jörg Schmid zum 60. Geburtstag, Zürich/Basel/Genf, 2019 (zit. Bearbeiter/in, in: Hürlimann-Kaup et al.)

Joggerst Laura/Wendt Janine, Die Weiterentwicklung der Produkthaftungsrichtlinie, InTeR 2021, S. 13 ff.

Kalbhenn Jan Christopher, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 2021, S. 663 ff.

Kapoor Arun/Klindt Thomas, «New Legislative Framework» im EU-Produktsicherheitsrecht – Neue Marktüberwachung in Europa?, EuZW 2008, S. 649 ff.

Kasper Gabriel, Extraterritorialer Geltungsbereich der EU-Digitalstrategie, Jusletter 23.09.2024

Kasper Lehne, Sabina/Münch, Peter/Probst, Franz (Hrsg.), Schweizer Vertrags-Handbuch, Musterverträge für die Praxis, 3. Aufl., Basel, 2018 (zit. Bearbeiter/in, in: Kasper Lehne/Münch/Probst)

Kleemans Mariska/Daalmans Serena/Carbaat Ilana/Anschütz Doeschka, Picture Perfect: The Direct Effect of Manipulated Instagram Photos on Body Image in Adolescent Girls, Media Psychology 1/2018, S. 93 ff.

Klett Barbara, Digitalisierte Gesundheit – Abgrenzungen und Regulierung, HAVE 2017, S. 104 ff. (zit. Klett, Digitalisierte)

Klett Barbara, Produktesicherheit – Produktehaftung in einer vorsichtigen stetigen Entwicklung, HAVE 2018, S. 436 (zit. Klett, Produktesicherheit)

Klett Barbara/Müller Dominique, Rechtsentwicklung zum PrHG und PrSG, HAVE 2018, S. 438 ff.

Klett Barbara/Verde Michel, Medizinprodukt- und haftpflichtrechtliche Aspekte bei Medizinal-Apps, Sicherheit & Recht 1/2016, S. 45 ff.

Klindt Thomas, Herausforderungen der Marktüberwachung im Produktsicherheitsrecht, InTeR 1/2021, S. 3 ff.

Klindt, Thomas (Hrsg.), Produktsicherheitsgesetz ProdSG, Kommentar, 3. Aufl., München, 2021 (zit. Beck ProdSG-Bearbeiter/in)

Koch Bernhard A./Pichonnaz Pascal, Der Entwurf einer neuen EU-Produkthaftungsrichtlinie aus schweizerischer Sicht, SJZ 119/2023, S. 627 ff.

Konertz Roman/Schönhof Raoul, Das technische Phänomen «Künstliche Intelligenz» im allgemeinen Zivilrecht, Eine kritische Betrachtung im Lichte von Autonomie, Determinismus und Vorhersehbarkeit, Baden-Baden, 2020

Kramer Ernst A./Arnet Ruth, Juristische Methodenlehre, 7. Aufl., Bern/München/Wien, 2024

Krimphove Dieter, Die europäische KI-Verordnung im Technikrecht, InTeR 2024, S. 154 ff.

Krönke Christoph, Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten, NVwZ 2024, S. 529 ff.

Krumm Malte/Meyer Johanna, Alles Gute kommt von oben? Datenschutz- und KI-rechtliche Implikationen des Einsatzes von Kameradrohnen, InTeR 2025, S. 16 ff.

Kuechenhof Jan/Berschik Markus C./Beibl Julia/Alonso Fernández Iñigo/Otto Kevin/Krause Dieter/Isaksson Ola, Incorporating Field Effects into the Design of Modular Product Families, Proc. Des. Soc. 2023, S. 2275 ff.

Lohmann Melinda Florina, Automatisierte Fahrzeuge im Lichte des Schweizer Zulassungs- und Haftungsrechts, Dissertation, St. Gallen, Robotik und Recht Band 7, Baden-Baden, 2016 (zit. Lohmann, Fahrzeuge)

Lohmann Melinda Florina, Ein zukunftsfähiger Haftungsrahmen für Künstliche Intelligenz, HAVE 2021, S. 111 ff. (zit. Lohmann, Haftungsrahmen)

Lohmann Melinda Florina, Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse, AJP 2017, S. 152 ff. (zit. Lohmann, Roboter)

Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Liability for artificial intelligence and the internet of things, Münster Colloquia on EU Law and the Digital Economy IV, Baden-Baden, 2019 (zit. Bearbeiter/in, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT)

Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Liability for AI, Münster Colloquia on EU Law and the Digital Economy VII, Baden-Baden, 2023 (zit. Bearbeiter/in, in: Lohsse/Schulze/Staudenmayer, Liability for AI)

Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Smart Products, Münster Colloquia on EU Law and the Digital Economy VI, Baden-Baden, 2022 (zit. Bearbeiter/in, in: Lohsse/Schulze/Staudenmayer, Smart Products)

Martini Mario, Blackbox Algorithmus – Grundfragen einer Regulierung künstlicher Intelligenz, Berlin/Heidelberg, 2019 (zit. Martini, Blackbox)

Martini, Mario/Wendehorst, Christiane (Hrsg.), Recht der Künstlichen Intelligenz, Künstliche Intelligenz-Verordnung, München, 2024 (zit. Beck KI-VO-Bearbeiter/in)

Mattheis Clemens, «Mental health risks» und das Safety-Konzept der neuen Produktsicherheitsverordnung – Wenn der Kühlschrank dir den Schlaf raubt und daher vom Markt genommen werden muss, ZfPC 1/2022, S. 104 ff.

May Elisa/Gaden Justus, Vernetzte Fahrzeuge, InTeR 2018, S. 110 ff.

MLL Legal (Hrsg.), Praxishandbuch Produktregulierung, Heilmittel, Lebensmittel, Kosmetika, Chemikalien, Alkohol und Tabak, Bern, 2023 (zit. Bearbeiter/in, in: Praxishandbuch Produktregulierung)

Molavi Vasse'i Ramak, Die Evolution der KI-Definition von Turings Anthropozentrik zur Funktionsorientierung der KI-VO, KIR 5/2025, S. 190 ff.

Müller Christoph, Ausservertragliches Haftpflichtrecht, Basel, 2025

Niggli, Marcel Alexander/Wiprächtiger, Hans (Hrsg.), Strafrecht I. Basler Kommentar, 4. Aufl., Basel, 2019 (zit. BSK StGB I-Bearbeiter/in)

Pfenninger Hanspeter, Produktsicherheitsrecht Schweiz – EU im Vergleich, AJP 2014, S. 1157 ff.

Piovano Christian, Der Hersteller im europäischen Produktsicherheitsrecht, Dissertation, InTeR – Zeitschrift zum Innovations- und Technikrecht Band 4, Frankfurt, 2020 (zit. Piovano, Hersteller)

Piovano Christian, Rechtsfragen bei der Identifikation des produktsicherheitsrechtlichen Herstellers bei OEM-Geschäften, InTeR 1/2021, S. 6 ff. (zit. Piovano, Rechtsfragen)

Piovano Christian/Schucht Carsten/Wiebe Gerhard, Quick Guide: Produktbeobachtung in der Digitalisierung, Wie Sie Product Compliance bei der Beobachtung der digitalisierten Produktwelt gewährleisten, Wiesbaden, 2023

Rehbinder Manfred/Haas Lorenz/Uhlig Kai-Peter (Hrsg.), URG, Urheberrechtsgesetz mit weiteren Erlassen und internationalen Abkommen, 4. Aufl., Zürich, 2022 (zit. OFK URG-Rehbinder/Haas/Uhlig)

Reiter Catherine, Künstliche Intelligenz im Verwaltungsverfahren, AJP 2022, S. 984 ff.

Reusch Philipp, KI und Software im Kontext von Produkthaftung und Produktsicherheit, RDi 4/2023, S. 152 ff. (zit. Reusch, KI und Software)

Reusch Philipp, Mobile Updates – Updatability, Update-Pflicht und produkthaftungsrechtlicher Rahmen, BB 2019, S. 904 ff. (zit. Reusch, Mobile Updates)

Reusch Philipp, Produkt Compliance 2025 – Entwicklungen und Ausblick, CB 2025, S. 93 ff. (zit. Reusch, Produkt)

Ritter Franziska/Schaa Volker, KI-System – Das unbekannte Wesen, DSB 02/2025, S. 32 ff.

Roberto Vito, Haftpflichtrecht, 4. Aufl., Bern, 2024

Rohrssen Benedikt, KI & CE – Die KI-VO, das Produktsicherheitsrecht für Künstliche Intelligenz, ZfPC 3/2024, S. 111 ff.

Roos Philipp/Weitz Alexander, Hochrisiko-KI-Systeme im Kommissionsentwurf für eine KI-Verordnung, MMR 2021, S. 844 ff.

Rosenthal David, Der EU AI Act – Verordnung über künstliche Intelligenz, Jusletter 05.08.2024

Röthlisberger Thomas, Zivilrechtliche Produktbeobachtungs-, Warn- und Rückrufpflichten der Hersteller, Unter Berücksichtigung wettbewerbs- und versicherungsrechtlicher Aspekte, Dissertation, Basel, Schweizer Schriften zum Handels- und Wirtschaftsrecht Band 222, Zürich, 2003

Russell Stuart J./Norvig Peter, Artificial intelligence, A modern approach, 4. Aufl., Boston, 2022

Schmid Alexander, IT- und Rechtssicherheit automatisierter und vernetzter cyberphysischer Systeme, Event Data Recording und integrierte Produktbeobachtung als Maßnahmen der IT-Risikominimierung am Beispiel automatisierter und vernetzter Luft- und Straßenfahrzeuge, Dissertation, Passau, Internetrecht und Digitale Gesellschaft (IDG) Band 16, Berlin, 2019 (zit. Schmid, IT)

Schmid Alexander, Pflicht zur «integrierten Produktbeobachtung» für automatisierte und vernetzte Systeme, CR 3/2019, S. 141 ff. (zit. Schmid, Pflicht)

Schopper Alexander/Raschner Patrick, Der internationale Anwendungsbereich der KI-VO in Drittstaatskonstellationen, KIR 2025, S. 91 ff.

Schucht Carsten, 30 Jahre New Approach im europäischen Produktsicherheitsrecht – prägendes Steuerungsmodell oder leere Hülle?, EuZW 2/2017 (zit. Schucht, New Approach)

Schucht Carsten, Der Einfluss des Produktsicherheits- auf das Produkthaftungsrecht – eine Analyse anhand des Entwurfs einer EU-Produkthaftungsrichtlinie, InTeR 2023, S. 71 ff. (zit. Schucht, Einfluss)

Schucht Carsten, Die neuen Informationspflichten der Wirtschaftsakteure und Verkaufsplattformen bei Verbraucherprodukten – Teil 1, CB 2024, S. 397 ff. (zit. Schucht, Informationspflichten)

Schucht Carsten, Produktkrisen-Management als Compliance-Aufgabe, CB 2023, S. 312 ff. (zit. Schucht, Produktkrisen)

Schucht Carsten, Wiebe Gerhard, Die neue EU-Produktsicherheitsverordnung, General Product Safety Regulation (GPSR), Baden-Baden, 2024 (zit. NP GPSR-Schucht/Wiebe)

Schucht, Carsten/Wiebe, Gerhard/Becker, Ulrich/Daehlen, Johannes (Hrsg.), EU-Produktsicherheitsverordnung, General Product Safety Regulation. Nomos Handkommentar, Baden-Baden, 2025 (zit. NHK GPSR-Bearbeiter/in)

Schuett Jonas, Risk Management in the Artificial Intelligence Act, Eur. j. risk regul. 2/2023, S. 1 ff.

Schwenke Thomas, Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog, DSB 2024, S. 205 ff.

Schwenzer Ingeborg/Fountoulakis Christiana, Schweizerisches Obligationenrecht, Allgemeiner Teil, 8. Aufl., Bern, 2020

Seiler Hansjörg, Recht und technische Risiken, Grundzüge des technischen Sicherheitsrechts, Zürich, 1997

Sheikh Haroon/Prins Corien/Schrijvers Erik, Mission AI, The New System Technology, Cham, 2023

Spindler Gerald, Die Vorschläge der EU-Kommission zu einer neuen Produkthaftung und zur Haftung von Herstellern und Betreibern Künstlicher Intelligenz, CR 11/2022, S. 689 ff. (zit. Spindler, Vorschläge)

Spindler Gerald, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien?, CR 12/2015, S. 766 ff. (zit. Spindler, Roboter)

Stiemerling Oliver, Was ist ein KI-System im Sinne der KI-VO? – Erste Ansätze zur praktischen Abgrenzung «normaler» Systeme der Informationsverarbeitung, CR 8/2024, S. 554 ff.

Straub Wolfgang, Produktehaftung für Informationstechnologiefehler, Genf/Zürich/Basel/Zürich/Basel/Genf, 2002 (zit. Straub, Produktehaftung)

Straub Wolfgang, Software als Produkt, Jusletter 18.03.2002

Taeger, Jürgen/Pohle, Jan (Hrsg.), Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, 38. Aufl., München, 2023 (zit. Bearbeiter/in, in: Taeger/Pohle)

Thouvenin Florent/Volz Stephanie/Weiner Soraya/Heitz Christoph, Diskriminierung beim Einsatz von Künstlicher Intelligenz (KI), Jusletter IT 04.07.2024

Twigg-Flesner Christian, Guiding Principles for Updating the Product Liability Directive for the Digital Age, European Law Institute, Wien, 2021

Voigt Paul/Hullen Nils, Handbuch KI-Verordnung, FAQ zum AI Act, Berlin, 2024

Wagner Gerhard, Die Richtlinie über KI-Haftung: Viel Rauch, wenig Feuer, JZ 4/2023, S. 123 (zit. Wagner, Rauch)

Wagner Gerhard, Produkthaftung für autonome Systeme, AcP 6/2017, S. 707 ff. (zit. Wagner, Produkthaftung)

Wagner Gerhard, Produkthaftung für das digitale Zeitalter – ein Paukenschlag aus Brüssel, JZ 1-2/2023, S. 1 (zit. Wagner, Paukenschlag)

Wagner Gerhard, Verantwortlichkeit im Zeichen digitaler Techniken, VersR 12/2020, S. 717 ff. (zit. Wagner, Verantwortlichkeit)

Waldmann, Bernhard/Belser, Eva Maria/Epiney, Astrid (Hrsg.), Bundesverfassung. Basler Kommentar, Basel, 2015 (zit. BSK BV-Bearbeiter/in)

Weltersbach Max/Aslan Gabriel, Praktische Umsetzung der KI-VO – Komponenten zur strategischen Ausrichtung, BKR 2/2025, S. 49 ff.

Wendehorst Christiane/Nessler Bernhard/Aufreiter Alexander/Aichinger Gregor, Der Begriff des «KI-Systems» unter der neuen KI-VO, MMR 2024, S. 605 ff.

Werro Franz, La responsabilité civile, 3. Aufl., Bern, 2017

Widmer Lüchinger, Corinne/Oser, David (Hrsg.), Obligationenrecht I, Art. 1-529 OR. Basler Kommentar, 7. Aufl., Basel, 2020 (zit. BSK OR I-Bearbeiter/in)

Wiebe Gerhard, IT-sicherheitsbezogene Pflichten von Herstellern smarter Produkte, InTeR 2021, S. 66 ff. (zit. Wiebe, Pflichten)

Wildhaber Isabelle, Eine Einführung in die ausservertragliche Haftung für Künstliche Intelligenz (KI), HAVE 2021, S. 15 ff. (zit. Wildhaber, Einführung)

Wildhaber Isabelle, KI und Haftung: Lösungsansätze für die Schweiz, Jusletter IT 04.07.2024

Wildhaber Isabelle/Rey Heinz, Ausservertragliches Haftpflichtrecht, 6. Aufl., Zürich, 2024

Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating artificial intelligence, Cham, 2020 (zit. Bearbeiter/in, in: Wischmeyer/Rademacher)

Wittbrodt Saskia, Industrie 4.0 und die Haftung für Maschinensoftware, InTeR 2020, S. 74 ff.

Wittig Daniel, Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten, Dissertation, Münster, Schriften zum Medien- und Informationsrecht Band 50, Baden-Baden, 2021

Yamashita, Naomi/Evers, Vanessa/Yatani, Koji/Ding, Xianghua/Lee, Bongshin/Chetty, Marshini/Toups-Dugas, Phoebe (Hrsg.), Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, New York, 2025 (zit. Bearbeiter/in, in: Yamashita et al.)

Zech Herbert, Empfehlen sich Regelungen zu Verantwortung und Haftung beim Einsatz Künstlicher Intelligenz?, NJW-Beil. 2022, S. 33 ff. (zit. Zech, Regelungen)

Zech Herbert, Verhandlungen des 73. Deutschen Juristentages Hamburg 2020/Bonn 2022, Band I: Gutachten, München, 2020 (zit. Zech, Gutachten)

Schweizer Materialien

BAKOM, Analyse der Regulierung von künstlicher Intelligenz in verschiedenen Ländern und Weltregionen, Basisanalyse für die Auslegeordnung zur Regulierung von künstlicher Intelligenz vom 16.12.2024 (zit. BAKOM, Länderanalyse KI)

BAKOM, Überblick zu aktuellen sektoriellen Regulierungsaktivitäten im Zusammenhang mit Künstlicher Intelligenz, BAKOM-Bericht vom 16.12.2024 (zit. BAKOM, Überblick Sektorregulierung KI)

BAKOM, Auslegeordnung zur Regulierung von künstlicher Intelligenz, Bericht an den Bundesrat vom 12.02.2025 (zit. BAKOM, Auslegeordnung KI)

BJ, Rechtliche Basisanalyse im Rahmen der Auslegeordnung zu den Regulierungsansätzen im Bereich künstliche Intelligenz vom 31.08.2024 (zit. BJ, Rechtliche Basisanalyse KI)

Bundesrat, Leitlinien «Künstliche Intelligenz» für den Bund, Orientierungsrahmen für den Umgang mit künstlicher Intelligenz in der Bundesverwaltung vom 25.11.2020 (zit. Bundesrat, Leitlinien)

Botschaft zur Revision des Fernmeldegesetzes vom 6. September 2017, BBl 2017 6559 (zit. Botschaft FMG)

Botschaft über das Folgeprogramm nach der Ablehnung des EWR-Abkommens vom 24. Februar 1993, BBl 1993 I 805 (zit. Botschaft über das Folgeprogramm nach der Ablehnung des EWR-Abkommens)

Botschaft zum Bundesgesetz über Lebensmittel und Gebrauchsgegenstände vom 25. Mai 2011, BBl 2011 5571 vom 25.05.2011 (zit. Botschaft LMG)

Botschaft zum Produktesicherheitsgesetz (Totalrevision des Bundesgesetzes über die Sicherheit von technischen Einrichtungen und Geräten) vom 25. Juni 2008, BBl 2008 7407 (zit. Botschaft PrSG)

EKK, Empfehlung EKK vom 27. Januar 2021 betreffend Internet der Dinge (IoT): Funktioniert ein «Ding» ohne Datenverkehr? (zit. EKK, Empfehlung)

ESTI, Aufsichts- und Kontrollaufgaben des ESTI, Welche Aufgaben weisen das Elektrizitätsgesetz und seine Ausführungsverordnungen dem ESTI zu? vom 01.08.2012 (zit. ESTI, Aufsichts- und Kontrollaufgaben)

Geschäftsstelle CNAI, Terminologie, Kompetenznetzwerk CNAI vom 15.12.2021, Version 1.0 (zit. Geschäftsstelle CNAI, Terminologie Version 1.0)

Geschäftsstelle CNAI, Terminologie, Kompetenznetzwerk CNAI vom 21.12.2023, Version 2.1 (zit. Geschäftsstelle CNAI, Terminologie Version 2.1)

IK-EUDP, Die Schweiz und die Digitalstrategie der Europäischen Union, Kommission von der Leyen (2023) vom 15.03.2023 (zit. IK-EUDP, Schweiz)

Produktsicherheit, Änderung des Bundesgesetzes über die Sicherheit von technischen Einrichtungen und Geräten (STEG), Bericht über die Ergebnisse des Vernehmlassungsverfahrens vom 24.01.2007 (zit. Bericht Vernehmlassungsverfahren STEG)

SBFI, Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» an den Bundesrat vom 13.12.2019 (zit. SBFI, KI Bericht)

SECO, FAQ zum Bundesgesetz über die Produktesicherheit (PrSG; SR 930.11) und zur Verordnung über die Produktesicherheit (PrSV; SR 930.111) vom 03.09.2015 (zit. SECO, FAQ)

SECO, Handelsstatistik zum Abkommen der Schweiz und der EU über die gegenseitige Anerkennung von Konformitätsbewertungen (MRA) – 2023 vom 06.08.2024 (zit. SECO, Handelsstatistik MRA)

UVEK, Erläuternder Bericht zur Revision der Verordnung über elektrische Niederspannungserzeugnisse (NEV, SR 734.26) vom 01.03.2021 (zit. UVEK, Erläuternder Bericht Revision NEV)

EU-Materialien

Antwort von Lord Cockfield im Namen der Kommission vom 15.11.1988, ABl. C 114/1 vom 08.05.1989 (zit. Antwort)

Entschliessung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung, New Approach, ABl. C 136/1 vom 04.06.1985 (zit. New Approach)

Europäische Kommission, EU General Product Safety Regulation, Frequently asked questions (FAQ), Questions and Answers about the GPSR (zit. Europäische Kommission, GPSR FAQ)

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, dem Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Künstliche Intelligenz für Europa vom 25.04.2018, COM(2018) 237 final (zit. Europäische Kommission, Mitteilung)

Europäische Kommission, Durchführungsbeschluss (EU) 2019/417 der Kommission vom 8. November 2018 zur Festlegung von Leitlinien für die Verwaltung des gemeinschaftlichen Systems zum raschen Informationsaustausch «RAPEX» gemäss Artikel 12 der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit und für das dazugehörige Meldesystem, ABl. L 73/121 vom 15.03.2019, ausser Kraft (zit. Europäische Kommission, RAPEX-Leitlinie)

Europäische Kommission, Konsolidierte Fassung vom 17.05.2023, Durchführungsbeschluss (EU) 2019/417 der Kommission vom 8. November 2018 zur Festlegung von Leitlinien für die Verwaltung des gemeinschaftlichen Systems zum raschen Informationsaustausch «RAPEX» gemäss Artikel 12 der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit und für das dazugehörige Meldesystem, ABl. L 73/121 vom 15.03.2019, ausser Kraft (zit. Europäische Kommission, Konsolidierte RAPEX-Leitlinie)

Europäische Kommission, Weissbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen vom 19.02.2020, COM(2020) 65 final (zit. Europäische Kommission, Weissbuch KI)

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021, COM(2021) 206 final (zit. Europäische Kommission, Vorschlag KI-VO)

Europäische Kommission, Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, Impact Assessment GPSR Proposal vom 30.06.2021, SWD(2021) 168 final (zit. Europäische Kommission, Impact Assessment GPSR)

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die allgemeine Produktsicherheit, Vorschlag GPSR vom 30.06.2021, COM(2021) 346 final (zit. Europäische Kommission, Vorschlag GPSR)

Europäische Kommission, CASP 2020, Recall effectiveness, Recall process from A to Z: Guidance for economic operators and market surveillance authorities vom 22.07.2021 (zit. Europäische Kommission, CASP 2020)

Europäische Kommission, Bekanntmachung der Kommission – Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 («Blue Guide»), ABl. C 247/1 vom 29.06.2022 (zit. Europäische Kommission, Blue Guide)

Europäische Kommission, Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte vom 28.09.2022, COM(2022) 495 final (zit. Europäische Kommission, Vorschlag PLD 2024)

Europäische Kommission, Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission – Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act) vom 06.02.2025, C(2025) 924 final (zit. Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25))

Europäische Kommission, Liste der förmlich aus dem Besitzstand zu streichenden Rechtsakte, ABl. C 2025/1229 vom 26.03.2025

Europäisches Parlament, Stellungnahme des Rechtsausschusses für den Ausschuss für Binnenmarkt und Verbraucherschutz zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 87/357/EWG des Rates und der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates (COM(2021)0346 – C9-0245/2021 – 2021/0170(COD)), Rechtsausschuss vom 18.03.2022, 2021/0170(COD) (zit. Europäisches Parlament, Stellungnahme GPSR)

Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 87/357/EWG des Rates und der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates (COM(2021)0346 – C9-0245/2021 – 2021/0170(COD)), Plenarsitzungsdokument vom 24.06.2022, A9-0191/2022 (zit. Europäisches Parlament, Bericht Vorschlag GPSR)

Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Plenarsitzungsdokument vom 22.05.2023, A9-0188/2023 (zit. Europäisches Parlament, Bericht Vorschlag KI-VO)

Europäisches Parlament, Gesetz über künstliche Intelligenz, Abänderungen des Europäischen Parlaments vom 14. Juni 2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) vom 14.06.2023, P9_TA(2023)0236 (zit. Europäisches Parlament, Abänderung Gesetz über KI)

Europäisches Parlament, Procedure File 2021/0106(COD), Ordentliches Gesetzgebungsverfahren, Artificial Intelligence Act vom 12.07.2024, 2021/0106(COD) (zit. Europäisches Parlament, Gesetzgebungsverfahren KI-VO)

Expert Group on Liability and New Technologies, Liability for artificial intelligence and other emerging digital technologies vom 2019 (zit. Expert Group on Liability and New Technologies, Liability)

High-Level Expert Group on Artificial Intelligence, A definition of AI: Main capabilities and scientific disciplines vom 18.12.2018 (zit. High-Level Expert Group on Artificial Intelligence, A definition of AI)

Low Voltage Directive 2014/35/EU Guidelines, Electrical equipment designed for use within certain voltage limits vom August 2018, (LVD Guide) (zit. Leitlinie LVD)

Schweizer Entscheide

BGE 64 II 254
BGE 116 II 525
BGE 124 III 350
BGE 129 III 335
BGE 133 III 81
BGE 134 IV 189
BGE 137 III 226
BGE 139 II 534
BGE 142 V 342
BGE 143 II 518
BGE 143 V 418
BGE 145 III 63
BGE 146 II 265
BGE 146 III 169
BVGer A-5814/2009 vom 24.08.2010
BGer 2C_905/2010 vom 22.03.2011
BGer 2C_488/2012 vom 01.04.2013
BVGer C-1177/2012 vom 12.06.2014
BVGer C-6412/2012 vom 03.11.2014
BVGer C-6342/2013 vom 23.02.2015
BGer 9C_482/2014 vom 20.03.2015
BVGer C-4660/2013 vom 28.05.2015
BVGer C-4789/2015 vom 29.01.2016
BVGer A-727/2016 vom 13.07.2016
BVGer C-914/2013 vom 06.10.2016
BVGer A-3085/2016 vom 26.06.2017
BVGer A-2734/2020 vom 02.08.2021
BVGer C-3805/2020 vom 09.05.2022
BVGer A-4413/2021 vom 20.09.2023
BGer 2C-136/2024 vom 13.09.2024

BGer 1C_63/2023 vom 17.10.2024

BVGer A-5896/2023 vom 05.11.2024

Urteil des Obergerichts des Kantons Zürich UE140296 vom 03.08.2015

EU-Entscheide

EuGH vom 20.02.1979, 120/78, Rewe-Zentral (Cassis de Dijon), ECLI:EU:C:1979:42

EuGH vom 12.11.1996, C-84/94, Vereinigtes Königreich / Rat, ECLI:EU:C:1996:431

EuGH vom 10.05.2001, C-203/99, Veedfald, ECLI:EU:C:2001:258

EuGH vom 09.09.2003, C-151/02, Jaeger, ECLI:EU:C:2003:437

EuGH vom 09.02.2006, C-127/04, O'Byrne, ECLI:EU:C:2006:93

EuGH vom 03.07.2012, C-128/11, UsedSoft, ECLI:EU:C:2012:407

EuGH vom 19.09.2013, C-579/12 RX-II, Réexamen Commission / Strack, ECLI:EU:C:2013:570

EuGH vom 21.10.2014, C-503/13, Boston Scientific Medizintechnik, ECLI:EU:C:2014:2306

EuGH vom 04.06.2015, C-195/14, Teekanne, ECLI:EU:C:2015:361

EuGH vom 10.06.2021, C-65/20, KRONE – Verlag, ECLI:EU:C:2021:471

Erlasse

Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die gegenseitige Anerkennung von Konformitätsbewertungen (Mutual Recognition Agreement) in Kraft getreten am 01.06.2002, SR 0.946.526.81 (zit. MRA)

Berichtigung der Durchführungsverordnung (EU) 2024/1435 der Kommission vom 24. Mai 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates zur Festlegung einer Vorlage für eine Rückrufanzeige (Amtsblatt der Europäischen Union L, 2024/1435, 27. Mai 2024), in: ABl. L 2024/90426 vom 24.07.2024 (zit. Vorlage Rückrufanzeige)

Beschluss des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE-Konformitätskennzeichnung, in: ABl. L 220/23 vom 30.08.1993 (zit. Global Approach)

Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates (New Legislative Framework), in: ABl. L 218/82 vom 13.08.2008 (zit. NLF)

Bundesgesetz betreffend die elektrischen Schwach- und Starkstromanlagen (Elektrizitätsgesetz) vom 24. Juni 1902, SR 734.0 (zit. EleG)

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220 (zit. OR)

Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz) vom 15. Dezember 2000, SR 812.21 (zit. HMG)

Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 9. Oktober 1992, SR 231.1 (zit. URG)

Bundesgesetz über den Datenschutz (Datenschutzgesetz) vom 25. September 2020, SR 235.1 (zit. DSG)

Bundesgesetz über den Umweltschutz (Umweltschutzgesetz) vom 7. Oktober 1983, SR 814.01 (zit. USG)

Bundesgesetz über die Gentechnik im Ausserhumanbereich (Gentechnikgesetz) vom 21. März 2003, SR 814.91 (zit. GTG)

Bundesgesetz über die Produktehaftpflicht (Produktehaftpflichtgesetz) vom 18. Juni 1993, SR 221.112.944 (zit. PrHG)

Bundesgesetz über die Produktesicherheit (Produktesicherheitsgesetz) vom 12. Juni 2009, SR 930.11 (zit. PrSG)

Bundesgesetz über die Sicherheit von technischen Einrichtungen und Geräten vom 19. März 1976, ausser Kraft, SR 819.1 (zit. STEG)

Bundesgesetz über die technischen Handelshemmnisse vom 6. Oktober 1995, SR 946.51 (zit. THG)

Bundesgesetz über Lebensmittel und Gebrauchsgegenstände (Lebensmittelgesetz) vom 20. Juni 2014, SR 817.0 (zit. LMG)

Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999, SR 101 (zit. BV)

Delegierte Verordnung (EU) 2024/3173 der Kommission vom 27. August 2024 zur Ergänzung der Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates um Vorschriften für den Zugang zum Schnellwarnsystem Safety Gate, den Betrieb des Systems, die in das System einzugebenden Informationen, die für Meldungen zu erfüllenden Anforderungen und die Kriterien für die Bewertung des Risikoniveaus, in: ABl. L 2024/3173 vom 13.12.2024 (zit. Delegierte VO (EU) 2024/3173)

Entscheidung der Kommission vom 14. Dezember 2004 zur Festlegung von Leitlinien für die Meldung gefährlicher Verbrauchsgüter bei den zuständigen Behörden der Mitgliedstaaten durch Hersteller und Händler nach Artikel 5 Absatz 3 der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates, ausser Kraft

Konsolidierte Fassungen vom 15.03.2025 des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, in: ABl. C 202/1 vom 07.06.2016 (zit. AEUV)

Lebensmittel- und Gebrauchsgegenständeverordnung vom 16. Dezember 2016, SR 817.02 (zit. LGV)

Medizinprodukteverordnung vom 1. Juli 2020, SR 812.213 (zit. MepV)

Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates (Product Liability Directive), in: ABl. L 2024/2853 vom 18.11.2024 (zit. PLD 2024)

Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit, in: ABl. L 11/4 vom 15.01.2002 (zit. Produktsicherheitsrichtlinie)

Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung), (Maschinenrichtlinie), in: ABl. L 157/24 vom 09.06.2006 (zit. MRL)

Richtlinie 2014/30/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit (Neufassung), in: ABl. L 96/79 vom 29.03.2014 (zit. EMV-RL)

Richtlinie 2014/35/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen auf dem Markt (Niederspannungsrichtlinie, Low Voltage Directive), in: ABl. L 96/357 vom 29.03.2014 (zit. LVD)

Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (Radio Equipment Directive), in: ABl. L 153/62 vom 22.05.2014 (zit. RED)

Richtlinie 73/23/EWG des Rates vom 19. Februar 1973 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen, in: ABl. L 77/29 vom 26.03.1973

Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (Product Liability Directive), in: ABl. L 210/29 vom 07.08.1985 (zit. PLD 1985)

Richtlinie 87/357/EWG des Rates vom 25. Juni 1987 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Erzeugnisse, deren tatsächliche Beschaffenheit nicht erkennbar ist und die die Gesundheit oder die Sicherheit der Verbraucher gefährden, in: ABl. L 192/49 vom 11.07.1987 (zit. RL 87/357/EWG)

Richtlinie 92/59/EWG des Rates vom 29. Juni 1992 über die allgemeine Produktsicherheit, in: ABl. L 228/24 vom 11.08.1992 (zit. RL 92/59/EWG)

Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210 (zit. ZGB)

Verfassung der Weltgesundheitsorganisation für die Schweiz in Kraft getreten am 7. April 1948, SR 0.810.1 (zit. WHO-Verfassung)

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), in: ABl. L 119/1 vom 04.05.2016 (zit. DSGVO)

Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, in: ABl. L 117/1 vom 05.05.2017 (zit. MDR)

Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011 (Marktüberwachungsverordnung), in: ABl. L 169/1 vom 25.06.2019 (zit. MÜVO)

Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates (Maschinenverordnung), in: ABl. L 165/1 vom 29.06.2023 (zit. MVO)

Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates und der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates und der Richtlinie 87/357/EWG des Rates (General Product Safety Regulation), in: ABl. L 135/1 vom 23.05.2023 (zit. GPSR)

Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), in: ABl. L 2024/1689 vom 12.07.2024 (zit. KI-VO)

Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), in: ABl. L 2024/2847 vom 20.11.2024 (zit. CRA)

Verordnung des EDI über die Sicherheit von Spielzeug (Spielzeugverordnung) vom 15. August 2012, SR 817.023.11 (zit. VSS)

Verordnung des WBF über den Vollzug der Marktüberwachung nach dem 5. Abschnitt der Verordnung über die Produktesicherheit vom 18. Juni 2010, SR 930.111.5 (zit. ZustV-PrSV)

Verordnung über das Eidgenössische Starkstrominspektorat vom 7. Dezember 1992, SR 734.24 (zit. ESTI-Verordnung)

Verordnung über die elektromagnetische Verträglichkeit vom 25. November 2015, SR 734.5 (zit. VEMV)

Verordnung über die Produktesicherheit vom 19. Mai 2010, SR 930.111 (zit. PrSV)

Verordnung über die Sicherheit von Maschinen (Maschinenverordnung) vom 2. April 2008, SR 819.14 (zit. MaschV)

Verordnung über die technischen Anforderungen an Strassenfahrzeuge vom 19. Juni 1995, SR 741.41 (zit. VTS)

Verordnung über elektrische Niederspannungserzeugnisse (Niederspannungsverordnung) vom 25. November 2015, SR 734.26 (zit. NEV)

Verordnung über Fernmeldeanlagen vom 25. November 2015, SR 784.101.2 (zit. FAV)

Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung) vom 27. Mai 2020, ausser Kraft, SR 120.73 (zit. CyRV)

Weitere Quellen

Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Gefährliche Produkte 2020, Dortmund vom 21.05.2025, abrufbar unter <https://www.baua.de/DE/Angebote/Publikationen/Berichte/ProdSG-2020>, zuletzt besucht am 31.05.2025

Centre for Strategy and Evaluation Services, Study on the Impact of Artificial Intelligence on Product Safety vom 23.05.2022, abrufbar unter <https://www.gov.uk/government/publications/study-on-the-impact-of-artificial-intelligence-on-product-safety>, zuletzt besucht am 31.05.2025

ESTI, Tätigkeitsbericht 2023, abrufbar unter <https://www.esti.admin.ch/de/dokumentation/jahresrechnung>, zuletzt besucht am 31.05.2025 (zit. ESTI, Tätigkeitsbericht)

ISO/IEC 22989:2022(en) Information technology, Artificial intelligence, Artificial intelligence concepts and terminology (zit. ISO 22989:2022)

McCarthy John/Minsky Marvin L./Rochester Nathaniel/Shannon Claude E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence vom 31.08.1955, abrufbar unter <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>, zuletzt besucht am 31.05.2025

OECD, Consumer Product Safety In The Internet Of Things vom März 2018, abrufbar unter <https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/03/consumer-product-safety-in-the-internet-of-things_278edad0/7c45fa66-en.pdf>, zuletzt besucht am 31.05.2025 (zit. OECD, Consumer)

OECD, Measuring and maximising the impact of product recalls globally vom Oktober 2018, abrufbar unter <https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/10/measuring-and-maximising-the-impact-of-product-recalls-globally_5f1484b3/ab757416-en.pdf>, zuletzt besucht am 31.05.2025 (zit. OECD, Measuring)

OECD, Explanatory Memorandum on the Updated OECD Definition of an AI System vom März 2024, abrufbar unter <https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf>, zuletzt besucht am 31.05.2025 (zit. OECD, Explanatory Memorandum)

Robomow, Betriebsanweisungen (DE), abrufbar unter <https://www.galaxus.ch/Files/1/4/8/4/0/6/7/RC_2014_MANUAL_DE_HiRes.pdf>, zuletzt besucht am 31.05.2025

Internetquellen und Websites

A Hacker Speaks: How Malware Might Blow Up Your Laptop, abrufbar unter <https://www.pcworld.com/article/481440/batteries_go_boom.html>, zuletzt besucht am 31.05.2025

Aktuelle Rückrufe, abrufbar unter <https://www.konsum.admin.ch/bfk/de/home/produktesicherheit/produkterueckrufe/produktrueckrufe-und-sicherheitsinformationen-2020.html>, zuletzt besucht am 31.05.2025

Android malware posing as porn can literally make your phone's battery explode, abrufbar unter <https://www.ibtimes.co.uk/android-malware-posing-porn-can-literally-make-your-phones-battery-explode-1652008>, zuletzt besucht am 31.05.2025

Attorney General James Sues TikTok for Harming Children's Mental Health, abrufbar unter <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-tiktok-harming-childrens-mental-health>, zuletzt besucht am 31.05.2025

B AiR kitchen – Moley Robotics, abrufbar unter <https://www.moley.com/b-air-kitchen/>, zuletzt besucht am 31.05.2025

BFU – LANDI Schweiz AG ruft das «E-Trottinett Street, Artikel 82182» wegen Sturz- und Unfallgefahr zurück, abrufbar unter <https://www.news.admin.ch/de/nsb?id=89995>, zuletzt besucht am 31.05.2025

Bundesrat ermöglicht automatisiertes Fahren, abrufbar unter <https://www.news.admin.ch/de/nsb?id=103529>, zuletzt besucht am 31.05.2025

Bundesrat prüft Regulierungsansätze für Künstliche Intelligenz, abrufbar unter <https://www.news.admin.ch/de/nsb?id=98791>, zuletzt besucht am 31.05.2025

CEN und CENELEC, abrufbar unter <https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/?utm>, zuletzt besucht am 31.05.2025

Die Kommission veröffentlicht Leitlinien zur Definition von KI-Systemen, um die Anwendung des ersten KI-Gesetzes zu erleichtern, abrufbar unter <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>, zuletzt besucht am 31.05.2025

Dog's Tail Gets Stuck in Robotic Vacuum, abrufbar unter <https://www.youtube.com/watch?v=vYU3UJdB42k>, zuletzt besucht am 31.05.2025

Doku: Verliebt in einen KI-Avatar: Echte Liebe zu virtuellen Partnern, abrufbar unter <https://www.youtube.com/watch?v=T2ts2iQ8ELM>, zuletzt besucht am 31.05.2025

Dreame Robotic Lawnmower A2, abrufbar unter <https://ch.dreametech.com/en/products/a2>, zuletzt besucht am 31.05.2025

«Todesfalle! Finger weg»: Shitstorm um smartes Katzenklo, abrufbar unter <https://www.chip.de/news/Todesfalle-Finger-weg-Shitstorm-um-smartes-Katzenklo_185470392.html>, zuletzt besucht am 31.05.2025

Ecovacs Robotics: the AI robotic vacuum cleaner powered by TensorFlow — The TensorFlow Blog, abrufbar unter <https://blog.tensorflow.org/2020/01/ecovacs-robotics-ai-robotic-vacuum.html>, zuletzt besucht am 31.05.2025

Europarat, abrufbar unter <https://www.eda.admin.ch/eda/de/home/aussenpolitik/internationale-organisationen/europarat.html>, zuletzt besucht am 31.05.2025

Europaratskonvention zu KI unter Mitarbeit der Schweiz verabschiedet, abrufbar unter <https://www.news.admin.ch/de/nsb?id=101063>, zuletzt besucht am 31.05.2025

Familie und Freizeit – Roboter-Rasenmäher: Die unterschätzte Gefahr im Vorgarten, abrufbar unter <https://www.srf.ch/sendungen/kassensturz-espresso/familie-und-freizeit-roboter-rasenmaeher-die-unterschaetzte-gefahr-im-vorgarten>, zuletzt besucht am 31.05.2025

FAQ – Moley Robotics, abrufbar unter <https://www.moley.com/faq/>, zuletzt besucht am 31.05.2025

Formular für Inverkehrbringer, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Arbeit/Arbeitsbedingungen/Produktsicherheit/meldung_gefaehrlicher_produkte/meldung_gefaehrlicher_produkte_inverkehrbringer.html>, zuletzt besucht am 31.05.2025

Gartner Hype Cycle for Emerging Technologies 2024, abrufbar unter <https://www.gartner.com/en/articles/hype-cycle-for-emerging-technologies>, zuletzt besucht am 31.05.2025

Global Recalls portal (OECD), abrufbar unter <https://globalrecalls.oecd.org/#/>, zuletzt besucht am 31.05.2025

Google Trends «chatgpt», abrufbar unter <https://trends.google.com/trends/explore?date=2022-01-01%202025-05-31&q=chatgpt&hl=en-GB>, zuletzt besucht am 31.05.2025

Google Trends «generative AI», abrufbar unter <https://trends.google.com/trends/explore?date=2022-01-01%202025-05-31&q=generative%20ai&hl=en-GB>, zuletzt besucht am 31.05.2025

Google's AI Recommended Adding Glue To Pizza And Other Misinformation – What Caused The Viral Blunders?, abrufbar unter <https://www.forbes.com/sites/jackkelly/2024/05/31/google-ai-glue-to-pizza-viral-blunders/>, zuletzt besucht am 31.05.2025

Harmonised Standards for the European AI Act, abrufbar unter <https://ai-watch.ec.europa.eu/news/harmonised-standards-european-ai-act-2024-10-25_en?utm>, zuletzt besucht am 31.05.2025

How does a smartphone battery explode and how you can prevent it, abrufbar unter <https://www.business-standard.com/article/technology/what-leads-phones-batteries-to-explode-here-s-how-you-can-prevent-it-122091400621_1.html>, zuletzt besucht am 31.05.2025

How exactly do robot lawn mowers work?, abrufbar unter <https://www.techradar.com/home/small-appliances/how-do-robot-lawn-mowers-work?utm>, zuletzt besucht am 31.05.2025

How to find your lost Samsung Galaxy Buds, abrufbar unter <https://www.androidauthority.com/how-to-find-lost-galaxy-buds-3318610/>, zuletzt besucht am 31.05.2025

ISO – Artificial intelligence, abrufbar unter <https://www.iso.org/sectors/it-technologies/ai>, zuletzt besucht am 31.05.2025

Kasper Gabriel/Dal Molin Luca, EU Cyber Resilience Act's Impact on Swiss Companies, abrufbar unter <https://www.homburger.ch/de/insights/eu-cyber-resilience-acts-impact-on-swiss-companies?>, zuletzt besucht am 31.05.2025

KI-Regulierung: Bundesrat will Konvention des Europarats ratifizieren, abrufbar unter <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-104110.html>, zuletzt besucht am 31.05.2025

Künstliche Intelligenz, abrufbar unter <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/ki_leitlinien.html>, zuletzt besucht am 31.05.2025

Meet Samsung Bot Chef – A Future Concept for the Connected Home, abrufbar unter <https://www.youtube.com/watch?v=OD83rmDb3ss>, zuletzt besucht am 31.05.2025

More ChatGPT Jailbreaks Are Evading Safeguards On Sensitive Topics, abrufbar unter <https://www.forbes.com/sites/alexvakulov/2025/02/01/more-chatgpt-jailbreaks-are-evading-safeguards-on-sensitive-topics/>, zuletzt besucht am 31.05.2025

MRA Schweiz – EU, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0/MRA_Schweiz_EU.html>, zuletzt besucht am 31.05.2025

Navimow i Series – Ohne Kabel, ohne Sorgen, abrufbar unter <https://navimow.segway.com/de-ch/pages/navimow-i?from=eu-website>, zuletzt besucht am 31.05.2025

NEDA Suspends AI Chatbot for Giving Harmful Eating Disorder Advice, abrufbar unter <https://www.psychiatrist.com/news/neda-suspends-ai-chatbot-for-giving-harmful-eating-disorder-advice/?utm>, zuletzt besucht am 31.05.2025

OECD member Switzerland, abrufbar unter <https://www.oecd.org/en/countries/switzerland.html>, zuletzt besucht am 31.05.2025

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/internationale_organisationen/oecd.html>, zuletzt besucht am 31.05.2025

Organoleptisch, abrufbar unter <https://www.duden.de/rechtschreibung/organoleptisch>, zuletzt besucht am 31.05.2025

Parlament bereit für Verhandlungen über Regeln für sichere und transparente KI, abrufbar unter <https://www.europarl.europa.eu/news/de/press-room/20230609IPR96212/parlament-bereit-fur-verhandlungen-uber-regeln-fur-sichere-und-transparente-ki>, zuletzt besucht am 31.05.2025

Produktesicherheit – die BFU überwacht den Markt, abrufbar unter <https://www.bfu.ch/de/die-bfu/ueber-die-bfu/marktueberwachung-produktesicherheit>, zuletzt besucht am 31.05.2025

Produktesicherheit – Übersicht, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Arbeit/Arbeitsbedingungen/Produktsicherheit.html>, zuletzt besucht am 31.05.2025

RecallSwiss, abrufbar unter <https://www.recallswiss.admin.ch/customer-access/>, zuletzt besucht am 31.05.2025

Safety Gate: the EU rapid alert system for dangerous non-food products, abrufbar unter <https://ec.europa.eu/safety-gate-alerts/screen/search?resetSearch=true>, zuletzt besucht am 31.05.2025

Samsung CES 2020: the best thing at the booth is this salad-making Chef Bot, abrufbar unter <https://www.techradar.com/news/samsungs-bot-chef-made-me-a-salad-at-ces-2020-and-i-ate-it>, zuletzt besucht am 31.05.2025

Schweiz unterzeichnet Europaratskonvention zu KI, abrufbar unter <https://www.news.admin.ch/de/nsb?id=104646>, zuletzt besucht am 31.05.2025

Staatsvertragliche Vereinbarungen (Mutual Recognition Agreements – MRA), abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0.html>, zuletzt besucht am 31.05.2025

The DEADLY self-cleaning litter boxes that have flooded the market, abrufbar unter <https://www.youtube.com/watch?v=xepC3-Ia9ho&t>, zuletzt besucht am 31.05.2025

The World's First Robot Chef Is Finally Here, and It Even Cleans Up After Itself, abrufbar unter <https://robbreport.com/gear/electronics/moley-robotics-robot-kitchen-uk-for-sale-1234590791/>, zuletzt besucht am 31.05.2025

Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day, abrufbar unter <https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist>, zuletzt besucht am 31.05.2025

VASELLA DAVID, EU-Kommission: Leitlinien zum Begriff des AI-Systems, abrufbar unter <https://datenrecht.ch/eu-kommission-leitlinien-zum-begriff-des-ai-systems/>, zuletzt besucht am 31.05.2025

Verfahren 2021/0170/COD, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/HIS/?qid=1700667068845&uri=CELEX%3A32023R0988>, zuletzt besucht am 31.05.2025

Vernehmlassung 2025/9, Teilrevision des Bundesgesetzes über die Produktesicherheit (PrSG), abrufbar unter <https://www.fedlex.admin.ch/de/consultation-procedures/foreseen#https://fedlex.data.admin.ch/eli/dl/proj/2025/9/cons_1>, zuletzt besucht am 31.05.2025

Vorschriften für elektrische Trendfahrzeuge, abrufbar unter <https://www.astra.admin.ch/astra/de/home/themen/verkehrsregeln/vorschriften-trendfahrzeuge.html>, zuletzt besucht am 31.05.2025

Vorsicht vor billigen elektrischen Geräten aus dem Ausland, abrufbar unter <https://energeiaplus.com/2024/02/14/vorsicht-vor-billigen-elektrischen-geraeten-aus-dem-ausland/>, zuletzt besucht am 31.05.2025

Website CEN, Arbeitsprogramm, abrufbar unter <https://standards.cencenelec.eu/dyn/www/f?p=205:22:0:::FSP_ORG_ID,FSP_LANG_ID:2916257,22&cs=1B1700B5140A45B45CB5CB68BAF808643>, zuletzt besucht am 31.05.2025

Website des ASTRA, abrufbar unter <https://www.astra.admin.ch/astra/de/home/themen/intelligente-mobilitaet.html>, zuletzt besucht am 31.05.2025

Website des Bundesamts für Statistik, abrufbar unter <https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/digitale kompetenzen.html>, zuletzt besucht am 31.05.2025

Website des EDA, abrufbar unter <https://www.eda.admin.ch/eda/de/home/das-eda/aktuell/newsuebersicht/2023/europa.html>, zuletzt besucht am 31.05.2025

Website des SECO zur CE-Kennzeichnung, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0/CE-Kennzeichnung.html>, zuletzt besucht am 31.05.2025

Website OpenAI Platform, abrufbar unter <https://platform.openai.com/docs/models>, zuletzt besucht am 31.05.2025

Teil 1:
Einleitung

Gefährliche Produkte sind keine Neuheit, weshalb schon lange Pflichten für Hersteller bestehen, Produkte nach Inverkehrbringung zu beobachten und wenn nötig Massnahmen zu ergreifen, um Gefahren einzudämmen. Einigermassen neu ist jedoch die grosse Verbreitung «smarter» Produkte.[1] Es handelt sich dabei um elektrische Geräte mit einer Softwarekomponente. Software (und damit Künstliche Intelligenz, KI) kann für sich allein als einzelne Komponente und unabhängig von einem bestimmten physischen Gerät bereits eine Gefahr für die Gesundheit und Sicherheit von Menschen auslösen. 1

[1] WAGNER, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157; OECD, Consumer, S. 6.

A. Relevanz der Thematik

2 Da Hersteller ihren Produkten am nächsten sind und den grössten Einfluss auf deren Design, Entwicklungs-, Konstruktions- und Herstellungsprozess haben,[2] wird vorliegend auf die Pflichten für Hersteller eingegangen. In dieser Arbeit sollen insbesondere die produktsicherheitsrechtlichen Nachmarktpflichten für Software- und KI-Produkte am Beispiel von «Smart Home Devices»[3] in der Schweiz untersucht werden. Da das Schweizer Produktsicherheitsrecht zum grössten Teil auf dem EU-Recht basiert, wird ein Rechtsvergleich zum gegenwärtig stark veränderten EU-Recht gezogen.

I. Technischer Fortschritt von Konsumentenprodukten

3 Die technologischen Fortschritte in den letzten Jahren ermöglichen günstigere Speichermöglichkeiten und schnellere Rechenleistungen, während die Verfügbarkeit grosser Datenmengen (sog. «Big Data») stetig zunimmt.[4] Dies hat zu einer Welle[5] smarter Konsumentenprodukte wie Smart Home Devices (z.B. Sprachassistenten, Staubsaugerroboter, vernetzte Thermostate), Smart Wearables (z.B. Smart Watches und Smart Rings) und smarter Fahrzeuge (z.B. Autos mit Fahrassistenzsystemen und E-Scooter) geführt. Diese Produkte sind oftmals untereinander sowie mit dem Hersteller über das Internet verknüpft. Sie enthalten immer Software- und seit neuerem manchmal KI-Komponenten. Die in smarten Produkten enthaltene Software stellt einen wichtigen Bestandteil des Produktes dar. Die Software kann das Produkt bspw. physisch steuern oder anderweitig beeinflussen. Die deutsche Bundesanstalt für Arbeitsschutz und Arbeitsmedizin gibt in ihrem Bericht zur Produktsicherheit mangelhafte Software als zweithäufigstes Gefährdungsmerkmal an.[6]

---

2 NHK GPSR-Wiebe, Art. 5 N 37.

3 Zur Definition siehe Rn. 102.

4 Sheikh/Prins/Schrijvers, S. 38; Wischmeyer, in: Wischmeyer/Rademacher Rn. 1; Martini, Blackbox, S. 20 Fn. 86; siehe auch Molavi Vasse'i, S. 191.

5 Mit dem «Personal Computer» gibt es schon länger Geräte, die nur dazu dienen, mit Software zu interagieren bzw. diese auszuführen. Die Ausbreitung auf viele verschiedene Produkte wie Transportmittel und Haushaltsgeräte ist jedoch neu, Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.

6 Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Gefährliche Produkte 2020, Informationen zur Produktsicherheit, S. 27, Tabelle 2.9, abrufbar unter <https://www.baua.de/DE/Angebote/Publikationen/Berichte/ProdSG-2020>, zuletzt besucht am 31.05.2025.

II. Neue Regulierung in der EU

2023 wurde die europäische Produktsicherheitsrichtlinie[7] von der Produktsicherheitsverordnung[8] abgelöst und reformiert. Da das Schweizer PrSG[9] auf der alten europäischen Produktsicherheitsrichtlinie basiert, wird eine Überarbeitung des Produktsicherheitsrechts in der Schweiz nötig, wenn die Schweiz mit dem EU-Markt kompatibel bleiben will.[10] In der Schweiz ist deshalb Ende 2025 eine Teilrevision des PrSG geplant.[11] 2024 trat die KI-VO (auch: AI Act)[12] in Kraft, welche ebenfalls vor allem produktsicherheitsrechtliche Bestimmungen enthält und damit das bestehende Produktsicherheitsrecht ergänzt.[13] Genau wie das Produkthaftungsrecht wurde das Produktsicherheitsrecht in der Schweiz lange vor der weiten Verbreitung von KI reguliert, weshalb Anpassungen benötigt werden.[14] Im Bericht des BAKOMs an den Bundesrat über eine Auslegeordnung zur Regulierung von KI wurden drei mögliche Regulierungsansätze in Bezug auf KI vorgeschlagen.[15] Aufgrund der Bestrebungen, im Be- 4

7 Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit, ABl. L 11/4 (zit. Produktsicherheitsrichtlinie).

8 Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates und der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates und der Richtlinie 87/357/EWG des Rates (General Product Safety Regulation), ABl. L 135/1 (zit. GPSR).

9 Bundesgesetz über die Produktesicherheit (Produktesicherheitsgesetz) vom 12. Juni 2009, SR 930.11 (zit. PrSG).

10 Eine solche Anpassung wurde bereits vorgenommen, als die Produktsicherheitsrichtlinie erlassen wurde, BÜHLER, Sicherheit, Rn. 8.

11 Vernehmlassung 2025/9, Teilrevision des Bundesgesetzes über die Produktesicherheit (PrSG), abrufbar unter <https://www.fedlex.admin.ch/de/consultation-procedures/foreseen#https://fedlex.data.admin.ch/eli/dl/proj/2025/9/cons_1>, zuletzt besucht am 31.05.2025.

12 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L 2024/1689 (zit. KI-VO).

13 S. u., Rn. 158.

14 BAKOM, Überblick Sektorregulierung KI, S. 37; WILDHABER, Jusletter IT 04.07.2024, Rn. 25, 29; WILDHABER/REY, 1409a; siehe auch mit Bezug auf das Produkthaftungsrecht, aber explizit Nachmarktpflichten erwähnend LOHMANN, Haftungsrahmen, S. 119.

15 Vorgeschlagen wurden die «Fortführung der themen- und sektorspezifischen Regulierungsaktivitäten», die «Ratifikation der KI-Konvention des Europarats mit einer Minimalumsetzung (Option 1) oder einer weitergehenden Umsetzung (Option 2)» und die «Ratifi-

reich der Produktsicherheit aus wirtschaftlichen Gründen eine Kompatibilität mit der Europäischen Union zu gewährleisten, könnten einzelne Bestimmungen der KI-VO in der Schweiz entweder im PrSG oder in den darauf basierenden sektoriellen Erlassen implementiert werden. Die genannten neuen europäischen Verordnungen enthalten wichtige neue Nachmarktpflichten für Wirtschaftsakteure, die ihre Produkte in der EU auf den Markt bringen. Um die Kompatibilität mit der EU im Bereich der Produktsicherheit weiterhin zu gewährleisten, wird die Schweiz voraussichtlich gezwungen sein, einige Neuerungen zu übernehmen. Zudem muss das Mutual Recognition Agreement (MRA) zwischen der Schweiz und der EU angepasst werden.[16]

5 2024 trat in der EU eine neue Produkthaftungsrichtlinie (PLD 2024)[17] in Kraft. Darin wird Stand-alone-Software (also Software, die unabhängig von einem physischen Gegenstand ist) als Produkt geregelt, was in der Schweiz auch schon lange diskutiert wird.[18] Auch die PLD 2024 kann die schweizerische Gesetzgebung zum PrSG beeinflussen, wird hier aber nur punktuell behandelt. Umgekehrt hat das Produktsicherheitsrecht grossen Einfluss auf die Produkthaftung,[19] weshalb das Thema der vorliegenden Arbeit auch für das Haftungsrecht relevant ist.[20] Nicht analysiert wird vorliegend die neue Cyberresilienzverordnung[21] der EU, da es dort um Security und nicht um Safety geht.[22]

kation der KI-Konvention und Umsetzung in Anlehnung an den AI Act der EU». BAKOM, Auslegeordnung KI, S. 2.

16 S. u., Rn. 64.

17 Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates (Product Liability Directive), ABl. L 2024/2853 (zit. PLD 2024).

18 S. u., Rn. 196 ff.

19 Fellmann, Tragweite, S. 7; siehe auch Wildhaber/Rey, Rn. 1496; zum europäischen Recht Schucht, Einfluss, S. 79; Lohsse/Schulze/Staudenmayer, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 22.

20 S. u., Rn. 148.

21 Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. L 2024/2847 (zit. CRA).

22 S. u., Rn. 265.

B. Kurzdefinitionen

Um das Lesen dieser Arbeit zu erleichtern, werden einige Definitionen an dieser Stelle bereits vorweggenommen. 6

I. Software- und KI-Produkte

KI ist eine Art von Software. Das bedeutet, dass sie mitgemeint sein kann, wenn von Software gesprochen wird. Software enthält jedoch nicht immer KI. Wenn spezifisch von KI die Rede ist, wird ausschliesslich auf lernfähige, autonome Software Bezug genommen.[23] Ein Softwareprodukt kann entweder aus einer eigenständigen Software (Stand-alone-Software) bestehen oder ein Gerät sein, das eine integrierte Software (Embedded Software) enthält.[24] Ein KI-Produkt hingegen umfasst entweder eine eigenständige Software, die ein KI-System beinhaltet, oder ein Gerät, in dem eine integrierte Software enthalten ist, die wiederum ein KI-System enthält. 7

Tabelle 1: Software- und KI-Produkte

Softwareprodukt	KI-Produkt
Stand-alone-Software	Stand-alone-Software (mit KI-System)
Gerät mit integrierter Software	Gerät mit integrierter Software (mit KI-System)

II. Nachmarktpflichten für Hersteller

Der Begriff «Nachmarktpflichten» findet sich in keinem Schweizer Gesetz. Dennoch werden die Pflichten nach dem Inverkehrbringen nach Art. 8 PrSG in dessen 3. Abschnitt in der Schweiz einheitlich Nachmarktpflichten genannt.[25] Auch in der Kommentierung zur GSPR wird der Ausdruck «Nachmarktpflichten» verwendet.[26] In der KI-VO heisst es in Art. 72 «Beobachtung nach dem Inverkehrbringen» (engl. «Post Market Monitoring»). Ebenso werden die Begriffe «Überwachung nach dem Inverkehrbringen» (engl. «Post Market Surveil- 8

23 S. u., Rn. 86 ff.
24 S. u., Rn. 79 ff.
25 BVGer C-4789/2015 vom 29.01.2016, E. 3.3.2; BVGer C-1177/2012 vom 12.06.2014, E.; Botschaft PrSG, S. 7441; statt vieler Gerster, Rn. 124.
26 Siehe bspw. NHK GPSR-Schucht, Art. 11 N 139.

lance»)[27] oder «After-Sales-Kontrolle»[28] verwendet. In Deutschland wird auch von «Rückrufmanagement» gesprochen.[29] Da sich der Begriff «Nachmarktpflichten» vor allem im allgemeinen Produktsicherheitsrecht etabliert hat,[30] wird hier weiterhin dieser Begriff verwendet.

9 Die Nachmarktpflichten gem. Art. 8 PrSG regeln die Pflichten von Herstellern (und weiteren Wirtschaftsakteuren) nach dem Inverkehrbringen von Konsumentenprodukten. Hersteller sind demnach verpflichtet, Massnahmen zu ergreifen, um auch nach dem Inverkehrbringen des Produktes Gefahren zu erkennen und die Bereitschaft zu gewährleisten, notwendige Sicherheitsvorkehrungen treffen zu können. Die Art der Massnahmen hängt vor allem vom Risikopotenzial des betreffenden Produktes ab. Des Weiteren trifft die Hersteller bei gefährlichen Produkten eine Meldepflicht an Behörden sowie eine Aufbewahrungspflicht bezüglich Informationen zur Rückverfolgbarkeit ihrer Produkte.[31]

10 Die Nachmarktpflichten sind nicht mit der Marktüberwachung zu verwechseln. Bei den Ersteren handelt es sich um Pflichten für verschiedene Parteien in der Lieferkette von Produkten. Neben dem hier genauer betrachteten Hersteller haben bspw. auch Importeure und Händler Nachmarktpflichten. Die Marktüberwachung ist die Kontrolle des Marktes durch den Staat, genauer durch die Marktüberwachungsbehörden.[32]

III. Softwareupdates

11 Software kann vom Hersteller i.d.R. und bei entsprechender Konfiguration aktualisiert (engl. «updated») werden.[33] Der Hersteller kann dem Nutzer bspw. via Internet eine neue Version der Software zur Verfügung stellen, welche der Nutzer dann herunterladen und installieren kann. Dadurch können sich die Funktionsweisen und Sicherheitseigenschaften von Softwareprodukten ver-

27 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. L 117/1 (zit. MDR), Art. 2 Ziff. 60.

28 SCHMID, Pflicht, Rn. 4.

29 FELLMANN, Jusletter 25.10.2010, Rn. 32; zum deutschen Recht Beck ProdSG-KAPOOR, § 6 N 47; mit Kritik SCHUCHT, Produktkrisen, S. 318.

30 Siehe auch im deutschen Recht Beck ProdSG-KAPOOR, § 6 N 55.

31 S. u., Rn. 305 ff.

32 S. u., Rn. 69.

33 S. u., Rn. 83 f.

ändern. Hersteller haben u.U. sogar die Möglichkeit, Software zu aktualisieren, ohne dass der Nutzer Einfluss darauf nehmen kann.[34]

[34] S. u., Rn. 354.

C. Gegenstand und Ziel der Arbeit

12 Diese Arbeit beschäftigt sich mit den herstellerseitigen Nachmarktpflichten für Produkte, die Software enthalten oder allein aus Software «bestehen». Insbesondere KI-Systeme sollen genauer betrachtet werden. Es wird ein Fokus auf die mögliche Veränderlichkeit dieser Produkte nach dem Inverkehrbringen gelegt. Das Ziel dieser Arbeit ist ein Rechtsvergleich zwischen den produktsicherheitsrechtlichen Nachmarktpflichten für Hersteller von Software- und KI-Produkten in der Schweiz und der EU. Zur Veranschaulichung sollen Smart Home Devices als Produktbeispiele dienen.

I. Gliederung

13 Der erste Teil beinhaltet die Einleitung in die Thematik und soll deren Relevanz aufzeigen. Zur einfacheren Lesbarkeit wurden soeben Kurzdefinitionen vorweggenommen. In diesem Abschnitt werden Gegenstand und Ziel der Arbeit dargelegt. Danach wird die Relevanz von produktsicherheitsrechtlichen Nachmarktpflichten für Software- und insbesondere für KI-Produkte mithilfe von Beispielen aufgezeigt. Sodann wird die Einbettung des Schweizer Produktsicherheitsrechts ins europäische System mit Auswirkung auf Gesellschaft und Wirtschaft beleuchtet.

14 Um das Thema zu verstehen, werden in einem zweiten Teil die Grundlagen dargelegt. Zuerst wird auf die technischen und rechtlichen Grundlagen für Software- und KI-Produkte eingegangen und die Definition von KI diskutiert. Danach werden die rechtlichen Grundlagen für die produktsicherheitsrechtlichen Nachmarktpflichten in der Schweiz und der EU beleuchtet.

15 Im dritten Teil dieser Arbeit wird aufgezeigt, inwiefern Nachmarktpflichten für Software- und KI-Produkte gelten. Danach wird erörtert, wer in der Schweiz und der EU als Hersteller gilt, der Nachmarktpflichten erfüllen muss. Weiter wird geklärt, ab welchem Zeitpunkt Nachmarktpflichten wahrgenommen werden müssen. Danach wird dargelegt, zu was die Nachmarktpflichten nach dem PrSG, der GPSR und der KI-VO die Hersteller verpflichten. Darüber hinaus wird geklärt, wie lange diese Pflichten beachtet werden müssen.

16 Der vierte und letzte Teil der Arbeit enthält eine zusammenfassende Darstellung mit tabellarischer Übersicht sowie ein Fazit. Darüber hinaus werden die zentralen Unterschiede zwischen den produktsicherheitsrechtlichen Nach-

marktpflichten für Hersteller von Software- und KI-Produkten in der Schweiz und der EU aufgezeigt. Abschliessend werden Anpassungen für das schweizerische Recht vorgeschlagen.

II. Methode

Um die rechtswissenschaftliche Problematik zu verstehen, müssen zuerst die technischen Grundlagen und Probleme dargelegt werden. Zur Analyse, inwiefern Software als Produkt verstanden werden kann, wird nach der etablierten Auslegungspraxis des BGer vorgegangen.[35] Da das PrSG und das PrHG eng miteinander verknüpft sind, wird zur Auslegung gewisser Punkte auch das PrHG bzw. die dazugehörige Literatur beigezogen.[36] Während diese Arbeit primär die produktsicherheitsrechtlichen Nachmarktpflichten für Hersteller von Softwareprodukten in der Schweiz klären soll, wird ein eingehender Rechtsvergleich zu diesen Pflichten gem. dem EU-Recht gezogen. Grundsätzlich muss Schweizer Recht, das auf europäischem Recht basiert, europakonform ausgelegt werden.[37] Wo nötig, wird deshalb auf die alte europäische Produktsicherheitsrichtlinie eingegangen, weil das PrSG auf dieser basiert. Vereinzelt und wo sinnvoll wird zur Veranschaulichung auf sektorielle Erlasse der Schweiz und der EU eingegangen. 17

III. Forschungslücke

Allgemein wurde wenig über die Produktsicherheit in der Schweiz und noch weniger über produktsicherheitsrechtliche Nachmarktpflichten geforscht. Soweit ersichtlich haben einige wenige Autorinnen und Autoren (insbesondere Bühler,[38] Hess,[39] Holliger-Hagmann,[40] und Tobler[41]) das PrSG umfassend oder auf spezifische Fragestellungen bezogen in mehreren Fachbeiträgen (vor 18

35 S. u., Rn. 197.

36 S. u., Rn. 148.

37 Kramer/Arnet, S. 356, m.w.H.

38 Bühler, Bestandteil; Bühler, Privatrecht; Bühler, Sicherheit; Bühler/Tobler, Produktsicherheit in der EU und in der Schweiz, Zürich, 2011.

39 SHK PrSG-Hess; Hess, Produktehaftung – Produktesicherheit.

40 Holliger-Hagmann, Büchse der Pandora; Holliger-Hagmann, Fallstricke; Holliger-Hagmann, Produktsicherheit und Haftpflicht; Haftpflichtkommentar-Holliger-Hagmann, Art. 1 PrSG ff.

41 Bühler/Tobler, Produktsicherheit in der EU und in der Schweiz, Zürich, 2011.

allem FELLMANN,[42] FORNAGE,[43] FURRER,[44] KLETT[45] und PFENNINGER[46]) intensiv behandelt.[47] Diese Texte sind (mit wenigen Ausnahmen) knapp zehn Jahre alt oder älter und gehen – wenn überhaupt – nur ansatzweise auf Software ein. Teilweise wurde das PrSG auch als «Nebenthema» zum Produkthaftungsrecht behandelt.[48] Die Dissertation von GERSTER[49] aus dem Jahr 2018 behandelt das PrSG eingehend und zeigt einige Probleme des Gesetzes anschaulich auf. Auf Softwareprodukte und die begleitenden Herausforderungen wird jedoch nicht eingegangen. KI wird in den letzten Jahren auch in rechtswissenschaftlichen Kreisen in der Schweiz viel diskutiert,[50] es fehlen aber Beiträge zu produktsicherheitsrechtlichen Nachmarktpflichten für KI-Produkte.[51] Einzig LOHMANN ging 2016 vertieft auf die Nachmarktpflichten nach Art. 8 PrSG in Bezug auf automatisierte Fahrzeuge ein.[52] Auch ein Rechtsvergleich zwischen produktsicherheitsrechtlichen Nachmarktpflichten in der Schweiz und der neuen Regulierung der EU wurde bis anhin nicht gezogen.

IV. Thematische Abgrenzung

19 Das Produktsicherheitsrecht ist in der Schweiz in diversen Erlassen geregelt. Produkte, die Software beinhalten, sind von speziellen Gesetzen oder Verord-

42 FELLMANN, Jusletter 25.10.2010; FELLMANN, Tragweite.

43 FORNAGE, in: Chappuis/Winiger/Campi; FORNAGE, Sécurité.

44 FURRER, in: Fellmann/Furrer, Schonzeit; FURRER, in: Fellmann/Furrer, Herausforderungen.

45 KLETT, Produktesicherheit; KLETT/MÜLLER, Rechtsentwicklung zum PrHG und PrSG, HAVE 2018, S. 438 ff.; KLETT, Digitalisierte; KLETT/VERDE, Medizinprodukt- und haftpflichtrechtliche Aspekte bei Medizinal-Apps, Sicherheit & Recht 1/2016, S. 45 ff.

46 PFENNINGER/SCHILD, in: Fellmann/Furrer, Herausforderungen; PFENNINGER, Produktsicherheitsrecht Schweiz – EU im Vergleich, AJP 2014, S. 1157 ff.

47 Siehe auch GERSTER, Rn. 6; HAAS/LEUTWILER, Nachmarktpflichten im Fokus internationaler Produktrückrufe, HAVE 2018, S. 452 ff.; WEY, in: Fellmann/Furrer, Schonzeit; BRUNNER, in: Fellmann/Furrer, Schonzeit; SCHWENZER/SCHMIDT, in: Guillod/Müller.

48 ROBERTO, Rn. 09.35; WILDHABER, Jusletter IT 04.07.2024; WILDHABER/REY, Rn. 493 ff.; WILDHABER, Einführung; FELLMANN, Haftpflichtrecht; LOHMANN, Haftungsrahmen; SHK PrHG-HESS.

49 GERSTER, Bundesgesetz über die Produktesicherheit (PrSG), Grundlagen, Pflichten und Folgen einer Pflichtverletzung unter besonderer Berücksichtigung des zivilrechtlichen Haftungsrechts, Dissertation, Zürich, 2018.

50 Siehe bspw. an verschiedenen Tagungen: GRAF/OBRECHT/WEINER, Jusletter 12.12.2022; GRAF/OBRECHT, Jusletter 29.11.2021.

51 Geht neben dem PrHG kurz auf das PrSG ein. Auf Nachmarktpflichten wird jedoch nicht eingegangen WILDHABER, Jusletter IT 04.07.2024, S. 18; siehe auch anekdotisch zu autonomen Drohnen HÄNSENBERGER, Drohnen, S. 135.

52 LOHMANN, Fahrzeuge, S. 359 ff.

nungen (sog. Sektorrecht) erfasst.[53] In einigen Bereichen wurde bereits Forschung betrieben, wie z.B. für autonome Fahrsysteme[54] und Drohnen[55] sowie für KI in Medizinprodukten[56]. Diese Arbeit konzentriert sich auf Smart Home Devices[57]. In diesem Bereich hat – soweit ersichtlich – noch keine vertiefte Auseinandersetzung im Produktsicherheitsrecht stattgefunden. Zudem werden sie immer relevanter.[58] Untersucht werden sollen damit nur Pflichten für Konsumentenprodukte (sog. B2C-Produkte), da die Nachmarktpflichten nach Art. 8 PrSG und die GPSR insgesamt nur auf Konsumentenprodukte anwendbar sind. Die KI-VO hingegen ist auch auf B2B-Produkte anwendbar.[59] Sie wird deshalb nur insoweit behandelt, als dies für Konsumentenprodukte relevant ist.

Nicht Gegenstand dieser Arbeit sind Lebensmittel, Kosmetika, Wasch- und Reinigungsprodukte, welche sich nach Inverkehrbringung ebenfalls verändern können, indem sie bspw. verderben. Weiter können sich Produkte verändern, indem Materialien verwittern oder erodieren. Diese möglichen Veränderungen nach dem Inverkehrbringen werden nicht behandelt. Obwohl die IT-Sicherheit oder Cybersicherheit (engl. «Cybersecurity») Teil der Produktsicherheit ist,[60] wird sie vorliegend ausgeklammert, da ihre Untersuchung den Rahmen dieser Arbeit sprengen würde. 20

53 S. u., Rn. 169.

54 Lohmann, Fahrzeuge; siehe auch die weiterführenden Informationen auf der Website des ASTRA, abrufbar unter <https://www.astra.admin.ch/astra/de/home/themen/intelligente-mobilitaet.html>, zuletzt besucht am 31.05.2025; Bundesrat ermöglicht automatisiertes Fahren, abrufbar unter <https://www.news.admin.ch/de/nsb?id=103529>, zuletzt besucht am 31.05.2025.

55 Hänsenberger, Drohnen, S. 130 ff.

56 Batache, Rn. 65 ff.

57 S. u., Rn. 102.

58 S. o., Rn. 3.

59 S. u., Rn. 184.

60 S. u., Rn. 265.

D. Relevanz von produktsicherheitsrechtlichen Nachmarktpflichten für Software und KI

21 Um darzulegen, weshalb produktsicherheitsrechtliche Nachmarktpflichten gerade im Bereich von Software- und KI-Produkten immer relevanter werden, wird in diesem Kapitel aufgezeigt, wie und weshalb Software- und KI-Produkte Personen und andere geschützte Rechtsgüter gefährden können. Dazu werden zunächst verschiedene Beispiele echter gefährlicher Produkte angeführt. Danach wird erörtert, worin die Risiken bei Software- und KI-Produkten liegen und was deren Ursachen sind. Weil Software und KI in Produkten auch Vorteile haben können, wird auch darauf eingegangen.

I. Beispiele unsicherer Software- und KI-Produkte und ihr Gefahrenpotenzial

22 Beeinträchtigen Konsumentenprodukte die körperliche Integrität von Menschen (oder ein vom jeweils anwendbaren Sektorrecht erfasstes Rechtsgut) in einer nicht mehr tolerierbaren Weise, handelt es sich um ein unsicheres Produkt.[61] Hersteller müssen dann verschiedene Nachmarktpflichten beachten.[62] Anhand verschiedener Beispiele wird deutlich gemacht, dass Software- und KI-Produkte Gefahren bergen können. Vorliegend wird zwischen Gefahren für die physische und für die psychische Gesundheit unterschieden.

1. Physische Gefahren durch Software und KI

23 Bei der Nutzung von Smart Home Devices sind verschiedene Gefahren zu berücksichtigen, wie etwa Überhitzung. Wenn Akkus oder Kabel nicht für die spezifische Stromstärke eines Ladegerätes ausgelegt sind, kann dies zu Brandgefahr führen, etwa durch zu dünne Kabel, die zu viel Strom leiten, oder durch Überhitzung beim Laden. Auch Fehler in der Software, die zu einer Überlastung des Systems führen – wie z.B. durch zu viele gleichzeitig durchgeführte Berechnungen, was besonders bei rechenintensiven KI-Prozessen der Fall ist – können problematisch sein. Dies führt zu Wärmeentwicklung in elektroni-

61 S. u., Rn. 267 f.
62 S. u., Rn. 305 ff.

schen Schaltelementen wie Transistoren, wodurch eine Überhitzung und im schlimmsten Fall Brandgefahr entsteht.[63] Ein weiteres Gefahrenpotenzial kann der Aktor sein, der eine Bewegung oder Drehung ausführt, im Gegensatz zum Sensor, der Daten erfasst.[64] Nachfolgende Beispiele sollen die Gefahren von Smart Home Devices veranschaulichen. Da von den Herstellern oftmals nicht transparent kommuniziert wird, wie die gefährliche Komponente genau funktioniert, kann nicht davon ausgegangen werden, dass es sich bei den unten aufgeführten Beispielen tatsächlich immer um KI-Produkte handelt. Auf jeden Fall ist bei allen Beispielen Software mindestens Teil der Gefahrenquelle. Die unten genannten Produkte fallen unter mindestens einen sektorrechtlichen Erlass und somit lediglich subsidiär unter das PrSG.[65] Wie sich jedoch zeigen wird, kann für die Nachmarktpflichten für Software auf das PrSG zurückgegriffen werden.

Beispielsweise können softwaregesteuerte Haushaltsgeräte wie «intelligente» Küchenroboter[66], die fähig sind, Kochabläufe auszuführen, eine Gefahr für Verwender, Dritte und Haustiere darstellen. Ein Beispiel für ein solches Produkt ist der Samsung Bot Chef in Abbildung 1. Solche Geräte können unerwartet reagieren und eine Person oder ein Tier verletzen, weil die Informationen aus den Sensoren von der Software nicht richtig verarbeitet werden und nicht zwischen einem Körperteil und Zutaten fürs Kochen unterschieden wird.[67] 24

63 Siehe auch Straub, Produktehaftung, Rn. 6.

64 S. u., Rn. 74.

65 S. u., Rn. 161 ff., 169 ff.

66 Bspw.: B AiR kitchen – Moley Robotics, abrufbar unter <https://www.moley.com/b-air-kitchen/>, zuletzt besucht am 31.05.2025; beim Samsung Bot Chef handelt es sich vorerst um ein Produktkonzept, The World's First Robot Chef Is Finally Here, and It Even Cleans Up After Itself, abrufbar unter <https://robbreport.com/gear/electronics/moley-robotics-robot-kitchen-uk-for-sale-1234590791/>, zuletzt besucht am 31.05.2025; Samsung CES 2020: the best thing at the booth is this salad-making Chef Bot, abrufbar unter <https://www.techradar.com/news/samsungs-bot-chef-made-me-a-salad-at-ces-2020-and-i-ate-it>, zuletzt besucht am 31.05.2025.

67 Siehe auch die Frage im FAQ «What if my pet jumps on the table?», FAQ – Moley Robotics, abrufbar unter <https://www.moley.com/faq/>, zuletzt besucht am 31.05.2025.

Abbildung 1: *Samsung Bot Chef*[68]

25 2024 wurde bekannt, dass automatische Katzentoiletten (sog. «Litterrobots») Katzen in der Öffnungsvorrichtung einklemmten und die Katzen daran starben. Die Konstruktion und Funktionsweise der Katzentoilette bergen Sicherheitsrisiken, da der Eingang aus hartem Kunststoff mit scharfen Kanten besteht, während eine rotierende Trommel im Inneren durch einen Motor bewegt wird. Wie die Abbildungen 2 und 3 zeigen, wird der Eingang während des Reinigungsvorgangs vollständig blockiert, was zum Einklemmen von Tieren und Körperteilen führte. Die Sensoren zur Unfallvermeidung, wie Infrarot-, Gewichts- und Klemmsensoren, funktionierten erst nach einem Firmware-Update.[69]

68 Die Bilder stammen aus dem Video Meet Samsung Bot Chef – A Future Concept for the Connected Home, abrufbar unter <https://www.youtube.com/watch?v=OD83rmDb3ss>, zuletzt besucht am 31.05.2025.

69 Zum ganzen Abschnitt siehe The DEADLY self-cleaning litter boxes that have flooded the market, ab Kapitel Cari Jay's TikTok videos about what happened to her cat, 2:14, abrufbar unter <https://www.youtube.com/watch?v=xepC3-Ia9ho&t>, zuletzt besucht am 31.05.2025; «Todesfalle! Finger weg»: Shitstorm um smartes Katzenklo, abrufbar unter <https://www.chip.de/news/Todesfalle-Finger-weg-Shitstorm-um-smartes-Katzenklo_185470392.html>, zuletzt besucht am 31.05.2025. Ein Hinweis bei neu verkauften Produkten, dass ein Update nötig sei, wurde in der Gebrauchsanweisung nicht dokumentiert.

Abbildung 2: *Eingeklemmte Plüschkatze im Roboter*[70]

Abbildung 3: *Eingeklemmte Hand im Roboter*[71]

[70] Das Bild stammt aus dem Video The DEADLY self-cleaning litter boxes that have flooded the market, 5:35, abrufbar unter <https://www.youtube.com/watch?v=xepC3-Ia9ho&t>, zuletzt besucht am 31.05.2025.

[71] Das Bild stammt aus dem Video The DEADLY self-cleaning litter boxes that have flooded the market, 8:08, abrufbar unter <https://www.youtube.com/watch?v=xepC3-Ia9ho&t>, zuletzt besucht am 31.05.2025.

26 Beliebte Smart Home Devices sind Staubsaugerroboter. Diese können bspw. Light Detection and Ranging and Simultaneous Localisation and Mapping (LiDar SLAM) und Kameras mit Objekterkennung (z.B. mittels Deep Neural Networks) nutzen.[72] Zudem waren bereits ältere Modelle mit Infrarotsensoren und sog. «Bumpers» ausgestattet, die mechanische Kollisionen mit Hindernissen erkennen. Identifizieren Staubsaugerroboter Hindernisse nicht richtig, können auch sie Gefahren verursachen, indem sie bspw. eine Treppe herunterfallen und dabei eine Person verletzen oder das Fell an der Rute eines Hundes einsaugen wie in Abbildung 4.[73]

Abbildung 4: *Staubsaugerroboter saugt Rute des Hundes ein*[74]

[72] Siehe eine detaillierte Erklärung zur Funktionsweise in Ecovacs Robotics: the AI robotic vacuum cleaner powered by TensorFlow – The TensorFlow Blog, abrufbar unter <https://blog.tensorflow.org/2020/01/ecovacs-robotics-ai-robotic-vacuum.html>, zuletzt besucht am 31.05.2025.

[73] Siehe bspw. in diesem Video, wobei nicht klar ist, ob es sich hier um einen automatischen Staubsauger mit Bilderkennung handelt, Dog's Tail Gets Stuck in Robotic Vacuum, abrufbar unter <https://www.youtube.com/watch?v=vYU3UJdB42k>, zuletzt besucht am 31.05.2025.

[74] Das Bild stammt aus dem Video Dog's Tail Gets Stuck in Robotic Vacuum, 0:19, abrufbar unter <https://www.youtube.com/watch?v=vYU3UJdB42k>, zuletzt besucht am 31.05.2025.

Zwar kein Smart Home Device[75], aber ein Beispiel aus der Schweiz ist der Fall eines Rasenmähroboters, der 2015 in den Zeh eines Kindes fuhr und diesen zerschnitt.[76] Laut der Bedienungsanleitung hätte der Mäher eine Funktion gehabt, Hindernisse zu erkennen und den Betrieb zu stoppen sowie in die entgegengesetzte Richtung des Hindernisses zu fahren.[77] Aus der Betriebsanweisung geht nicht hervor, welche Technologie der Blockierungssensor verwendete. Verbreitet sind heutzutage Rasenmähroboter, die gem. Herstellerangaben «intelligent» sind. So können sie u.a. Hindernisse mittels «KI-Kameras» oder anderer Sensoren (z.B. Real-Time Kinematic Global Positioning System (RTK GPS) oder LiDar SLAM) erkennen und diese entsprechend umfahren.[78] Rasenmähroboter funktionieren ähnlich wie Staubsaugerroboter. 27

Ebenfalls kein Smart Home Device, aber ein Fallbeispiel aus der Schweiz stellt das «E-Trottinett Street, Artikel 82182» dar. E-Trottinette gelten als «Leicht-Motorfahrräder» gem. Art. 18 lit. b VTS[79].[80] 2022 rief die LANDI Schweiz AG in Zusammenarbeit mit der Beratungsstelle für Unfallverhütung (BFU)[81] das E- 28

75 Rasenmäher gelten nicht als Haushaltsgeräte s. u., Rn. 169.

76 Es handelte sich um das Modell Robomow MC500 siehe auch Familie und Freizeit – Roboter-Rasenmäher: Die unterschätzte Gefahr im Vorgarten, abrufbar unter <https://www.srf.ch/sendungen/kassensturz-espresso/familie-und-freizeit-roboter-rasenmaeher-die-unterschaetzte-gefahr-im-vorgarten>, zuletzt besucht am 31.05.2025.

77 Robomow, Betriebsanweisungen (DE), Mähroboter, S. 6 Ziff. 1.4.5, abrufbar unter <https://www.galaxus.ch/Files/1/4/8/4/0/6/7/RC_2014_MANUAL_DE_HiRes.pdf>, zuletzt besucht am 31.05.2025.

78 Siehe bspw. den Segway-Navimow i105E Navimow i Series – Ohne Kabel, ohne Sorgen, abrufbar unter <https://navimow.segway.com/de-ch/pages/navimow-i?from=eu-website>, zuletzt besucht am 31.05.2025; und den Dreame Robotic Lawnmower A2 Dreame Robotic Lawnmower A2, abrufbar unter <https://ch.dreametech.com/en/products/a2>, zuletzt besucht am 31.05.2025; für eine Beschreibung zur Funktionsweise siehe bspw. How exactly do robot lawn mowers work?, abrufbar unter <https://www.techradar.com/home/small-appliances/how-do-robot-lawn-mowers-work?utm>, zuletzt besucht am 31.05.2025.

79 Verordnung über die technischen Anforderungen an Strassenfahrzeuge vom 19. Juni 1995, SR 741.41 (zit. VTS).

80 Siehe auch die Vorschriften über Zulassung und Betrieb von Motorfahrrädern, langsamen E-Bikes, E-Trottinetten und Elektro-Rikschas (Stand 1. April 2022), Vorschriften für elektrische Trendfahrzeuge, abrufbar unter <https://www.astra.admin.ch/astra/de/home/themen/verkehrsregeln/vorschriften-trendfahrzeuge.html>, zuletzt besucht am 31.05.2025.

81 Die BFU führt im Auftrag des ASTRA die Marktüberwachung von Strassenfahrzeugen durch, die nicht zulassungspflichtig sind. Produktesicherheit – die BFU überwacht den Markt, abrufbar unter <https://www.bfu.ch/de/die-bfu/ueber-die-bfu/marktueberwachung-produktesicherheit>, zuletzt besucht am 31.05.2025. Die Grundlage dafür ergibt sich aus Art. 220 Abs. 3 VTS i.V.m. Art. 20 PrSV.

Trottinett wegen Sturz- und Unfallgefahr zurück. Ein Softwarefehler führte dazu, «dass das Tempo nicht reduziert wird, wenn man vom Gas geht».[82] Laut Rückrufmitteilung (Abbildung 5) ist dies mit einer Sturz- und Unfallgefahr verbunden. Die LANDI bot an, das Gerät in die nächste Filiale zu bringen, um ein Softwareupdate installieren zu lassen, welches das Problem behob.

Abbildung 5: *Rückruf E-Trottinett*[83]

[82] BFU – LANDI Schweiz AG ruft das «E-Trottinett Street, Artikel 82182» wegen Sturz- und Unfallgefahr zurück, abrufbar unter <https://www.news.admin.ch/de/nsb?id=89995>, zuletzt besucht am 31.05.2025.

[83] Rückruf-Plakat der LANDI Schweiz AG, abrufbar unter BFU – LANDI Schweiz AG ruft das «E-Trottinett Street, Artikel 82182» wegen Sturz- und Unfallgefahr zurück, abrufbar unter <https://www.news.admin.ch/de/nsb?id=89995>, zuletzt besucht am 31.05.2025.

Neue Beispiele kommen laufend dazu. Aktuelle Produktrückrufe werden in der Schweiz über das Eidgenössische Büro für Konsumentenfragen (BFK) publiziert.[84] Leider lassen sich aufgrund von Beispielen keine gemeinsamen Ursachen für die gezeigten Gefahren ausmachen, da sich keine öffentlichen Informationen dazu finden lassen, wie genau es zur gefährlichen Funktion kam. Auf jeden Fall hat die Software aber einen Einfluss auf die sichere Verwendung obengenannter Produkte. Anschaulich lässt sich dies am E-Trottinett zeigen: Die gefährliche Software sollte wohl dafür sorgen, dass die Geschwindigkeit gedrosselt wird, wenn der Beschleunigungsauslöser nicht mehr betätigt wird. Dies ist eine Sicherheitsfunktion, die nicht richtig funktionierte. Ob es sich bei der gefährlichen Komponente um KI – also Software, die tatsächlich «lernfähig» bzw. «autonom» ist – handelt, spielt keine Rolle. Dennoch bergen KI-Produkte besondere Gefahren.[85] Natürlich können die meisten der oben beschriebenen Gefahren nicht nur durch Software, sondern auch durch mechanische Defizite entstehen. 29

2. Psychische Gefahren durch Software und KI

Wie sich unten zeigen wird, ist nicht nur die physische, sondern auch die psychische körperliche Unversehrtheit durch das Produktsicherheitsrecht geschützt. Es ist möglich, dass Software und KI-Systeme einen negativen Einfluss auf die psychische Gesundheit haben können.[86] Dies wird vorliegend anhand verschiedener Beispiele diskutiert. 30

Gefahren für die psychische Gesundheit können bspw. durch Algorithmen in sozialen Medien entstehen. Diese sind darauf ausgelegt, Inhalte zu zeigen, die auf vorherigen Interaktionen basieren. Die gezeigten Inhalte werden für Nutzende personalisiert, damit sie interessanter sind und die User deshalb mehr Zeit auf der Plattform verbringen.[87] Dies kann zu einer «Filterblase» führen, in der Nutzende nur noch Inhalte sehen, die die bestehenden Überzeugungen 31

---

84 Aktuelle Rückrufe, abrufbar unter <https://www.konsum.admin.ch/bfk/de/home/produktesicherheit/produkterueckrufe/produktrueckrufe-und-sicherheitsinformationen-2020.html>, zuletzt besucht am 31.05.2025; ebenfalls vom BFK herausgegeben wird RecallSwiss, abrufbar unter <https://www.recallswiss.admin.ch/customer-access/>, zuletzt besucht am 31.05.2025; weitere Beispiele für Produktrückrufe mit Software können via OECD-Seite gefunden werden, Global Recalls portal (OECD), abrufbar unter <https://globalrecalls.oecd.org/#/>, zuletzt besucht am 31.05.2025.

85 S. u., Rn. 36 ff. und 47 ff.

86 Beck KI-VO-Martini, Art. 14 N 55.

87 Costello et al., S. 137.

bestätigen und relativ unausgewogen sind.[88] Vorgeworfen wird, dass der Konsum dieser Inhalte die psychische Gesundheit beeinträchtigt.[89] Weit verbreitet sind mittlerweile verschiedene Chatbots. KI-basierte persönliche Assistenten (z.B. Chatbots wie Replika) könnten dazu führen, dass Menschen vermehrt digitale Interaktionen bevorzugen, anstatt persönliche soziale Kontakte zu pflegen.[90] KI-gestützte Chatbots werden zudem als unterstützendes Mittel in der psychologischen Beratung eingesetzt. Es hat sich jedoch gezeigt, dass diese Chatbots teilweise sehr schlechte und sogar gesundheitsschädliche Empfehlungen abgeben. So können Empfehlungen von trainierten Chatbots bspw. zu Essstörungen führen, welche neben der psychischen auch die physische Gesundheit beeinträchtigen.[91] Weiter können Chatbots beleidigend und diskriminierend werden.[92] Zudem könnte die Nutzung von KI-Filtern, die Personen in Bildern und Videos «schöner» erscheinen lassen, zu einem negativen Körperbild und damit zu psychischer Belastung führen.[93] Als mögliche Folgen der Nutzung werden soziale Isolation und Vernachlässigung von Offlinebeziehungen, Essstörungen, Angstzustände, Schlafstörungen, Depressionen, ein gestörtes Selbstwertgefühl und Suizidalität genannt.[94]

32 Problematisch an allen obengenannten Beispielen ist, dass es schwierig ist, die Kausalität zwischen der Interaktion der Software und der Beeinträchtigung der psychischen Gesundheit festzustellen.[95] Es ist fraglich, ob bereits psychisch beeinträchtigte Menschen zum Konsum der oben genannten Inhalte neigen und die Gesundheit z.B. aufgrund der Art, wie die Inhalte konsumiert werden, weiter darunter leidet, oder ob die Inhalte an sich eigentlich gesunde

88 Areeb et al., S. 3.

89 Costello et al., S. 135; siehe auch Attorney General James Sues TikTok for Harming Children's Mental Health, abrufbar unter <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-tiktok-harming-childrens-mental-health>, zuletzt besucht am 31.05.2025.

90 Zhang et al., in: Yamashita et al., S. 13; siehe auch die Reportage über «Replika». Doku: Verliebt in einen KI-Avatar: Echte Liebe zu virtuellen Partnern, abrufbar unter <https://www.youtube.com/watch?v=T2ts2iQ8ELM>, zuletzt besucht am 31.05.2025.

91 NEDA Suspends AI Chatbot for Giving Harmful Eating Disorder Advice, abrufbar unter <https://www.psychiatrist.com/news/neda-suspends-ai-chatbot-for-giving-harmful-eating-disorder-advice/?utm>, zuletzt besucht am 31.05.2025.

92 So z.B. der Chatbot Tay von Microsoft Beck KI-VO-Braun Binder/Egli, Art. 10 N 53; Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day, abrufbar unter <https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist>, zuletzt besucht am 31.05.2025.

93 Kleemans et al., S. 103.

94 Zhang et al., in: Yamashita et al., S. 13; Costello et al., S. 143; Europäische Kommission, Impact Assessment GPSR, S. 13 f.; siehe auch NHK GPSR-Wiebe, Art. 5 N 14.

95 S. u., Rn. 256.

Personen psychisch beeinträchtigen. Die Auswirkungen von KI-Systemen auf die psychische Gesundheit hängt stark von der individuellen Nutzung ab.[96] Hat eine Person bereits eine Beeinträchtigung der psychischen Gesundheit, könnten KI-Systeme diese verstärken. Dies hängt jedoch wiederum von der Veranlagung der betroffenen Person ab. Es wird deshalb schwierig sein, die Software bzw. das KI-System als Ursache der Gefahr und somit als unsicheres Produkt für die psychische Gesundheit anzuerkennen. Ein Beispiel eines KI-Systems, welches für sich allein die psychische Gesundheit einer gesunden Person schädigt, so wie dies ein System mit einer physischen Auswirkung (z.B. durch einen Stromschlag) kann, konnte nicht gefunden werden.

II. Eigenständiges Gefahrenpotenzial von Software- und KI-Produkten

Die alte RAPEX-Leitlinie zählte verschiedene klassische produktsicherheitsrechtliche Gefahren auf. Dazu gehörten z.B. die mechanische oder thermische Gefahr sowie die Stromschlag- oder Lärmgefahr.[97] Diese Gefahren können nicht nur von herkömmlichen Produkten ausgelöst werden, sondern auch von Software- und KI-Produkten. Software und KI müssen immer durch ein physisches Gerät genutzt werden, um eine physische Gefahr auszulösen, da sie selbst keine Körperlichkeit besitzen.[98] Auch um eine psychische Gefahr auszulösen, müssen bspw. KI-generierte Inhalte dem Nutzer mindestens über ein Gerät angezeigt werden. Vorweggenommen werden soll bereits zu diesem Zeitpunkt, dass vorliegend Stand-alone-Software als selbstständiges Produkt bzw. als eine selbständige Produktkomponente angesehen wird,[99] weil es sein kann, dass die Software die alleinige Ursache für eine Gefahr darstellt.[100] Software und KI stellen jedoch nicht für sich allein eine Gefahr dar, sondern Software und KI sind Produkte, die gefährliche Situationen auslösen oder zur Folge haben können. Dies ist vergleichbar mit einer Schraube. Die Schraube ist auch ein eigenständiges Produkt. Sie ist jedoch für sich allein nicht gefährlich. Wird die Schraube aber in verschiedenen Produkten verwendet und löst sie sich dann z.B. aufgrund eines Material- oder Konstruktionsfehlers, kann sie allein die Ursache einer Gefahr sein. 33

96 Ähnlich, jedoch mit Bezug auf digitales Zubehör NHK GPSR-Wiebe, Art. 5 N 15, m.w.H.; siehe auch Mattheis, S. 105.

97 S. u., Rn. 261.

98 Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.

99 S. u., Rn. 216.

100 Siehe auch Piovano/Schucht/Wiebe, S. 85.

34 Die Unterteilung zwischen integrierter oder Embedded Software und nichtintegrierter bzw. Stand-alone-Software im Produktsicherheitsrecht ist nach hier vertretener Meinung überholt[101] und kommt aus einer Zeit, in welcher Programme ausschliesslich speziell für ein bestimmtes technisches Gerät entwickelt wurden.[102] Die Unterscheidung wird der komplexen, vernetzten und oft hardwareunabhängigen Natur moderner Software- und KI-Systeme nicht mehr gerecht.[103] Die Grenze ist zunehmend schwieriger zu ziehen, da Applikationen online zur Verfügung gestellt und dann installiert werden können.[104] Es wäre dann zu fragen, ob eine installierte Applikation als «embedded» gilt oder ob diese als «stand-alone» zu betrachten wäre. Stand-alone-Software kann heute auch über Internetverbindungen, APIs oder Cloud-Dienste mit verschiedensten Geräten interagieren und dabei in Echtzeit sicherheitsrelevante Risiken auslösen, ohne physisch integriert zu sein.[105] Die konventionelle Unterscheidung verfehlt daher die Realität moderner IT-Architekturen wie Cloud-Computing und Software-as-a-Service (SaaS), da sicherheitsrelevante Auswirkungen auch ohne physische Kopplung mit dem bzw. «Integration» im Endgerät entstehen können.[106]

III. Risiken

35 Durch den Einsatz von Software und KI-Systemen können neue Risiken für die Sicherheit und Gesundheit von Konsumenten entstehen oder bestehende Risiken können in veränderter Weise auftreten.[107] Nachfolgend werden die Risiken für die körperliche Integrität, die sich aus der Nutzung von Software- und KI-Produkten ergeben können, dargestellt.

101 Ähnlich zum PrHG KOCH/PICHONNAZ, S. 638, m.w.H.; ähnlich mit Bezug auf das deutsche Produkthaftungsgesetz REUSCH, Mobile Updates, S. 906, m.w.H.

102 S. u., Rn. 79 f.

103 Siehe auch BEURSKENS, in: Bomhard et al., § 16 Rn. 151, welcher festhält: «bei Smart Home Geräten ist es eine reine Designfrage, welche Funktionen lokal und welche auf einem entfernten System serverseitig durchgeführt werden».

104 PIOVANO/SCHUCHT/WIEBE, S. 85.

105 PIOVANO/SCHUCHT/WIEBE, S. 85.

106 Siehe auch DAMIAN, in: Praxishandbuch Produktregulierung, § 19 Rn. 2347, der feststellt, dass SaaS immer verbreiteter wird und das PrHG Software zunehmend nicht mehr erfassen würde, wenn Stand-alone-Software kein Produkt wäre.

107 Europäische Kommission, Weissbuch KI, S. 17; ErwG 25 GPSR; siehe auch OECD, Consumer, S. 6.

1. Ursache 1: Dynamisches Verhalten und Veränderlichkeit

Die Europäische Kommission hielt im Weissbuch zur Künstlichen Intelligenz im Jahr 2020 fest, dass in Produkte eingebundene Software, «einschliesslich KI», «die Funktionsweise dieser Produkte und Systeme im weiteren Verlauf ihres Lebenszyklus verändern» kann. Explizit werden Systeme genannt, die auf maschinellem Lernen beruhen oder häufige Softwareupdates erfordern. Dies führe zu neuen Risiken, die beim Inverkehrbringen dieser Produkte und Systeme noch nicht bestanden.[108] Es handelt sich bei der Veränderlichkeit nach Inverkehrbringung des Produktes durch neue Daten, die entweder vom Hersteller, von Umwelteinflüssen (z.B. Sensoren) oder von Dritten stammen, um einen relevanten Unterschied für die Sicherheit von Produkten im Vergleich zu nicht technisch veränderbaren Produkten.[109] 36

1.1. Veränderungsmöglichkeiten

Weil smarte Produkte normalerweise mit dem Internet verbunden sind oder Daten aus der Umgebung beziehen können, können sie sich nach Inverkehrbringung verändern.[110] Erstens können sich lernfähige Systeme – je nach Konfiguration – stetig weiterentwickeln.[111] Zweitens haben Hersteller i.d.R. die Möglichkeit, auf durch das Internet[112] verbundene Systeme auch nach deren Inverkehrbringung Einfluss zu nehmen.[113] Drittens können u.U. auch Dritte auf KI-Produkte Einfluss nehmen.[114] Diese drei Veränderungsmöglichkeiten können auch nebeneinander für das gleiche KI-Produkt gelten. 37

108 Europäische Kommission, Weissbuch KI, S. 16; siehe auch Lohsse/Schulze/Staudenmayer, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 22.

109 Alle Produkte verändern sich mit der Zeit auf sicherheitsrelevante Weise. Bspw. können Lebensmittel verderben, Metalle korrodieren oder Kunststoffe verspröden.

110 Dies kann lokal auf dem Gerät geschehen oder über ein externes System mittels Verbindung via Internet.

111 S. u., Rn. 38, Veränderungsmöglichkeit 1.

112 Denkbar sind auch andere Methoden, s. u., Rn. 84.

113 S. u., Rn. 39, Veränderungsmöglichkeit 2.

114 S. u., Rn. 40, Veränderungsmöglichkeit 3.

a. Veränderungsmöglichkeit 1: selbstständiges Lernen des KI-Systems

38 Je nachdem, wie ein Hersteller sein Produkt konfiguriert, kann das integrierte KI-System selbstständig weiterlernen bzw. sich weiterentwickeln.[115] Die Lernfähigkeit selbst ist nicht per se ein Problem, sondern ein Risiko[116], das eingeschränkt werden kann (sog. «Safety by Design»). So können einem System bspw. Werte vorgegeben werden, die es nicht unter- oder überschreiten darf (z.B. wie Leitplanken, innerhalb welcher es agieren darf). Was für einen Nutzer aber gefährliche Resultate (z.B. eine Raumtemperatur einer Wohnung unter 18 Grad für ältere Personen) sind, sind für andere gewollte Resultate (z.B. 18 Grad, während einer Ferienabwesenheit). Das heisst, die Konfiguration von Grenzen ist nicht immer eine zielführende Lösung und hilft nicht, wenn sie zu grosszügig konfiguriert werden. Ausserdem können KI-Systeme Dinge lernen, die nicht gewollt sind. So empfahl Googles KI-System Gemini bspw. Pizzabelag mit Leim auf eine Pizza zu kleben, damit er gut hält.[117] Die Risiken, die mit dem Einsatz von KI-Systemen einhergehen, können von jenen traditioneller Software abweichen oder die bestehenden Risiken verschärfen.[118]

b. Veränderungsmöglichkeit 2: Softwareupdates des Herstellers

39 Software kann nach der Inverkehrbringung mittels «Updates» verändert werden. Updates können Funktionen hinzufügen oder entfernen. Auch die Veränderung via Updates ist kein eigenständiges Risiko, da sie vom Hersteller kontrollierbar ist.[119]

c. Veränderungsmöglichkeit 3: Einwirkung durch Dritte

40 Zudem können Nutzer durch die Eingabe eigener Daten, die selbstständige Beeinflussung der Software oder mechanische Veränderungen Einfluss auf Software- und KI-Produkte nehmen.[120] Hersteller haben jedoch die Möglichkeit, Veränderungen durch Dritte ein Stück weit einzuschränken, indem sie

---

115 S. u., Rn. 92.

116 ZECH, Gutachten, A 67.

117 Google's AI Recommended Adding Glue To Pizza And Other Misinformation – What Caused The Viral Blunders?, abrufbar unter <https://www.forbes.com/sites/jackkelly/2024/05/31/google-ai-glue-to-pizza-viral-blunders/>, zuletzt besucht am 31.05.2025.

118 ARIOLI, Jusletter IT 04.07.2024, Rn. 2.

119 S. u., Teil 2:A.I.2.1.c.

120 WAGNER, Rauch, S. 127 f.

bspw. technische Schutzmechanismen implementieren oder den Zugriff auf bestimmte Funktionen eingrenzen.[121]

Während es sich bei der Veränderung aus dem System selbst (selbstständiges Weiterlernen) und Updates vom Hersteller um gewollte Veränderungen handelt, besteht das Risiko, dass auch böswillige Dritte auf Software- und KI-Produkte Einfluss nehmen. Unsichere Konfigurationen von Produkten mit einer Verbindung zum Internet können von aussen «angegriffen» («gehackt») werden.[122] Die fremde «Übernahme» kann bspw. dazu genutzt werden, dass die Software oder das KI-System ungewollte Resultate erzielt, anzeigt oder ausführt. So kann schädliche Software bspw. Geräte überhitzen und explodieren lassen.[123] Bei KI-Systemen kommen zusätzlich spezifische Angriffsformen (z.B. sog. «Adversarial Attacks») hinzu.[124] Dabei werden Eingabedaten gezielt so manipuliert, dass das System falsche Entscheidungen trifft, ohne dass der Angriff für Menschen erkennbar wäre. IT-Sicherheitsmassnahmen sind ein integraler Bestandteil der Produktsicherheit.[125] Dies gilt sowohl auf technischer Ebene als auch in Bezug auf die Robustheit des KI-Modells gegenüber gezielten Täuschungsversuchen. Da die Cybersicherheit für sich allein ein sehr umfangreiches Gebiet ist, das eigenständig erforscht wird und oft andere Fragestellungen und Regulierungen betrifft (z.B. Datenschutz, Netzwerkarchitekturen, kryptografische Methoden), soll dies vorliegend nicht genauer behandelt werden.[126] 41

121 Z.B. verhindert OpenAI Antworten von ChatGPT zur Erstellung von Waffen. Mittels spezifischer Eingaben (sog. «Jailbreaks») können diese Restriktionen jedoch umgangen werden, weshalb sie laufend angepasst werden müssen. More ChatGPT Jailbreaks Are Evading Safeguards On Sensitive Topics, abrufbar unter <https://www.forbes.com/sites/alexvakulov/2025/02/01/more-chatgpt-jailbreaks-are-evading-safeguards-on-sensitive-topics/>, zuletzt besucht am 31.05.2025.

122 Siehe auch ErwG 25 GPSR.

123 Android malware posing as porn can literally make your phone's battery explode, abrufbar unter <https://www.ibtimes.co.uk/android-malware-posing-porn-can-literally-make-your-phones-battery-explode-1652008>, zuletzt besucht am 31.05.2025; How does a smartphone battery explode and how you can prevent it, abrufbar unter <https://www.business-standard.com/article/technology/what-leads-phones-batteries-to-explode-here-s-how-you-can-prevent-it-122091400621_1.html>, zuletzt besucht am 31.05.2025; A Hacker Speaks: How Malware Might Blow Up Your Laptop, abrufbar unter <https://www.pcworld.com/article/481440/batteries_go_boom.html>, zuletzt besucht am 31.05.2025.

124 Siehe auch Art. 15 Abs. 5 Uabs. 3 KI-VO.

125 S. u., Rn. 265.

126 S. o., Rn. 20.

1.2. Beispiele zur Veränderlichkeit

42 KI kann auf verschiedene Weisen «angelernt» werden. Beim Batch-Learning[127] wird das KI-Modell nach dem Training finalisiert und nach dem Inverkehrbringen nicht mehr laufend aktualisiert. Beim Online-Learning[128] lernt ein KI-Modell kontinuierlich weiter.

a. Beispiel A: Veränderungsmöglichkeiten 1 und 2

43 Hersteller können ihre KI-Produkte so konfigurieren, dass diese mit Daten, die der Nutzer des Produktes durch ebendiese Nutzung zur Verfügung stellt (z.B. mittels Batch-Learning), trainiert werden.[129] Der Hersteller kann diese vor dem Training des Produktes sichten, aufbereiten und wenn nötig «schlechte» Daten aussortieren. Das KI-Modell wird dann mit den bereinigten Nutzerdaten trainiert und die Resultate des KI-Systems damit verändert. Ist das Modell fertig trainiert, kann der Hersteller dem Nutzer ein Update mit den Neuerungen zur Verfügung stellen.

44 Ein Hersteller kann somit ein KI-gesteuertes Smart Home Device zur Heizungssteuerung (z.B. einen smarten Thermostat) anbieten, welches Nutzerdaten wie Heizpräferenzen und Raumaufenthalte sammelt, bereinigt und zur Verbesserung des Modells verwendet. Fehlerhafte Daten (z.B. fehlerhafte Sensorwerte) können jedoch falsche Annahmen im Modell verursachen, etwa dass ein oft genutzter Raum selten verwendet wird. Dies könnte nach einem Update dazu führen, dass die Heizung in wichtigen Räumen wie Schlafzimmern bei niedrigen Temperaturen deaktiviert wird, was gesundheitliche Risiken für vulnerable Personen birgt. Dieses Beispiel zeigt auf, dass sich KI-Produkte durch die Möglichkeit des selbstständigen Lernens des Systems sowie durch Softwareupdates des Herstellers verändern können.

b. Beispiel B: Veränderungsmöglichkeiten 1 und 3

45 KI-Systeme können sich nach ihrer Inverkehrbringung auch ohne weiteren Einfluss des Herstellers (also unabhängig von einem Update) verändern. Bspw. können KI-Systeme so konfiguriert sein, dass sie kontinuierlich mit den Daten

127 S. u., Rn. 97.

128 S. u., Rn. 98.

129 Das Verwenden von produktspezifischen Daten ist aus Sicht des Herstellers i.d.R. sinnvoller, als wenn er Daten z.B. einkauft oder selbst generiert (synthetische Daten). Erstens kommt der Hersteller durch seine Nutzer an eine grosse Menge kostenloser Trainingsdaten und zweitens sind diese direkt auf sein spezifisches Produkt bezogen.

von Nutzern oder Betreibern weitertrainiert werden. Daten des Nutzers eines Produktes können bspw. mit seinem spezifischen Profil verbunden werden und ein KI-System kann damit kontinuierlich lernen und sich an die Bedürfnisse des Nutzers anpassen.

So kann ein Saugroboter durch kontinuierliches Training lernen, dass in seiner eingesetzten Umgebung üblicherweise kleine Hindernisse auf dem Boden liegen, wie Spielzeug oder Kleidung. Der Saugroboter «lernt», dass diese Hindernisse sehr nahe umfahren werden können, um effizient zu reinigen. Wenn ein Kind auf dem Boden sitzt und spielt, könnte der Roboter es fälschlicherweise als solches Hindernis einstufen. Er könnte dann zu nah an das Kind heranfahren und dabei dessen Hand oder Fuss erfassen, was zu Verletzungen des Kindes durch rotierende Bürsten oder mechanische Teile führen kann. Dieses Beispiel zeigt auf, dass sich KI-Produkte durch die Möglichkeit des selbstständigen Lernens des Systems sowie durch Einwirkungen Dritter verändern können. 46

2. Ursache 2: Opazität

Die Opazität, also die fehlende Transparenz von KI-Systemen, kann aus zwei Gründen Gefahren verursachen: Erstens kann die technische Komplexität KI zu einer «Black Box»[130] machen, deren Entscheidungen selbst für Experten oft nicht vollständig nachvollziehbar sind.[131] Dies kann zu unvorhersehbarem Verhalten führen, wie falschen Reaktionen in kritischen Situationen, und erschwert die schnelle Fehlerbehebung. Zweitens schaffen Hersteller bewusst zusätzliche Opazität, etwa zum Schutz von Geschäftsgeheimnissen.[132] Zudem erschweren es intransparente Systeme Dritten (z.B. Nutzern, Behörden oder Gutachtern), Fehler nachzuverfolgen oder den Hersteller direkt zur Verantwortung zu ziehen.[133] Diese «strategische Opazität» verhindert, dass Konsumenten und Dritte die Funktionsweise der KI oder potenzielle Risiken verstehen und überwachen können.[134] Die Kombination dieser beiden Faktoren macht es schwer, gefährliches Verhalten zu erkennen und rechtzeitig einzugreifen. 47

130 Thouvenin et al., Jusletter IT 04.07.2024, Rn. 40, m.w.H.; Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 31; siehe auch Wagner, Verantwortlichkeit, S. 720.

131 Martini, Blackbox, S. 44.

132 Martini, Blackbox, S. 33; siehe auch Wischmeyer, in: Wischmeyer/Rademacher, Rn. 46.

133 Martini, Blackbox, S. 27 f.

134 Ähnlich, Reusch, Mobile Updates, S. 908.

48 Technische und strategische Opazität sind nicht nur bei KI-Systemen, sondern auch bei Produkten mit Software ohne KI relevant.[135] Auch bei herkömmlicher Software kann die technische Komplexität dazu führen, dass Fehler oder unvorhergesehene Wechselwirkungen mit vernetzten Produkten schwer nachvollziehbar sind. Die Wechselwirkung zwischen Gegenständen, «die an andere Gegenstände angeschlossen werden, oder nicht eingebettete Gegenstände, die beeinflussen, wie ein anderer Gegenstand funktioniert»[136] ist als Sicherheitsrisiko anerkannt.[137] Strategische Opazität durch den Hersteller, etwa durch Zurückhalten von Informationen über Schwachstellen oder Updates, ist bei herkömmlicher Software ebenfalls möglich.

49 Der entscheidende Unterschied zu KI-Systemen liegt jedoch in deren dynamischer Verhaltensweise, während klassische Software nach ihrer Programmierung statisch bleibt und festgelegte Funktionen ausführt. Dadurch sind Risiken bei KI-Systemen oft schwerer zu erkennen und zu beherrschen, auch wenn mangelnde Transparenz bei traditioneller Software ebenfalls ernsthafte Probleme verursachen kann.

3. Risiko 1: Fehlende Vorhersehbarkeit durch Veränderlichkeit und Opazität

50 Die Veränderlichkeit und Opazität von Software und KI-Systemen in Produkten führt zur fehlenden Vorhersehbarkeit des Verhaltens dieses Produktes.

51 Die technische Opazität von KI-Systemen entsteht aus ihrer hochkomplexen Struktur, insbesondere bei Modellen wie Deep Learning.[138] Diese Algorithmen verarbeiten Daten auf eine Weise, die für Menschen schwer nachvollziehbar ist,[139] sodass Entscheidungen und Verhaltensänderungen oft nicht erklärt werden können.[140] Dies macht es bei gefährlichen Produkten schwierig zu eruieren, wo genau die Ursache eines Problems liegt.[141] Datenverzerrungen oder unerwartete Reaktionen auf seltene Szenarien verstärken diese Unvorherseh-

135 Siehe auch MARTINI, Blackbox, S. 285 f.
136 ErwG 24 GPSR.
137 Siehe auch BVGer A-727/2016 vom 13.07.2016, E. 5.2.1 darauf hinweisend, dass das Prüfen einzelner Komponenten nicht ausreicht, sondern diese aufeinander abgestimmt sein müssen.
138 MARTINI, Blackbox, S. 42 f.
139 MARTINI, Blackbox, S. 19.
140 MARTINI, Blackbox, S. 43.
141 HESS, Haftungsverschärfung, S. 28.

barkeit und machen es für den Hersteller schwierig, Risiken frühzeitig zu erkennen.

Die strategische Opazität verhindert, dass Nutzer und andere Dritte die Entscheidungsprozesse oder Grenzen des KI-Systems verstehen können. Dadurch bleibt für sie unklar, wie sich das System in ungewöhnlichen Situationen verhält oder ob systematische Fehler vorliegen, was die Einschätzung (und Beherrschung[142]) potenzieller Risiken erschwert. Nutzer sind dadurch nicht in der Lage, fundierte Entscheidungen darüber zu treffen, wie das Produkt sachgerecht und sicher eingesetzt werden kann. 52

Da es sein kann, dass sich ein KI-Produkt nach der Inverkehrbringung verändert, ist es sehr schwierig, ein Produkt von Anfang an ausreichend sicher herzustellen.[143] Gerade bei selbstlernenden KI-Systemen (aber auch generell bei Software) können die Resultate des Systems schwierig erkennbar und vorhersehbar sein.[144] Nachmarktpflichten sind in diesem Bereich besonders wichtig, um sicherheitsrelevante Veränderungen rechtzeitig zu erkennen und darauf reagieren zu können.[145] 53

4. Risiko 2: Kontrollverlust durch Veränderlichkeit und Opazität

Durch die Möglichkeit der Veränderung eines KI-Systems und die resultierenden unvorhergesehenen Verhaltensweisen wird es dem Hersteller erschwert, die Funktionalität und Sicherheit seiner Produkte über deren gesamten Lebenszyklus zu beherrschen.[146] Hinzu kommt: Je mehr Einflussmöglichkeiten der Hersteller durch Dritte auf ein Produkt zulässt, desto geringer ist seine eigene Kontrolle über das Produkt und desto schwieriger wird es für ihn, dessen Verhalten vorherzusehen.[147] Dies gilt insbesondere, wenn das Produkt mit der Fähigkeit ausgestattet ist, sich durch kontinuierliches Lernen eigenständig 54

142 S. u., Rn. 54.

143 Straub vertritt, dass Software gar nicht ohne Fehler entwickelt werden könne, Straub, Produktehaftung, Rn. 3; ähnlich Honsell/Isenring/Kessler, § 21 Rn. 31; siehe auch Roberto, 09.16, welcher an die Sicherheit von für Menschen gefährlicher Software richtigerweise die gleichen Erwartungen stellt wie an andere Produkte.

144 S. u., Rn. 264.

145 Siehe auch Zech, Gutachten, A 67.

146 In Bezug auf autonome Systeme Wagner, Verantwortlichkeit, S. 726; siehe auch Zech, Gutachten, A 51.

147 Siehe auch Zech, Gutachten, A 71, der zwischen dem Training durch den Nutzer und dem Training durch den Hersteller unterscheidet.

weiterzuentwickeln.[148] Der Hersteller kann durch die selbstständige Veränderung des KI-Systems die Kontrolle darüber verlieren.[149] Das Weiterlernen kann zu unvorhersehbarem Verhalten wie etwa unerwarteten Wechselwirkungen mit anderen Systemen und Fehlfunktionen des Systems führen.[150] Noch schwieriger wird es für den Hersteller, wenn die Trainingsdaten des Systems nicht von ihm selbst kommen. Wenn andere Dritte, z.B. Teilhersteller oder Betreiber, das Produkt mit ihren Daten trainieren, hat der Hersteller weniger Kontrolle darüber.[151] Dennoch ist der Hersteller jene Person, die das «Verhalten» von Systemen, mit denen er weiterhin verbunden ist, am ehesten steuern kann, selbst wenn sich das Produkt physisch beim Nutzer befindet.[152]

55 Wie in den technischen Grundlagen dargelegt werden wird, werden KI-Systeme auf verschiedene Arten trainiert.[153] Die Batch-Learning-Methode, bei welcher das KI-System «eingefroren» wird, ist für den Hersteller viel einfacher kontrollierbar,[154] da er das fertig trainierte Modell zuerst ausgiebig testen kann, bevor er es in Verkehr bringt. Es ist dafür aber weniger flexibel und damit bspw. weniger aktuell als die Online-Learning-Methode. Beeinflusst der Hersteller, mit welchen Daten er das Modell bei der Online-Learning-Methode weitertrainiert, ist eine ständige Verbindung des Systems zum Hersteller nötig. Es handelt sich in dem Sinne um ständige Updates, da das System kontinuierlich verändert wird. Auch wenn der Hersteller das System so nicht unter Berücksichtigung der neusten Trainingsdaten testen kann, bevor er es in Verkehr bringt, kann er immerhin selbst bestimmen, welche Daten er für das Training verwendet.[155]

56 Im oben beschriebenen Kapitel «Beispiel A: Veränderungsmöglichkeiten 1 und 2» hat der Hersteller die grössere Kontrolle über sein System, da er dieses vor

148 Siehe auch McGuire, in: Foerste/Westphalen, § 58 Rn. 26, welche der Meinung ist, dass eingefrorene Systeme sich «hinsichtlich Prognose und Erklärbarkeit der [...] Ergebnisse nicht von einer regelbasierten Software» unterscheiden würden. Dies ergibt Sinn bezogen auf das von ihr gewählte Beispiel (Entwicklung einer Gussform), jedoch kann dieser Meinung nicht generell gefolgt werden, da insbesondere Resultate generativer KI auch als eingefrorene Systeme schwierig vorherzusehen und zu erklären sind.

149 Zech, Gutachten, A 51.

150 Martini, Blackbox, S. 131.

151 McGuire, in: Foerste/Westphalen, § 58 Rn. 27; Etzkorn, S. 364 f.; siehe auch Zech, Gutachten, A 51, 89.

152 Etzkorn, S. 365; ähnlich Wagner, Verantwortlichkeit, S. 734.

153 Zum Batch- und Online-Learning siehe Rn. 96 f.

154 Wildhaber, Einführung, S. 47, m.w.H.

155 Im Gegensatz dazu, wenn die Trainingsdaten direkt vom Nutzer oder aus anderen Quellen kommen, s. u., Rn. 99.

dem Update testen kann. Im Kapitel «Beispiel B: Veränderungsmöglichkeiten 1 und 3» hat er deutlich weniger Kontrolle, da er nicht weiss, welche Inputs der Nutzer dem System rückmelden wird. Der Hersteller kann nicht ausschliessen, dass die KI etwas lernt, was er nicht vorausgesehen und so nicht gewollt hat.[156]

Bei Softwareprodukten zeichnet sich eine Verlagerung der Nutzer- hin zur Herstellerkontrolle ab.[157] Für den Konsumenten ist die fehlende Kontrolle über ein Produkt ein sicherheitsrelevantes Problem. Durch die obengenannte Veränderlichkeit und Opazität hat er wenig Wissen über die Vorgänge im System[158] und kann Risiken deshalb nur schwer rechtzeitig erkennen und sich dagegen schützen. Ebenfalls problematisch ist, dass sich Konsumenten auf KI-Systeme verlassen, obwohl sie aufgrund der Opazität nicht genau wissen, wie sie funktionieren. 57

IV. Vorteile

An dieser Stelle ist anzumerken, dass neben den erwähnten Risiken durch die Möglichkeit der Veränderung eines Software- oder KI-Produktes auch Vorteile in Bezug auf die Produktsicherheit[159] entstehen. Vorteilhaft ist u.a., dass KI-Modelle mit mehr Training genauer oder besser werden können. Geräte, die zuerst ohne KI unsicher waren, können mit KI sicherer gemacht werden.[160] So könnte im obengenannten Beispiel des Staubsaugerroboters, der die Rute des Hundes eingesaugt hat, eine Bilderkennung eingebaut werden. Die Bilderkennung könnte dazu beitragen, dass Haustiere erkannt und umfahren werden. 58

Der Vorteil gegenüber Produkten, die nach deren Inverkehrbringung nicht mehr im Einflussbereich des Herstellers stehen, ist, dass der Hersteller Probleme erkennen und z.B. in Form von Softwareupdates auf Gefahren reagieren kann.[161] Dies gilt auch für KI-Systeme.[162] Technische Voraussetzung für eine 59

156 S. u., Rn. 38.

157 Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157; Wagner, Verantwortlichkeit, S. 734; Zech, Gutachten, A 88-89.

158 Siehe auch Wagner, Rauch, S. 127, der festhält, dass es «gerade ein Kennzeichen digitaler Produkte» sei, «dass der Nutzer bei ihrem Betrieb von relevanten Entscheidungen und Einflussnahmen weitgehend ausgeschlossen» bleibe.

159 OECD, Consumer, S. 6.

160 Wagner, Verantwortlichkeit, S. 727.

161 Koch/Pichonnaz, S. 630; siehe auch Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.

162 Spindler, Vorschläge, Rn. 21.

mögliche Veränderung nach Inverkehrbringung ist, dass der Hersteller weiterhin eine Verbindung zu seinem Produkt aufbauen kann.[163] Der Hersteller kann seine IT-Produkte bspw. so konfigurieren, dass er sie kontinuierlich überwachen und darauf zugreifen kann.[164] So können Produkte vom Hersteller aus der Ferne verbessert und müssen deshalb seltener zurückgerufen werden.[165] Es können bspw. Funktionen hinzugefügt oder entfernt sowie Sicherheitslücken geschlossen werden. Mitunter können Hersteller sogar dazu verpflichtet sein, Updates zur Verfügung zu stellen.[166] Grundsätzlich hat der Hersteller deshalb – im Vergleich zum Nutzer und im Gegensatz zu herkömmlichen Produkten – mehr Kontrolle bei einem Softwareprodukt.[167] Für den Grad der Kontrolle von KI-Produkten kommt es auf die Art des Modells, die Menge und Qualität der verwendeten Trainingsdaten, die Nachvollziehbarkeit der Entscheidungsprozesse sowie die Fähigkeit des Herstellers an, die laufende Überwachung und Anpassung des Systems sicherzustellen.

V. Fazit

60 Die technischen Entwicklungen und die zunehmende Integration von Software und KI in Konsumentenprodukte stellen neue Herausforderungen für das Produktsicherheitsrecht dar. Die oben beschriebenen Entwicklungen führen dazu, dass Konsumenten vermehrt mit Produkten interagieren, die – mehr oder weniger – neue Gefahren bergen.[168] Neue Gefahren für Konsumenten ergeben sich vor allem aus der Opazität und der Veränderlichkeit des Produktes u.a. durch seine Verbindung mit der Software sowie dem Internet. Bei der Softwarekomponente oder der eigenständigen Software kann es sich auch um KI handeln, welche – aus produktsicherheitsrechtlicher Sicht – die Gefahren von Softwareprodukten durch zusätzliche Opazität und ihre dynamische Verhaltensweise verstärkt. Ein weiteres Risiko ist die Einflussnahme durch Dritte bzw. der (teilweise) Verlust der Kontrolle des Herstellers über seine Produkte.

61 Weder die Veränderlichkeit noch die fehlende Transparenz der Funktionsweise von Produkten sind an sich neue Phänomene. Auch Produkte ohne Software und KI können sich nach der Inverkehrbringung verändern. So können Lebensmittel verderben oder Materialien können mit der Zeit abgenutzt wer-

163 S. u., Rn. 84, 354.
164 S. u., Rn. 362.
165 Europäische Kommission, CASP 2020, S. 15.
166 Zumindest als eine Option aufgeführt: Art. 37 Abs. 3 GPSR.
167 Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.
168 Siehe auch ErwG 25 GPSR.

den oder korrodieren. Schon lange sind gewisse technische Vorgänge von Geschäftsgeheimnissen geschützt und Hersteller informieren nicht immer transparent über die Grenzen ihrer Produkte. Diese Phänomene werden durch den Einsatz von KI jedoch verstärkt, weil KI-Systeme sich auch nach der Inverkehrbringung «eigenständig» verändern können. Zudem erschweren die Komplexität und mangelnde Erklärbarkeit vieler KI-Modelle die Vorhersehbarkeit des Verhaltens der KI-Produkte für Hersteller und Nutzer. Die Möglichkeit der Veränderlichkeit von Software- und KI-Produkten ist aber vorhersehbar, da sie auf Updates, Algorithmen oder Lernprozessen beruhen, die vom Hersteller implementiert werden.[169]

Auch der Kontrollverlust des Herstellers ist nur in Bezug auf die Lernfähigkeit der KI neu. Bei herkömmlichen Produkten ohne bestehende Verbindung zum Hersteller gibt dieser mit Inverkehrbringung des Produktes die Kontrolle darüber ganz auf. Die neue Herausforderung liegt deshalb bei Softwareprodukten in der Kombination der genannten Risiken. Bei KI-Produkten im Besonderen liegt die neue Herausforderung vor allem in der Lernfähigkeit und Autonomie sowie der damit verbundenen Opazität. 62

Die Europäische Kommission hielt 2020 fest, dass sich die (damals) bestehenden Rechtsvorschriften hauptsächlich auf Sicherheitsrisiken zum Zeitpunkt des Inverkehrbringens konzentrieren würden und Risiken, die sich durch die Veränderung von Produkten und Systemen während ihres Lebenszyklus ergeben, nicht angemessen berücksichtigt seien.[170] Durch das ungewisse Risiko aufgrund der Veränderlichkeit und Komplexität von Software- und KI-Produkten gewinnen Nachmarktpflichten an Bedeutung.[171] Insbesondere die Produktbeobachtung wird umso relevanter, damit gefährliche Veränderungen rechtzeitig erkannt werden können.[172] 63

169 Ähnlich mit Bezug auf den Entwurf der PLD 2024 Spindler, Vorschläge, Rn. 20; ebenso Wildhaber, Einführung, S. 47, m.w.H.; a.A. Hänsenberger, Drohnen, S. 125.

170 Europäische Kommission, Weissbuch KI, S. 16.

171 Siehe auch bereits Röthlisberger, S. 45, der sich aufgrund des ungewissen «Gefahrenrisikos» neuer Produkte für eine erhöhte Beobachtungspflicht aussprach, sofern daraus eine Verletzung von Rechtsgütern resultieren kann.

172 Zech, Gutachten, A 72-73.

E. Einbettung ins europäische System mit Auswirkung auf Gesellschaft und Wirtschaft

64 Das moderne schweizerische Produktsicherheitsrecht hat seinen Ursprung im europäischen Produktsicherheitsrecht. Die verschiedenen Erlasse, welche die Produktsicherheit regeln, sind in ein europäisches System von verschiedenen Rechtsvorschriften eingebettet. Dieses System besteht aus der «neuen Konzeption», dem «Gesamtkonzept zur Konformitätsbewertung» und dem «neuen Rechtsrahmen». Art. 4 Abs. 2 THG hält fest, dass die technischen Vorschriften auf die wichtigsten Handelspartner der Schweiz abgestimmt werden. Dazu gehört die EU.[173] Deshalb haben die EU-Regelungen einen sehr grossen Einfluss auf das Schweizer Produktsicherheitsrecht und eine Abweichung der Schweizer Regelungen zu den Regelungen der EU stellt ein Marktzugangshindernis dar. Im Rahmen der Bilateralen I haben die Schweiz und die EU u.a. ein Abkommen über die gegenseitige Anerkennung von Konformitätsbewertungen (Mutual Recognition Agreement, MRA[174]) abgeschlossen.[175] Dieses dient dem Abbau von technischen Handelshemmnissen zwischen der EU und der Schweiz[176] und trat 2002 in Kraft.[177] Es umfasst 20 verschiedene Produktsektoren und regelt 64 % aller Importe aus der EU und 72 % aller Exporte in die EU.[178] Aufgrund des MRA ist es teilweise nötig, dass die Schweiz produktsi-

---

173 Zur Angleichung an die EU siehe auch SHK PrSG-Hess, Einleitung, Rn. 85.

174 Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die gegenseitige Anerkennung von Konformitätsbewertungen (Mutual Recognition Agreement) in Kraft getreten am 01.06.2002, SR 0.946.526.81 (zit. MRA).

175 Die Schweiz hat noch weitere MRAs abgeschlossen, z.B. mit Kanada und den USA, siehe Staatsvertragliche Vereinbarungen (Mutual Recognition Agreements – MRA), abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0.html>, zuletzt besucht am 31.05.2025.

176 BGE 143 II 518, 526 E. 5.4.2.

177 BJ, Rechtliche Basisanalyse KI, S. 125; ausführlich zum MRA: Pfenninger, S. 1161 ff.; SHK PrSG-Hess, Einleitung N 86 und Art. 3 N 21; siehe auch MRA Schweiz – EU, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0/MRA_Schweiz_EU.html>, zuletzt besucht am 31.05.2025.

178 Mit Verweis auf die Handelsstatistik BAKOM, Überblick Sektorregulierung KI, S. 35; siehe dazu SECO, Handelsstatistik MRA; siehe auch Europäische Kommission, Blue Guide, S. 130.

cherheitsrechtliche Regelungen der EU autonom nachvollzieht,[179] damit die technischen Vorschriften weiterhin als gleichwertig beurteilt werden.[180] Diese gegenseitige Anerkennung verhindert vor allem, dass eine doppelte Konformitätsbewertung in der Schweiz und der EU nötig ist.[181] Da die Nachmarktpflichten unabhängig von allenfalls nötigen Konformitätsbewertungen zu erfüllen sind, betrifft das MRA die Nachmarktpflichten nicht direkt. Weil im MRA jedoch zwölf Produktsektoren geregelt werden, die von den Regeln der KI-VO betroffen sind, wird vom BAKOM empfohlen, die schweizerischen Vorschriften für diese Sektoren an die KI-VO anzupassen und das MRA zu erweitern.[182] Diese künftigen Anpassungen könnten auch die Nachmarktpflichten betreffen. Die EU verweigerte 2019 neue Verhandlungen zum MRA.[183] Zwischenzeitlich wurden diese jedoch wieder aufgenommen.[184]

Ab 1985 wurde in der damaligen Europäischen Wirtschaftsgemeinschaft der «New Approach» (deutsch: «neue Konzeption») eingeführt.[185] An die Stelle von detaillierten produktbezogenen Harmonisierungsvorschriften rückten sektorale Richtlinien, die Produktgruppen oder spezifische Gefahren harmonisieren sollten.[186] Ziel war es, durch «einheitliche Anforderungen an Produkte», die europäische Warenverkehrsfreiheit sowie die Herstellung von innovativen Produkten zu fördern.[187] Der New Approach legte die produktsicherheitsrechtlichen «grundlegenden Sicherheitsanforderungen» fest und lagerte deren Konkretisierung an europäische Normenorganisationen (heute CEN, Cenelec und ETSI[188]) aus.[189] Es handelt sich dann um harmonisierte europäische 65

179 Diebold/Rütsche, Rn. 528; Bühler, Sicherheit, Rn. 5.

180 BJ, Rechtliche Basisanalyse KI, S. 125 f.; siehe auch Europäische Kommission, Blue Guide, S. 130.

181 BAKOM, Überblick Sektorregulierung KI, S. 35; BJ, Rechtliche Basisanalyse KI, S. 125.

182 BAKOM, Überblick Sektorregulierung KI, S. 35 f. auf Basis von BJ, Rechtliche Basisanalyse KI, S. 127 f.

183 Diebold/Rütsche, Rn. 529.

184 Aktuelle Informationen zu den Verhandlungen finden sich auf der Website des EDA, abrufbar unter <https://www.eda.admin.ch/eda/de/home/das-eda/aktuell/newsuebersicht/2023/europa.html>, zuletzt besucht am 31.05.2025.

185 Schucht, New Approach, S. 46; Bühler, Sicherheit, Rn. 2; SHK PrSG-Hess, Art. 4 N 15 ff.

186 Schucht, New Approach, S. 46; Kapoor/Klindt, S. 650, m.w.H.

187 Piovano, Hersteller, S. 4; Schucht, New Approach, S. 46.

188 Europäische Kommission, Blue Guide, S. 129; Klindt, S. 4; SHK PrSG-Hess, Einleitung N 41 Fn. 142.

189 Schucht, New Approach, S. 46; SHK PrSG-Hess, Art. 4 N 17; dies ist in der Schweiz in Art. 6 Abs. 4 PrSG geregelt.

technische Normen.[190] Nach der Erarbeitung der technischen Details werden die Normen noch in nationale Normen umgesetzt.[191] Auch wenn diese Normen nicht zwingend befolgt werden müssen, löst die Herstellung danach eine Konformitätsvermutung aus.[192] Das heisst, wenn ein Produkt die anwendbaren Normen erfüllt, wird (widerlegbar) vermutet, dass dieses sicher ist.[193] Hält ein Hersteller die Normen nicht ein, kann er die Einhaltung der Sicherheitsanforderungen anderweitig beweisen.[194] Genehmigungsverfahren vor der Inverkehrbringung von Produkten wurden soweit möglich abgeschafft und Produkte werden seither weitgehend selbstverantwortlich in Verkehr gebracht.[195]

66 Ergänzend harmonisierte der «Global Approach» (deutsch: «Gesamtkonzept zur Konformitätsbewertung») durch einen Beschluss[196] die Konformitätsbewertung und führte Regeln für das CE-Kennzeichnen[197] ein.[198]

67 Das 2008 verabschiedete «New Legislative Framework» (NLF)[199] (deutsch: «neuer Rechtsrahmen») vereinte den New Approach und den Global Approach.[200] Das NLF hat das Ziel, das Produktsicherheitsrecht in der EU zu vereinheitlichen.[201] Mit dem NLF müssen alle Produkte, die auf dem EU-Markt in

190 Harmonisierte Normen sind europäische Normen, die «auf der Grundlage eines Mandats der EU-Kommission von den privatrechtlich organisierten europäischen Normenorganisationen [...] erlassen werden». Es handelt sich dabei lediglich um Empfehlungen, SHK PrSG-Hess, Art. 4 N 45 ff.

191 SHK PrSG-Hess, Art. 4 N 46; Kapoor/Klindt, S. 650.

192 Schucht, New Approach, S. 46 f.; SHK PrSG-Hess, Art. 4 N 17.

193 Schucht, New Approach, S. 47; SHK PrSG-Hess, Art. 4 N 17; siehe auch Art. 5 Abs. 2 PrSG.

194 SHK PrSG-Hess, Einleitung N 41.

195 Hess, in: Häner/Waldmann S. 220.

196 Beschluss des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE-Konformitätskennzeichnung, ABl. L 220/23 (zit. Global Approach). Dieser wurde mit dem NLF aufgehoben.

197 Dieses wird nur für den Export in den EWR verlangt und muss in der Schweiz nicht angebracht werden. Website des SECO zur CE-Kennzeichnung, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/Technische_Handelshemmnisse/Mutual_Recognition_Agreement_MRA0/CE-Kennzeichnung.html>, zuletzt besucht am 31.05.2025.

198 Siehe auch im Detail Piovano, Hersteller, S. 5, m.w.H.

199 Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates (New Legislative Framework), ABl. L 218/82 (zit. NLF).

200 Piovano, Hersteller, S. 6; Bühler, Sicherheit, Rn. 38; SHK PrSG-Hess, Art. 4 N 19; Kapoor/Klindt, S. 469.

201 Voigt/Hullen, S. 1.

Betrieb genommen oder bereitgestellt werden, «die Anforderungen aller anwendbaren Harmonisierungsrechtsvorschriften erfüllen».[202] Für ein Produkt können deshalb mehrere Verordnungen und Richtlinien, die die Produktsicherheit regeln, gleichzeitig gelten.[203] Mit dem NLF gewannen die öffentlichrechtlichen Produktbeobachtungspflichten in der EU an Bedeutung.[204] Auch die KI-VO gehört zum NLF.[205] Der 2022 aktualisierte Blue Guide der EU «fasst gemeinsame Prinzipien der EU-Rechtsakte innerhalb des» NLF zusammen[206] und geht spezifisch auf Software ein.[207] Der Blue Guide soll zu einer einheitlichen Anwendung der EU-Produktvorschriften im EU-Binnenmarkt führen.[208] Da es sich beim Blue Guide um eine Leitlinie handelt, ist er rechtlich nicht verbindlich und dient lediglich der Interpretation.[209]

Auch die Schweiz folgt bereits seit der Revision des STEG dem europäischen New Approach[210] und geht auch im PrSG «von der grundsätzlichen Selbstverantwortung aus».[211] Die Verantwortung zur Erfüllung der produktsicherheitsrechtlichen Pflichten liegt bei den Inverkehrbringern.[212] Deshalb sind auch die Überwachungs- und Meldepflichten in erster Linie Pflichten, die in der Eigenverantwortung der Hersteller (und der Importeure) stehen. 68

Die Mitgliedstaaten der EU (und die Schweiz[213]) erklären sog. «Marktüberwachungsbehörden» zuständig für den Vollzug des Produktsicherheitsrechts.[214] Sie haben ab der Inverkehrbringung eine Kontrollfunktion und können – wenn 69

202 Beck KI-VO-Hartmann, Art. 72 N 5.
203 Beck KI-VO-Hartmann, Art. 72 N 5.
204 Piovano/Schucht/Wiebe, S. 9 ff.
205 Beck KI-VO-Wendehorst, Art. 2 N 34; Beck KI-VO-Braun Binder/Egli, Art. 8 N 21; Wagner, Rauch, S. 128.
206 Voigt/Hullen, S. 2.
207 Europäische Kommission, Blue Guide, S. 18 f.
208 Zudem gilt der Blue Guide für die EWR-Staaten und je nach Fall für die Türkei und die Schweiz: Europäische Kommission, Blue Guide, S. 5.
209 NHK GPSR-Wiebe, Art. 8 N 15.
210 Botschaft PrSG, S. 7413 f., 7448; siehe auch Diebold/Rütsche, Rn. 527.
211 BGE 146 II 265, 269 E. 4.1; siehe auch BVGer C-3805/2020 vom 09.05.2022, E. 8.2.4; BVGer C-4789/2015 vom 29.01.2016, E. 2.1; BVGer C-4660/2013 vom 28.05.2015, E. 3.5; BVGer C-6342/2013 vom 23.02.2015, E. 2.1; BVGer C-6412/2012 vom 03.11.2014, E. 4.1; Botschaft PrSG, S. 7432; statt aller und zuletzt Hess, in: Häner/Waldmann, S. 220.
212 Hess, in: Häner/Waldmann, S. 220; in Bezug auf die Inverkehrbringung BVGer C-3805/2020 vom 09.05.2022, E. 8.2.4.
213 Siehe bspw. Verordnung über die Produktesicherheit vom 19. Mai 2010, SR 930.111 (zit. PrSV), 5. Abschnitt; siehe auch Produktesicherheit – die BFU überwacht den Markt, abrufbar unter <https://www.bfu.ch/de/die-bfu/ueber-die-bfu/marktueberwachung-produktesicherheit>, zuletzt besucht am 31.05.2025.
214 Kapoor/Klindt, S. 651.

nötig – Massnahmen ergreifen.[215] Die Marktüberwachung wurde in der EU 2019 mit der Marktüberwachungsverordnung für viele Produkte harmonisiert.[216]

70 Werden die produktsicherheitsrechtlichen Nachmarktpflichten in der Schweiz nicht an die oben dargelegten Risiken angepasst, kann es sein, dass die Gesundheit und Sicherheit der Bevölkerung ungenügend geschützt sind. Ist für Hersteller unklar, welche produktsicherheitsrechtlichen (Nachmarkt-)Pflichten bestehen, kann diese Rechtsunsicherheit zu enormen Kosten für Abklärungen, zu langsamen Prozessen und zur Hemmung von Innovation führen.[217]

215 KAPOOR/KLINDT, S. 653.

216 Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011 (Marktüberwachungsverordnung), ABl. L 169/1 (zit. MÜVO), ErwG 6 i.V.m. Anhang I.

217 Ähnlich Europäische Kommission, Impact Assessment GPSR, S. 14 f.

Teil 2:
Grundlagen

Im zweiten Teil dieser Arbeit werden die Grundlagen erläutert, die für das Verständnis der Nachmarktpflichten für Smart Home Devices, Software und KI wichtig sind. Zunächst werden die technischen und rechtlichen Grundlagen von Smart Home Devices, Software und KI aufgezeigt. Danach werden die rechtlichen Grundlagen für die produktsicherheitsrechtlichen Nachmarktpflichten in der Schweiz und der EU dargelegt. Zuletzt werden die rechtlichen Grundlagen für Smart Home Devices, Software und KI in Bezug auf das Produktsicherheitsrecht beschrieben. 71

A. Technische und rechtliche Grundlagen für Software- und KI-Produkte

72 Diese Arbeit betrachtet die produktsicherheitsrechtlichen Nachmarktpflichten für Software und KI-Systeme mit und ohne Zusammenhang mit physischen Produkten. Da Smart Home Devices als Beispiele dienen, muss definiert werden, was genau Software, KI-Systeme und Smart Home Devices sind. Damit die besonderen Herausforderungen von Nachmarktpflichten in Bezug auf die genannten Produkte verstanden werden können, ist es nötig, gewisse technische Eigenschaften zu kennen. Diese werden in diesem Kapitel dargelegt. Zudem werden die rechtlichen Grundlagen von Software und KI betrachtet. Es wird auf die Entstehungsgeschichte der KI-Regulierung in der EU eingegangen, und die Diskussionen, die in der Schweiz stattfinden, werden aufgezeigt.

I. Technische Grundlagen für Software- und KI-Produkte

73 Technische Produkte werden zunehmend komplizierter und für Konsumenten wird es deshalb schwieriger, die damit einhergehenden Gefahren zu erkennen. Wie BÜHLER/TOBLER treffend schreiben: «Während früher dazu die allgemeine Lebenserfahrung genügte, sind im technischen Sicherheitsrecht spezielles technisches Erfahrungswissen oder wissenschaftliche Erkenntnisse notwendig».[218] In diesem Kapitel werden deshalb Hardware, Software, KI und Smart Home Devices definiert. Es werden dabei für das Produktsicherheitsrecht relevante Abgrenzungen vorgenommen.

1. Hardware

74 Als Hardware wird ein physisches, technisches Gerät[219] bezeichnet. Ein Computersystem besteht jeweils aus Software und Hardware.[220] Hardware ist ein

218 BÜHLER/TOBLER, S. 127.

219 BOMHARD/SCHREIBER, in: Bomhard et al., § 1 Rn. 3; Beck ProdSG-KLINDT/SCHUCHT, § 2 N 168; siehe auch Art. 3 Ziff. 5 CRA, welcher Hardware, als «ein physisches elektronisches Informationssystem, das digitale Daten verarbeiten, speichern oder übertragen kann, oder Teile eines solchen Systems» definiert.

220 BOMHARD/SCHREIBER, in: Bomhard et al., § 1 Rn. 2.

Sammelbegriff[221] für jenen physischen Teil, auf welchem Software ausgeführt wird (z.B. Staubsaugerroboter, Smartphone, Computer) oder mit welchem man auf Software zugreifen kann (z.B. Knopf auf dem Staubsaugerroboter, Touchscreen, Tastatur). Sie besteht normalerweise aus elektronischen Komponenten, welche bspw. die Berechnungen, Speicherungen und Anzeigen von Ausgaben eines Computersystems möglich machen, und aus einem Gehäuse, welches die elektronischen Komponenten vor äusseren Einwirkungen schützt.[222] Bei Smart Home Devices können somit das «sichtbare» Gerät (z.B. die Ladestation und der fahrende Roboter bei einem Staubsaugerroboter) und die darin verbaute Elektronik zur Hardware gezählt werden. Wichtige Hardwareteile bei Smart Home Devices sind Sensoren und Aktoren. Während Sensoren Informationen aus der Umwelt erfassen[223], beeinflussen Aktoren die Umwelt[224].

2. Software

Unter dem Begriff «Software» werden Computerprogramme verstanden.[225] Es handelt sich dabei um nichtphysische Teile eines Computers.[226] Eine einheitliche und allgemein anerkannte Definition für Software gibt es nicht.[227] Der Begriff «Software» hat sich als Gegensatz zum Begriff «Hardware» entwickelt.[228] Sie kann – muss aber nicht – Hardwaregeräte steuern.[229] Es kann zwischen Systemprogrammen, welche den «unmittelbaren Betrieb des Computers» möglich machen, und Anwendungsprogrammen (wie z.B. «Apps»), die Probleme lösen sollen, unterschieden werden.[230] Software besteht aus Befehlen, die Steuerfunktionen auslösen.[231] 75

221 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 2.
222 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 3; Fröhlich-Bleuler, Rn. 37.
223 Bspw. über Mikrofone oder Kameras, Röglinger/Püschel/Egger, in: Bräutigam/Kraul/Bauer, § 2 Rn. 12; Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 17.
224 Bspw. über Töne oder Bewegungen, Röglinger/Püschel/Egger, in: Bräutigam/Kraul/Bauer, § 2 Rn. 13; Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 17.
225 Konertz/Schönhof, S. 25; ähnlich bereits Fröhlich-Bleuler, Rn. 25.
226 Wittbrodt, S. 74; ebenso Nosetti, in: Hürlimann-Kaup et al., S. 219 Fn. 4.
227 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 7; Borges, Begriff, Rn. 31.
228 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 2; Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.
229 Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.
230 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 5.
231 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 22.

76 Software kann sowohl in Form von Quellcode (auf Deutsch auch «Quelltext» oder engl. «Source Code»[232]) als auch als Binärcode vorliegen. Während Software von der Hardware als Binärcode ausgeführt wird, arbeiten Programmierer mit Quellcode in verschiedenen Sprachen.[233] Ohne Quellcode können normalerweise keine Änderungen an der Software vorgenommen werden.[234] Soweit im Folgenden von Software die Rede ist, ist hierunter jeweils unmittelbar ausführbarer Code zu verstehen.

2.1. Abgrenzung von Softwarekategorien

77 Software lässt sich nur schwer in einzelne Kategorien aufteilen. Es ist jedoch nötig, verschiedene Kategorien zu definieren, weil in der Lehre teilweise gleiche Begriffe mit völlig anderem Inhalt verwendet werden.[235]

a. Individualsoftware und Standardsoftware

78 Die Unterscheidung zwischen Individual- und Standardsoftware ist im Produktsicherheitsrecht relevant, weil es umstritten ist, ob beides als Produkt erfasst ist.[236] Individualsoftware wird – im Gegensatz zu Standardsoftware – spezifisch für einen Auftraggeber nach dessen Anforderungen entwickelt.[237] Diese Unterscheidung lässt sich auch bei KI vornehmen:[238] Individualsoftware mit KI kann für spezifische Funktionen eines Auftraggebers entwickelt werden, etwa durch Training mit individuellen Trainingsdatensets. Standardsoftware mit KI hingegen wird für vielfältige Anwendungen erstellt und ist vor der Nutzung normalerweise abgeschlossen (der Lernprozess wird «eingefroren»). Die Grenzen zwischen Individual- und Standardsoftware verschwimmen, da standardisierte KI-Modelle in verschiedenen Entwicklungsstufen bereitgestellt werden können. Basisfunktionen können bspw. durch individuelles Training oder Add-ons spezifisch angepasst werden, wodurch sich das ursprüng-

232 Dal Molin-Kränzlin/Dal Molin, S. 383.

233 Dal Molin-Kränzlin/Dal Molin, S. 383; Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 19, 21.

234 Dal Molin-Kränzlin/Dal Molin, S. 383.

235 Siehe bspw. Bühler, Bestandteil, S. 33 f., welcher Stand-alone-Software beschreibt, aber den Begriff «Individualsoftware» verwendet; siehe auch etwas verwirrend SHK PrSG-Hess, Art. 2 N 12.

236 S. u., Rn. 214.

237 Fröhlich-Bleuler, Rn. 36, 1639; Passadelis, in: Kasper Lehne/Münch/Probst, Kap. 84 Rn. 0.1.

238 McGuire, in: Foerste/Westphalen, § 58 Rn. 29.

liche Modell durch die Nutzung verändert.[239] Verschwimmende Grenzen gibt es auch bei Individual- und Standardsoftware ohne KI, da auch diese durch Add-ons ergänzt werden können. Im B2C-Bereich wird jedoch i.d.R. lediglich Standardsoftware eingesetzt.

b. Embedded Software und Stand-alone-Software

Wenn Software in Hardware integriert ist, wird diese meistens «Embedded Software» oder «integrierte Software» genannt.[240] Embedded Software kann die Vernetzung von Geräten ermöglichen (bspw. bei IoT-Geräten) oder ein Gerät wie einen Staubsaugerroboter steuern.[241] Ein häufig genanntes Beispiel ist Firmware.[242] Es gibt jedoch keine genaue Definition für Firmware (bspw. sind Betriebssysteme je nach Definition Firmware oder auch nicht). Unbestritten ist, dass Firmware eine Art von Software ist. Firmware wird i.d.R. konkret für eine bestimmte Art von Gerät geschrieben und funktioniert deshalb nicht auch bei anderen Geräten (im Gegensatz zu anderer Software). Ohne Firmware funktionieren die elektronischen Komponenten der Hardware nicht. 79

Im Gegensatz dazu gibt es Software, die zwar auf physischer Hardware ausgeführt wird, aber nicht auf ein bestimmtes Gerät mit spezifischen physischen Funktionen (z.B. Sensoren oder Aktoren) zugeschnitten ist, sondern unabhängig davon bereitgestellt und betrieben werden kann.[243] Diese sog. Standalone-Software, «eigenständige Software» oder «isolierte Software» wird z.B. online auf einer Website zur Verfügung gestellt, über die Hardware heruntergeladen und installiert.[244] In manchen Fällen erfolgt die Nutzung auch rein webbasiert via Browser, ohne lokale Installation beim Nutzer, wie etwa bei SaaS. Auch SaaS kann Funktionen auf Geräten beeinflussen, etwa durch cloudbasierte Steuerungsmechanismen.[245] In all diesen Fällen erfolgt der Zugriff letztlich über Hardware. 80

239 McGuire, in: Foerste/Westphalen, § 58 Rn. 29.

240 Oster, in: Foerste/Westphalen, § 57 Rn. 7; auf Deutsch auch «eingebettete Software»: Beck KI-VO-Ruschemeier, Art. 6 N 39; auch «unselbstständige» oder «produktnahe» Software: Beck ProdSG-Klindt/Schucht, § 2 N 164a; für die Schweiz Bühler, Bestandteil, S. 33.

241 Oster, in: Foerste/Westphalen, § 57 Rn. 7 mit weiteren Beispielen.

242 Verwenden Firmware und Embedded Software bspw. austauschbar: Wiebe, Pflichten, S. 66, 69; Schmid, IT, S. 196.

243 Oster, in: Foerste/Westphalen, § 57 Rn. 7.

244 Oster, in: Foerste/Westphalen, § 57 Rn. 7.

245 Piovano/Schucht/Wiebe, S. 85.

81 Diese Unterscheidung zwischen Embedded und Stand-alone-Software wird auch bei KI-Systemen verwendet.[246]

82 Wie bereits beschrieben, ist die Unterscheidung zwischen Embedded und Stand-alone-Software nicht mehr zeitgemäss.[247] Dennoch wird in dieser Arbeit wo nötig weiterhin zwischen Embedded und Stand-alone-Software differenziert, da sich die Lehrmeinungen über die Behandlung dieser zwei «Arten» von Software teilweise sehr unterschiedlich gestalten.

c. *Updates von Software und Versionen*

83 Ein Softwareupdate bezeichnet vorliegend eine vom Hersteller veranlasste gezielte Veränderung der Software nach dem Inverkehrbringen. Updates können bspw. Funktionen erneuern[248], Fehler entfernen[249] sowie Sicherheitslücken schliessen[250]. Statt «Update» wird auch der Begriff «Upgrade» verwendet, welcher nicht nur lediglich eine Veränderung, sondern eine weitergehende Verbesserung sowie Funktionserweiterung der Software impliziert.[251] Statt Update und Upgrade wird auf Deutsch auch für beide Begriffe die Übersetzung «Aktualisierung» benutzt,[252] ohne zwischen inhaltlichem Umfang und technischer Tiefe zu differenzieren. In der Praxis wird ein Update meist durch eine Anpassung der Versionsnummer kenntlich gemacht. Kleinere Änderungen führen etwa von Version 1.0 zu 1.1, während grundlegende Erweiterungen zu einem Sprung auf Version 2.0 führen können. Spezifisch in Bezug auf KI kann der Hersteller ein im Vergleich zur ersten Version erweitert angelerntes KI-System in Verkehr bringen (z.B. ChatGPT 3.5 zu ChatGPT 4 und dann zu ChatGPT 4o). Dies entspricht einem Update.[253]

84 Ein Update kann vom Hersteller bspw. vor Ort über kabelgebundene Verbindungen auf das zu aktualisierende Gerät übertragen werden. Ebenfalls möglich ist die kabellose Übertragung («over the air») aus der Ferne z.B. via Wi-Fi

246 McGuire, in: Foerste/Westphalen, § 58 Rn. 29; siehe auch Borges, Begriff, Rn. 46.
247 S. o., Rn. 34.
248 Kohm/Schreiber, in: Bomhard et al., § 9 Rn. 56; Reusch, Mobile Updates, S. 904.
249 Kohm/Schreiber, in: Bomhard et al., § 9 Rn. 56; Reusch, Mobile Updates, S. 904.
250 Hessel, in: Bomhard et al., § 14 Rn. 33; Reusch, Mobile Updates, S. 904.
251 Kohm/Schreiber, in: Bomhard et al., § 9 Rn. 56.
252 Kohm/Schreiber, in: Bomhard et al., § 9 Rn. 56; siehe auch Erwägung 25 und Art. 37 Abs. 3 GPSR, wo die beiden Begriffe Software- «Update» und – «Aktualisierung» synonym verwendet werden.
253 Solche grösseren Updates könnten durch eine sicherheitsrelevante wesentliche Veränderung des Produktes einer erneuten Inverkehrbringung gleichkommen. Das Produkt würde dann durch das Update zu einem neuen Produkt werden. S. u., Rn. 302.

(aus dem Internet) oder aus der Nähe z.B. via Bluetooth.[254] Geräte mit Softwarekomponenten können nicht «automatisch» vom Hersteller aus der Ferne aktualisiert werden. Die Software sowie in vielen Fällen auch die Hardware müssen entsprechend konfiguriert[255] werden, bevor das Produkt in Verkehr gebracht wird, damit der Hersteller später eine Verbindung dazu aufbauen kann (sog. Update-Fähigkeit).[256]

Verändert sich ein KI-System durch selbstständiges Lernen, etwa auf Basis von Nutzer- oder Umweltdaten, liegt kein Update im oben beschriebenen Sinn vor, weil es sich nicht um eine aktive und gezielte Veränderung der Software durch den Hersteller handelt. 85

3. Künstliche Intelligenz (KI)

Der Begriff «Künstliche Intelligenz» wird unterschiedlich verwendet und definiert.[257] Weder in der Informatik[258] noch in der Rechtswissenschaft[259] gibt es bis anhin eine allgemein anerkannte Definition.[260] Mit laufender technologischer Entwicklung kann sich der Inhalt von KI weiter verändern.[261] Als der Begriff «artificial intelligence» das erste Mal beschrieben wurde, wurde er nicht definiert.[262] Es handelt sich bei KI um einen Sammelbegriff für verschiedene Methoden, Techniken und Konzepte,[263] die in KI-Anwendungen eingesetzt werden, um Probleme zu lösen oder bestimmte Aufgaben zu erfüllen. Sie umfassen verschiedene Verfahren, die je nach Anwendungsbereich und Zielsetzung variieren.[264] Zu den KI-Methoden gehören maschinelles Lernen (engl. «Machine Learning»), künstliche neuronale Netzwerke (z.B. Deep Learning), natürliche Sprachverarbeitung (engl. «Natural Language Processing», abge- 86

254 Reusch, Mobile Updates, S. 904; siehe auch May/Gaden, S. 111.

255 NHK GPSR-Piovano, Art. 9 N 104; Beurskens, in: Bomhard et al., § 16 Rn. 108; Oster, in: Foerste/Westphalen, § 57 Rn. 26, m.w.H.

256 Reusch, Mobile Updates, S. 906.

257 SBFI, KI Bericht, S. 7, 19; Reiter, S. 985, m.w.H.; Konertz/Schönhof, S. 30.

258 Batache, Rn. 26, m.w.H.; Beurskens, in: Bomhard et al., § 16 Rn. 1; Konertz/Schönhof, S. 30.

259 Beurskens, in: Bomhard et al., § 16 Rn. 1.

260 Es wird zu beobachten sein, ob sich dies nun mit der Definition des KI-Systems in der KI-VO ändert. S. u., Rn. 140.

261 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 8, m.w.H.; zur technologischen Entwicklung siehe auch Molavi Vasse'i, 191–192.

262 McCarthy et al., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, abrufbar unter <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>, zuletzt besucht am 31.05.2025.

263 Konertz/Schönhof, S. 68; Reiter, S. 985.

264 Für eine Übersicht und Beispiele siehe etwa Konertz/Schönhof, S. 34 ff.

kürzt «NLP»), Bayes'sche Methoden und Fuzzy-Logiken.[265] KI-Anwendungen werden oft als SaaS zur Verfügung gestellt[266] (z.B. ChatGPT, DeepL, Midjourney, Sora). Neben den unten diskutierten rechtlichen Definitionen können auch die Definitionen verschiedener Normenorganisationen relevant sein. Während die europäischen Normen momentan ausgearbeitet werden,[267] existieren bereits internationale Normen wie jene der International Organization for Standardization (ISO)[268].

87 Während die KI-VO den Begriff «KI-System»[269] definiert hat, war lange Zeit der Begriff «KI» ohne den Zusatz «System» gebräuchlicher. Obwohl der Begriff «KI» an sich[270] sowie die Definition von KI in der KI-VO[271] unscharf sind, werden sich die Bezeichnung «KI-System» und die Definition dessen vermutlich durchsetzen.[272] Die «Intelligenz» in KI kann menschlicher Intelligenz nicht gleichgestellt werden.[273]

88 Eine wichtige Unterkategorie von KI ist generative KI (engl. Abkürzung «Gen-AI»). Generative KI ist speziell für die Erzeugung neuer Inhalte konzipiert (z.B. Texte oder Bilder).[274] Demgegenüber ist KI ohne generative Komponente allgemeiner und auf die Analyse, Mustererkennung und Problemlösung fokussiert, ohne dass neue Inhalte generiert werden. Generativer KI ist ein höheres Risiko inhärent, da ihre Resultate weniger vorhersehbar sind als bei anderen

265 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 30 ff., wobei die Leitlinien bis zum 31.05.2025 noch nicht förmlich angenommen wurden.; Konertz/Schönhof, S. 68.

266 Borkert/Nomerowskaja, S. 167, m.w.H.

267 Harmonised Standards for the European AI Act, abrufbar unter <https://ai-watch.ec.europa.eu/news/harmonised-standards-european-ai-act-2024-10-25_en?utm>, zuletzt besucht am 31.05.2025; CEN und CENELEC, abrufbar unter <https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/?utm>, zuletzt besucht am 31.05.2025.

268 Insbesondere ISO/IEC 22989:2022 zu Konzept und Terminologie, die bspw. KI als Disziplin in Ziff. 3.1.3 und KI-System in Ziff. 3.1.4 definiert: ISO – Artificial intelligence, abrufbar unter <https://www.iso.org/sectors/it-technologies/ai>, zuletzt besucht am 31.05.2025.

269 Zur Einführung des Begriffes KI-System durch die Europäische Kommission siehe Borges, Begriff, Rn. 8 ff. m.w.H.; siehe auch Schwenke, S. 205.

270 Beurskens, in: Bomhard et al., § 16 Rn. 1.

271 Rosenthal, Jusletter 05.08.2024, Rn. 17.

272 Rosenthal, Jusletter 05.08.2024, Rn. 17; feststellend, dass sich der Begriff bereits durchgesetzt habe, Borges, Begriff, Rn. 10, m.w.H.

273 SBFI, KI Bericht, S. 29; ausführlich Molavi Vasse'i, S. 193; Konertz/Schönhof, S. 69; Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 9.

274 ErwG 99 KI-VO; siehe auch Krimphove, S. 155 Fn. 6, m.w.H.

KI-Methoden. Generative KI-Modelle sind typische Beispiele für General Purpose AI (GPAI).[275]

3.1. Abgrenzung schwache und starke KI (AGI)

Bei der vorliegend beschriebenen Form von KI handelt es sich stets um sog. «schwache KI» (engl. «narrow AI»). Diese Art von KI wird für die Lösung spezifischer Probleme entwickelt und kann nur für eingeschränkte Aufgaben und Bereiche angewandt werden.[276] Ein Bildgenerierungsprogramm wird bspw. nicht erkennen können, ob die Temperatur in einer Wohnung richtig eingestellt ist. 89

«Starke KI» (engl. «Artificial General Intelligence», kurz «AGI») ist momentan eine hypothetische Form von KI, da sie technisch (noch) nicht realisierbar ist.[277] Es handelt sich dabei um die Vorstellung einer KI, die generell Probleme lösen sowie menschlich denken und handeln kann.[278] 90

3.2. Technische Abgrenzung «herkömmlicher» Software und «KI»

Bei KI handelt es sich immer um eine Art von Software.[279] Fraglich ist, wie sich KI von herkömmlicher Software abgrenzen lässt und was die ausschlaggebenden Kriterien für diese Abgrenzung sind.[280] 91

275 ErwG 99 KI-VO; s. u., Rn. 132.

276 Asenger, S. 135; Konertz/Schönhof, S. 27.

277 SBFI, KI Bericht, S. 28 f.; Sheikh/Prins/Schrijvers, S. 159; Konertz/Schönhof, S. 28; Gartner schätzt, dass es noch mindestens zehn Jahre dauern wird, bis AGI relevant wird Gartner Hype Cycle for Emerging Technologies 2024, abrufbar unter <https://www.gartner.com/en/articles/hype-cycle-for-emerging-technologies>, zuletzt besucht am 31.05.2025.

278 Konertz/Schönhof, S. 27 ff.; siehe auch ISO/IEC 22989:2022(en) Information technology, Artificial intelligence, Artificial intelligence concepts and terminology, Ziff. 3.1.14, Note 2 (zit. ISO 22989:2022).

279 McGuire, in: Foerste/Westphalen, § 58 Rn. 15; so sind bspw. auch neuronale Netze und grosse Sprachmodelle (LLMs) unter dem Begriff Software erfasst, Borges, Begriff, Rn. 38, 40; Konertz/Schönhof, S. 31, 79.

280 Die ursprüngliche Definition der EU für KI wurde im Vorschlag für die KI-VO vor allem kritisiert, weil sie zu umfassend war und auch «herkömmliche» Software erfasste, s. u., Rn. 119.

a. «Lernen» und «Ableiten» im Kontext von KI

92 Im Kontext von KI-Systemen bezeichnet «Lernen» den technischen Prozess, bei dem aus vorhandenen Daten mithilfe algorithmischer Verfahren Muster erkannt, mathematische Modelle gebildet und diese auf neue Daten angewendet werden. Der Lernprozess ermöglicht es dem System, sein Verhalten anzupassen und auf dieser Grundlage eigenständig Entscheidungen oder Empfehlungen zu generieren.[281] Ein Algorithmus ist eine Abfolge von Regeln, die nach genauen Vorgaben maschinell abgearbeitet werden können.[282] Die Implementierung von Algorithmen in einem «Programm, einer Software oder [in] einem Informationssystem» wird auch algorithmisches System genannt.[283] Software[284] und damit auch KI-Systeme[285] beruhen jeweils auf implementierten Algorithmen, aber nicht alle algorithmischen Systeme sind Software[286] oder KI[287].

93 Der Lernprozess erfolgt bspw. durch technische Trainingsmethoden des maschinellen Lernens wie überwachtes (engl. «supervised»), unüberwachtes (engl. «unsupervised») oder bestärkendes (engl. «reinforcement») Lernen.[288] Ziel ist es, die Leistung des Systems hinsichtlich spezifischer Aufgaben zu optimieren, ohne dass für jede Entscheidung explizite Programmieranweisungen erforderlich sind. Während des Lernens und zum Teil auch während der Anwendung werden Zufalls- oder Pseudozufallszahlen verwendet,[289] was ebenfalls dazu führt, dass das Verhalten solcher Systeme nicht vollständig deterministisch ist. Der Übergang von rein deterministischen,[290] regelbasierten Programmen zu adaptiven und selbstoptimierenden Systemen kann mit er-

281 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 31.

282 Thouvenin et al., Jusletter IT 04.07.2024, Rn. 28, m.w.H.; eine einheitliche Definition gibt es jedoch nicht: Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 25, 28, m.w.H.; Konertz/Schönhof, S. 53.

283 Thouvenin et al., Jusletter IT 04.07.2024, Rn. 31.

284 Konertz/Schönhof, S. 55 f. m.w.H.

285 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 31.

286 Konertz/Schönhof, S. 56.

287 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 31.

288 Siehe dazu im Detail Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 32-38; und Thouvenin et al., Jusletter IT 04.07.2024, Rn. 48 ff.

289 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 31; Thouvenin et al., Jusletter IT 04.07.2024, Rn. 34.

290 Für eine Definition siehe Russell/Norvig, S. 63; zu deterministischen und nicht-deterministischen Algorithmen siehe auch Thouvenin et al., Jusletter IT 04.07.2024, Rn. 33 f. m.w.H.

höhten Risiken einhergehen, insbesondere der fehlenden Vorhersehbarkeit und dem Kontrollverlust durch Veränderlichkeit und Opazität.[291]

Die Fähigkeit des «Ableitens» (engl. «inference») eines KI-Systems wird neben dem maschinellen Lernen auch mit logik- und wissensgestützten Konzepten erreicht, indem statt aus grossen Datenmengen aus menschlichem Expertenwissen «gelernt» wird.[292] Dabei handelt es sich um explizit strukturierte und codierte Informationen bzw. symbolisch aufgebaute Darstellungen, die die zu lösenden Aufgaben formalisieren und für die Verarbeitung durch das KI-System zugänglich machen,[293] z.B. durch Ontologien, welche Objekte und deren Beziehungen in einer formalen Sprache abbilden und so komplexe Wissensstrukturen repräsentieren.[294] Auf der Grundlage des menschlichen Expertenwissens können diese KI-Systeme durch logisches Schliessen («via deductive or inductive engines») oder durch bestimmte Rechenoperationen wie Sortieren, Suchen, Vergleichen und Verknüpfen Resultate «ableiten» (engl. «reason»).[295] 94

«Ableiten» kann in der Lern- (auch: Trainingsphase oder engl. «pre-deployment or building phase»[296]) und der Anwendungsphase (auch: Inferenzphase oder engl. «post-deployment or use phase»[297]) stattfinden. Generell bezieht sich «Ableiten» auf die Generierung von Output aus Input in der Anwendungsphase.[298] KI-Systeme müssen jedoch nach ihrer Inverkehrbringung oder Inbetriebnahme nicht zwingend weiterlernen können.[299] Zur Präzisierung der Definition bezieht das Memorandum zur KI-Definition der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) die Formulierung «infer how to generate outputs» auch auf die Lernphase eines KI-Systems, in welcher ein Modell aus Daten ableitet.[300] 95

291 Siehe dazu oben, Rn. 54.
292 ErwG 12 KI-VO; Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 39; OECD, Explanatory Memorandum, S. 8, welches festhält, dass es auch Mischformen gibt.
293 ErwG 12 KI-VO.
294 Russell/Norvig, S. 272 f., 332 ff., 356.
295 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 39; siehe auch Ziff. 3.1.17 ISO 22989:2022.
296 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 10.
297 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 10.
298 OECD, Explanatory Memorandum, S. 9.
299 S. u., Rn. 126.
300 OECD, Explanatory Memorandum, S. 9.

b. Batch- und Online-Learning

96 Wie oben beschrieben[301], kann KI auf verschiedene Weisen «angelernt» werden, namentlich durch das sog. «Batch-Learning» (auch: Offline-Learning) und das sog. «Online-Learning» (auch: Incremental Learning).[302] Die zurzeit (noch) am häufigsten eingesetzten KI-Systeme, welche mittels maschinellem Lernen trainiert wurden, haben zwar «gelernt», sind aber nach dem Inverkehrbringen nicht mehr «lernfähig».[303] Wird das Training vor der Anwendung des Systems abgeschlossen, handelt es sich um «Batch-Learning» bzw. um ein «eingefrorenes System»[304]. Der Hersteller hat weiterhin die Möglichkeit, das System weiter zu trainieren und das Produkt mit einer neuen Version zu aktualisieren.[305] Eine andere Methode ist das «Online-Learning», bei welchem das Training kein Ende nimmt und kontinuierlich mit neuen Daten weitertrainiert wird.[306] WENDEHORST et al. beschreiben diese drei Vorgehensweisen auch als «Nutzung fixierter Modelle», «Nutzung fixierter Modelle mit Updates» und «selbstständige Anpassung des KI-Systems».[307]

97 Beim Batch-Learning wird ein KI-Modell auf einem vollständigen, vorab gesammelten Datensatz trainiert, wobei das Training in einem einzigen Schritt oder mehreren grossen Abschnitten erfolgt. Die «Batches», also die verwendeten Datensätze, werden dazu genutzt, die Gewichtung verschiedener Parameter zu bestimmen.[308] Sind die Gewichte einmal bestimmt, wird das trainierte Modell immer mit diesen Gewichten arbeiten. Die Lernphase ist dann abgeschlossen und das System befindet sich in der Anwendungsphase.[309] Die «Lernfähigkeit» ist sozusagen «eingefroren».[310] In der Regel führt die gleiche Eingabe zur gleichen Ausgabe, es sei denn, das System enthält bewusst einge-

---

301 S. o., Rn. 42.

302 HOI et al., S. 249 f., 269. Wobei es noch weitere Methoden und Varianten gibt, die je nach Anwendungsfall und Datenstruktur zum Einsatz kommen. Einige davon sind Kombinationen oder Spezialisierungen dieser zwei Kategorien; siehe auch Ziff. 3.1.9 ISO 22989:2022.

303 MCGUIRE, in: Foerste/Westphalen, § 58 Rn. 26; HOI et al., S. 249; ETZKORN, S. 361; OECD, Explanatory Memorandum, S. 8.

304 MCGUIRE, in: Foerste/Westphalen, § 58 Rn. 26; ZECH, Gutachten, A 72.

305 MCGUIRE, in: Foerste/Westphalen, § 58 Rn. 26.

306 RUSSELL/NORVIG, S. 720 ff.; siehe auch THOUVENIN et al., Jusletter IT 04.07.2024, Rn. 55, Fn. 85; dabei ist das Online-Learning vom Continual-Learning abzugrenzen, HOI et al., S. 281.

307 WENDEHORST et al., S. 607.

308 Siehe auch BOMHARD/SCHREIBER, in: Bomhard et al., § 1 Rn. 32.

309 HÄNSENBERGER, Drohnen, S. 51 f. m.w.H.

310 MCGUIRE, in: Foerste/Westphalen, § 58 Rn. 26; ZECH, Gutachten, A 72; ebenso: WILDHABER, Einführung, S. 47; LOHMANN, Haftungsrahmen, S. 112.

baute Zufallselemente. Auch diesen Systemen kann die Transparenz fehlen, sie sind jedoch für Hersteller einfacher zu kontrollieren als Systeme, die «selbstständig» weiterlernen.[311]

Systeme können nicht nur lediglich trainiert und nach vollendetem Training in Betrieb genommen werden. Beim Online-Learning lernt ein KI-Modell kontinuierlich aus neuen Datenpunkten oder kleinen Datenmengen, die fortlaufend generiert oder bereitgestellt werden, und passt sich in Echtzeit an veränderte Daten oder Bedingungen an. Sie kombinieren Lern- und Anwendungsphase.[312] Es werden also kontinuierlich neue Trainingsdaten in die Berechnungen einbezogen, was natürlich zu neuen Resultaten führen kann.[313] Lernt ein System nach seiner Inbetriebnahme weiter, werden die Resultate, Entscheide oder Ergebnisse für den Hersteller unberechenbarer[314] im Vergleich zu «Batch-Learning»-Systemen. Beispiele für «Online-Learning»-Systeme sind Empfehlungssysteme und Systeme zur Portfoliooptimierung.[315] 98

c. *Trainingsdaten*

Die Trainingsdaten, welche benötigt werden, um «weiterzulernen», erhält das System entweder, indem es sie selbstständig mittels Sensoren aus seiner Umwelt bezieht (z.B. nimmt eine Kamera in einem Staubsaugerroboter Bilder ihrer Umgebung auf und das KI-System wertet diese dann aus), oder sie werden dem System vom Hersteller (z.B. die von seinen Kunden erhobenen Daten verschiedener Wohnungsgrundrisse) oder vom Nutzer «gefüttert» (z.B. durch Angaben von Hindernissen wie Teppichen oder Pflanzen in der App des Staubsaugerroboters).[316] Ein solches System kann also auch Entscheidungen aufgrund von Daten fällen, die es bei seiner Inbetriebnahme noch nicht hatte. 99

311 KONERTZ/SCHÖNHOF, S. 49 f. nennen als Ausnahme davon «Generative Adversarial Networks», bei welchen es sich um eine Form generativer KI handelt.

312 HÄNSENBERGER, Drohnen, S. 52, m.w.H.

313 Siehe auch, HÄNSENBERGER, Drohnen, S. 52.

314 SPINDLER, Vorschläge, Rn. 20; KONERTZ/SCHÖNHOF, S. 49 ff. verwenden als Beispiel den Chatbot Tay, welcher sich innerhalb weniger Stunden zu einem rassistischen und beleidigenden Bot entwickelte, weil er ungefiltert aus Twitter-Beiträgen lernte.

315 HOI et al., S. 250.

316 Siehe auch MCGUIRE, in: Foerste/Westphalen, § 58 Rn. 34; RUSSELL/NORVIG, S. 723 f.

d. Autonomie von KI

100 «Autonomie» ist von «Automation» zu unterscheiden.[317] Automation umfasst «vorprogrammierte»[318] Prozesse, bei denen Aufgaben nach festen Regeln ausgeführt werden, ohne dass z.B. von einem KI-System selbstständig Entscheidungen getroffen werden können.[319] Als «autonom» werden hingegen Systeme bezeichnet, die eigenständig Entscheidungen basierend auf ihrem Training[320] oder regelbasierter Wissensverarbeitung treffen und sich an neue Situationen anpassen können.[321]

101 Mit «selbstständig» und «eigenständig» soll nicht impliziert werden, dass KI-Systeme eine Art menschlichen «freien Willen» hätten.[322] KI-Systeme agieren immer nach vordefinierten Parametern gem. ihrer Programmierung, Architektur und dem errechneten Modell.[323] Die Autonomie im Zusammenhang mit KI wird deshalb auch «digitale Autonomie»[324] genannt.

4. Smart Home Devices

102 Dieser Arbeit liegt das Verständnis von PIOVANO von «smarten Produkten» zugrunde. Er definiert sie als «Produkte, die entweder mit dem Internet verbunden sind oder zumindest die Möglichkeit haben, mit dem Internet verbunden zu werden, oder die zum Zwecke der Funkkommunikation andere Funkwellen aussenden und/oder empfangen können».[325] Smarte Geräte werden auch IoT[326]-Geräte oder Smart Objects genannt und sind technische Geräte mit integrierter Informations- und Kommunikationstechnologie,[327] die über das Internet oder ein lokales Netzwerk miteinander verbunden sind.[328] Die auf IoT-Technologien basierenden Produkte und Dienstleistungen können in die

317 Ziff. 3.1.5, 3.1.7 ISO 22989:2022; BRÄUTIGAM, in: Bräutigam/Kraul/Bauer, § 1 Rn. 9; siehe auch HÄNSENBERGER, Drohnen, S. 43, m.w.H.

318 WAGNER, Verantwortlichkeit, S. 720.

319 Ziff. 3.1.7. ISO 22989:2022; BRÄUTIGAM, in: Bräutigam/Kraul/Bauer, § 1 Rn. 9.

320 Ausführlich WAGNER, Verantwortlichkeit, S. 720, m.w.H.; siehe auch ZECH, Regelungen, S. 37, welcher Autonomie und Lernfähigkeit gleichsetzt.

321 Siehe auch 3.1.5. ISO 22989:2022.

322 Siehe auch WAGNER, Verantwortlichkeit, S. 720, m.w.H.

323 BATACHE, Rn. 56, m.w.H.

324 Ausführlich ausgearbeitet von BATACHE, Rn. 54 ff. m.w.H.; WAGNER, Verantwortlichkeit, S. 720.

325 NHK GPSR-PIOVANO, Art. 9 N 98; ebenso PIOVANO/SCHUCHT/WIEBE, S. 2.

326 IoT steht für «Internet of Things».

327 BRÄUTIGAM, in: Bräutigam/Kraul/Bauer, § 1 Rn. 8.

328 BRÄUTIGAM, in: Bräutigam/Kraul/Bauer, § 1 Rn. 18; siehe auch WAGNER, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.

Kategorien Wearables, Smart-Home-Geräte und -Anwendungen, vernetzte Fahrzeuge und vernetzte Produktionsmaschinen eingeteilt werden.[329] Vorliegend werden nur sog. «Consumer IoT» untersucht. Dieser Begriff umfasst mit dem Internet verbundene Konsumentenprodukte.[330] Viele dieser Consumer IoT können Teil eines ganzen Netzwerks von smarten Geräten sein, die miteinander verknüpft sind und in privaten Haushalten eingesetzt[331] werden.[332] Es handelt sich bei diesen smarten Haushaltsgeräten um Smart Home Devices.[333] Eine der wichtigsten Eigenschaften von smarten Objekten ist, dass sie mit Sensoren, Aktoren und Software ausgestattet sind.[334] Software ist ein essenzieller Bestandteil von smarten Geräten, da die Hardware ohne Software nutzlos[335] oder zumindest stark eingeschränkt wäre. Durch Sensoren und Software werden diese Geräte in die Lage versetzt, Daten aus der Umwelt zu sammeln. Nutzer können smarte Geräte dann bspw. überwachen, steuern und automatisierte Aufgaben ausführen lassen.[336] Die gesammelten Daten lassen sich auch als Trainingsdaten für KI nutzen.[337] Demgegenüber kann KI die Datenanalyse verbessern und zu weiterer Wertschöpfung beitragen.[338] Wird KI integriert, können smarte Geräte nicht nur automatisiert, sondern auch zu einem gewissen Grad autonom agieren.[339] Soweit ersichtlich sind momentan keine Smart Home Devices auf dem Markt, die zu echtem Online-Learning fähig sind. Sie werden stattdessen «eingefroren» vermarktet.[340]

Smart Home Devices sind bspw. Thermostate, welche die Raumtemperatur steuern und sie basierend auf der Anwesenheit von Personen oder vordefinierten Zeitplänen anpassen. Weitere Beispiele sind Lautsprecher, die mit 103

329 Piovano/Schucht/Wiebe, S. 2 f.

330 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 21, welcher als Beispiele «intelligente Haushaltsgeräte, Wearables oder Smartphones» nennt.

331 Dies schliesst nicht aus, dass es sich dabei um Dual-Use-Produkte handeln kann. S. u., Rn. 187.

332 Siehe auch Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157.

333 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 21; siehe auch die Beispiele in Röglinger/Püschel/Egger, in: Bräutigam/Kraul/Bauer, § 2 Rn. 64 ff.

334 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 9, m.w.H. zu Interaktions-, Daten- und Serviceebenen.

335 Ähnlich Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 160.

336 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 9.

337 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 9.

338 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 39. Bräutigam bezeichnet das Verhältnis zwischen IoT und KI deshalb als «symbiotisch».

339 Bräutigam, in: Bräutigam/Kraul/Bauer, § 1 Rn. 9.

340 Ähnlich Wagner, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 27 f., der 2019 feststellte, dass die meisten IoT-Geräte keine autonomen Entscheidungen oder sogar maschinelles Lernen zuliessen.

Sprachassistenten (wie Alexa, Google Assistant oder Siri) verbunden sind, um Musik abzuspielen, Informationen bereitzustellen oder Geräte zu steuern. Kühlschränke, Waschmaschinen und Öfen, die über eine Verbindung zum Internet optimiert werden können, um z.B. Fernsteuerung oder Wartungsbenachrichtigungen zu ermöglichen, gehören ebenfalls dazu. Auch als Smart Home Device bezeichnen kann man z.B. Staubsaugerroboter, die Räume selbstständig vermessen und reinigen.[341] Smart Home Devices werden aufgrund von Vorteilen wie Komfort, Energieeinsparungen und Sicherheit[342] eingesetzt, da sie es Nutzern ermöglichen, verschiedene Funktionen zu automatisieren oder aus der Ferne zu steuern.

5. Zusammenfassung

104 Smart Home Devices bestehen aus Hardware- und Softwarekomponenten. Die Software kann ein oder mehrere KI-Systeme enthalten. Dies ist jedoch nicht zwingend. Praktisch jedes Haushaltsgerät kann durch smarte Funktionen, also Funkverbindungen, die bspw. deren Steuerung ermöglichen, zum Smart Home Device entwickelt werden.

105 Vorliegend wird unter «KI» oder «KI-System» Software verstanden, die lernfähig ist. Je nach Verfahren kann das Lernen in der Lernphase oder im laufenden Betrieb, also der Anwendungsphase, erfolgen. In dieser Arbeit ist bei der Bezeichnung «Software» KI mitgemeint. Nach vorliegend vertretener Auffassung sind die Lernfähigkeit bzw. die daraus resultierende Ableitungsfähigkeit und dadurch erreichte Autonomie eines KI-Systems die ausschlaggebenden Kriterien, welche «KI» von herkömmlicher Software abgrenzen.[343] KI ist somit eine Art von Software, die durch selbstständiges Lernen autonom Entscheidungen treffen kann. Da AGI zurzeit technisch nicht umsetzbar ist, ist durchgehend schwache KI gemeint.

106 Die bislang im Produktsicherheitsrecht gängigen Kategorisierungen von Individual- und Standardsoftware sowie Embedded und Stand-alone-Software verschwimmen zunehmend. Trotz der nicht mehr zeitgemässen Unterscheidung zwischen Embedded und Stand-alone-Software wird – wo nötig – weiterhin zwischen diesen Kategorien differenziert.

---

341 Für eine Auswahl von Beispielen siehe auch OECD, Consumer, S. 10.

342 Gemeint ist hier «Safety», da gerade mit dem Internet verbundene Geräte oft Schwachstellen in der «Security» haben. S. o., Rn. 41 und s. u., Rn. 265.

343 Ebenso: Oster, in: Foerste/Westphalen, § 57 Rn. 8; Batache, Rn. 64.

Mittels Updates können Hersteller aus der Ferne Einfluss auf ihre Produkte nehmen. Die Möglichkeit zur Einflussnahme muss technisch explizit eingerichtet werden. Wenn sich ein KI-System durch eigenständige Verarbeitung von Umwelt- oder Nutzungsdaten weiterentwickelt, beruht diese Veränderung nicht auf einem bewussten Eingriff des Herstellers. Eine solche fortlaufende Anpassung durch Lernen in der Anwendungsphase ist daher kein Update im konventionellen Sinne. Die meisten KI-Systeme, die momentan eingesetzt werden, lernen in der Anwendungsphase nicht mehr weiter und sind sozusagen «eingefroren» (Batch-Learning). Sie können jedoch in Form einer neuen Version durch ein Update auch nach der ersten Inbetriebnahme vom Hersteller verändert werden. 107

II. Rechtliche Grundlagen für Software und KI

In diesem Kapitel werden die rechtlichen Grundlagen und die damit einhergehenden Unklarheiten von Software und KI erläutert. Die Entstehungsgeschichte der verschiedenen Versionen der Definition des KI-System in der EU wird dargelegt. Danach wird auf den Stand der Definition des KI-Systems in der Schweiz eingegangen. 108

1. Rechtliche Definition von Software

In der Schweiz ist Software bis anhin in keinem Gesetz definiert. Art. 2 Abs. 3 URG[344] hält fest, dass Werke i.S.d. URG auch Computerprogramme sein können. Dennoch wird das Computerprogramm nicht näher definiert.[345] 109

Vor dem am 10.12.2024 in Kraft getretenen CRA gab es in der EU ebenfalls keine gesetzliche Definition von Software.[346] Verwiesen wurde bis dahin auf die Mustervorschriften der Weltorganisation für geistiges Eigentum[347] sowie ver- 110

344 Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 9. Oktober 1992, SR 231.1 (zit. URG).

345 OFK URG-Rehbinder/Haas/Uhlig, Art. 2 N 31.

346 Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 1, 7; Beck KI-VO-Wendehorst, Art. 3 N 8; siehe auch die Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates (Maschinenverordnung), ABl. L 165/1 (zit. MVO), welche den Begriff Software zwar etliche Male verwendet, ihn aber nicht definiert.

347 Oster, in: Foerste/Westphalen, § 57 Rn. 5 Fn. 13; Bomhard/Schreiber, in: Bomhard et al., § 1 Rn. 7 f. m.w.H.

schiedene Normen[348]. OSTER differenziert zwischen Software i.e.S. und Software i.w.S.[349] Unter Software i.w.S. versteht er alle «digitalen Inhalte», was wiederum als «Oberbegriff für alle Daten in digitaler Form» verwendet wird und elektronische Daten sowie Computerprogramme umfasst.[350] Computerprogramme sind gem. OSTER Software i.e.S. und «werden definiert als eine Folge von Befehlen, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind, zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt».[351] Zu den Computerprogrammen gehören gem. OSTER z.B. «Betriebssysteme, Anwendungsprogramme, Makros, Suchmaschinen, [...] Quellcode[352] sowie einzelne Programmteile».[353] Art. 3 Ziff. 4 CRA definiert Software als «den Teil eines elektronischen Informationssystems, der aus Computercode besteht». Abgegrenzt wird Software damit vom «Produkt mit digitalen Elementen».[354] Vorliegend ist mit Software jeweils Software i.e.S. gemeint. Damit sind nicht alle digitalen Inhalte (wie bspw. reine Daten) erfasst.

2. Diskussionen in der EU um den Inhalt des Begriffs «KI»

111 Schon lange vor dem Inkrafttreten der KI-VO am 1. August 2024 wurde versucht, eine allgemeingültige Definition für KI zu finden. In diesem Unterkapitel soll aufgezeigt werden, welche Schritte zur heute geltenden Definition in der EU führten.

2.1. 2018: Mitteilung der Europäischen Kommission

112 Bereits 2018 versuchte die Europäische Kommission in der Mitteilung «Künstliche Intelligenz für Europa» eine Definition für KI zu finden. Diese lautete:

348 DIN 44300 (1988): BOMHARD/SCHREIBER, in: Bomhard et al., § 1 Rn. 9; OSTER, in: Foerste/Westphalen, § 57 Rn. 5 Fn. 13; ISO 24765:2017: BORGES, Begriff, Rn. 31; WITTIG, S. 28.

349 OSTER, in: Foerste/Westphalen, § 57 Rn. 4 f. m.w.H.

350 OSTER, in: Foerste/Westphalen, § 57 Rn. 4.

351 OSTER, in: Foerste/Westphalen, § 57 Rn. 5.

352 Nach Art. 3 Ziff. 35 MVO bezeichnet der Begriff «Quellcode» «die derzeit installierte Version der Software eines in den Anwendungsbereich dieser Verordnung fallenden Produkts, die in einer Programmiersprache so geschrieben ist, dass sie für den Menschen eindeutig und verständlich ist». Vorliegend wird Quellcode nicht unter den Softwarebegriff subsumiert s. o., Rn. 76.

353 OSTER, in: Foerste/Westphalen, § 57 Rn. 5.

354 S. u., Rn. 235.

> «Künstliche Intelligenz (KI) bezeichnet *Systeme* mit einem ‹intelligenten› Verhalten, die *ihre Umgebung analysieren* und mit einem *gewissen Grad an Autonomie* handeln, um bestimmte *Ziele* zu erreichen.
>
> KI-basierte Systeme können *rein softwaregestützt* in einer virtuellen Umgebung arbeiten (z.B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme), aber auch *in Hardware-Systeme eingebettet* sein (z.B. moderne Roboter, autonome Pkw, Drohnen oder Anwendungen des «Internet der Dinge»)».[355]

Diese Definition bezog sich bereits auf «Systeme» und stellte darauf ab, dass diese «ihre Umgebung analysieren» und in gewisser Hinsicht «autonom» handeln, um ein «Ziel» zu erreichen. Es wurde hervorgehoben, dass KI-Systeme aus Stand-alone-Software («rein softwaregestützt») oder Embedded Software («in Hardwaresysteme eingebettet») bestehen können. 113

2.2. 2018: Hochrangige Expertengruppe für KI

Die Hochrangige Expertengruppe für Künstliche Intelligenz bezog sich auf obengenannte Definition[356] und schlug – ebenfalls 2018 – eine aktualisierte Version vor: 114

> «Artificial intelligence (AI) refers to *systems designed by humans* that, given a *complex goal*, *act* in the physical or digital world *by perceiving their environment*, *interpreting* the collected structured or unstructured *data*, *reasoning* on the *knowledge derived from this data and deciding the best action*(s) to take (according to pre-defined parameters) to achieve the given *goal*. AI systems can also *be designed to learn to adapt* their behaviour by analysing how the environment is affected by their previous actions.
>
> As a *scientific discipline*, AI includes *several approaches and techniques*, such as *machine learning* (of which deep learning and reinforcement learning are specific examples), *machine reasoning* (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and *robotics* (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)».[357]

355 Europäische Kommission, Mitteilung, S. 1.

356 Europäische Kommission, Weissbuch KI, S. 19.

357 High-Level Expert Group on Artificial Intelligence, A definition of AI, S. 7. Eine deutsche (jedoch abweichende) Übersetzung findet sich unter <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Mittelstand/Downloads/Experten.html>, zuletzt besucht am 31.05.2025.

115 Im Gegensatz zur ersten Definition wurde hier hervorgehoben, dass es sich um ein System handelt, welches von Menschen konzipiert («designed») wird. Es wird deutlicher, dass das System seine Umgebung «wahrnimmt» («perceiving»), es die gewonnenen Daten interpretiert und anhand von Vorgaben Entscheidungen («deciding [...] according to pre-defined parameters») trifft. Neu ist, dass hervorgehoben wird, dass KI-Systeme so konfiguriert werden können, dass sie lernen können, ihr Verhalten anzupassen. Ebenfalls werden zusätzlich verschiedene Ansätze und Techniken aufgezählt («machine learning», «machine reasoning» und «robotics»). Dass es sich bei KI um Software handelt, fiel in dieser neuen Definition weg.[358]

2.3. 2020: Weissbuch zur KI

116 2020 umschrieb das «Weissbuch zur Künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen» der Europäischen Kommission KI, legte sich jedoch nicht auf eine Definition fest. Es verweist auf die zwei obengenannten Definitionen und weist drauf hin, dass «die KI-Definition einerseits flexibel genug sein [muss], damit dem technischen Fortschritt Rechnung getragen werden kann, und andererseits präzise, um die erforderliche Rechtssicherheit zu gewährleisten».[359]

2.4. 2021: KI-VO-Entwurf

117 Daraufhin wurde der Entwurf für die KI-VO ausgearbeitet. Der Entwurf der KI-VO[360] wurde am 21. April 2021 veröffentlicht und enthielt folgende Definition:

> «‹System der künstlichen Intelligenz› (KI-*System*) [bezeichnet] eine *Software*, die mit einer oder mehreren der in *Anhang I aufgeführten Techniken und Konzepte* entwickelt worden ist und im Hinblick auf eine Reihe von *Zielen*, die *vom Menschen festgelegt* werden, *Ergebnisse* wie *Inhalte*, *Vorhersagen*, *Empfehlungen oder Entscheidungen* hervorbringen kann, die das *Umfeld beeinflussen*, mit dem sie interagieren».[361]

Zudem führte Anhang I des KI-VO-Entwurfs folgende Techniken und Konzepte auf:

358 Wobei festgehalten wurde, dass der Begriff «KI-System» für jede KI-basierte Komponente verwendet wird («software and/or hardware»). High-Level Expert Group on Artificial Intelligence, A definition of AI, S. 2.

359 Europäische Kommission, Weissbuch KI, S. 19.

360 Europäische Kommission, Vorschlag KI-VO.

361 Europäische Kommission, Vorschlag KI-VO, Art. 3 Ziff. 1.

> «a) Konzepte des *maschinellen Lernens*, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschliesslich des tiefen Lernens (Deep Learning);
>
> b) *Logik- und wissensgestützte Konzepte*, einschliesslich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme;
>
> c) *Statistische Ansätze*, Bayessche Schätz-, Such- und Optimierungsmethoden».[362]

Die Definition des KI-Systems des Entwurfs nahm die Erklärung, dass es sich bei KI-Systemen um Software handelt, wieder auf. Auch auf Techniken und Ansätze wurde in Anhang I detailliert eingegangen. Auch diese Definition bezog sich wieder darauf, dass Menschen Vorgaben machen, die von einem System umgesetzt werden. Es wurde beschrieben, welche Art von Ergebnissen ein KI-System «hervorbringen kann» und dass diese «das Umfeld beeinflussen». Dass ein solches System etwas «interpretiert» oder «analysiert» und «lernen» kann, war nur noch aus Anhang I, jedoch nicht mehr aus der eigentlichen Definition herauszulesen. Dass das System seine Umwelt «wahrnimmt», fiel ganz weg. 118

Die Definition des KI-VO-Entwurfs war stark umstritten.[363] Die Kritik bezog sich vor allem auf den zu grossen Anwendungsbereich, wobei viele «algorithmengesteuerte Verfahren»[364] und eigentlich fast jede Software als KI-System erfasst gewesen wären.[365] Auch der Unterschied zwischen «KI» und «KI-System» war unklar.[366] Die Definition war nicht technologieneutral.[367] Gefordert wurde zudem, dass die Definition näher an diejenige der OECD[368] angelehnt wird, welche 2019 bereits einen technologieneutralen Vorschlag gemacht hatte.[369] Weil Software auf Vorgaben von Menschen basiert und immer irgendwelche Ergebnisse hervorbringt, wurde der zweite Teil der Definition als 119

362 Europäische Kommission, Vorschlag KI-VO, Anhang 1.

363 Beck KI-VO-Wendehorst, Art. 3 N 14; in Bezug auf die ganze KI-VO Borges, Teil 1, Rn. 2.

364 Spindler, Vorschläge, Rn. 70, mit der gleichen Kritik über die Definition im Entwurf einer KI-Haftungsrichtlinie, die mittlerweile zurückgezogen wurde.

365 Bomhard/Merkle, Rn. 7, mit alternativen Lösungsvorschlägen in Rn. 8 f.; Ebers et al., Rn. 6; Kalbhenn, S. 664 f.

366 Ebers et al., Rn. 6; unter KI kann die Disziplin und unter KI-System das entwickelte System verstanden werden, Ziff. 3.1.3 und 3.1.4 ISO 22989:2022.

367 Beck KI-VO-Wendehorst, Art. 3 N 14.

368 S. u., Rn. 121.

369 Siehe auch Beck KI-VO-Wendehorst, Art. 3 N 16, m.w.H.

«Leerformel» bezeichnet, die für die Abgrenzung keinen Mehrwert bietet.[370] Es wurde stattdessen vorgeschlagen, bspw. lediglich Anwendungen, welche auf maschinellem Lernen basieren, als «KI» zu bezeichnen.[371]

2.5. 2022: Popularität generativer KI

120 Ende 2022 gewann generative KI[372] durch den Erfolg von ChatGPT massiv an Popularität.[373] Dies machen bspw. nachfolgende Google-Trends-Statistiken deutlich, die die Suchresultate für «chatgpt» und «generative AI» zeigen:

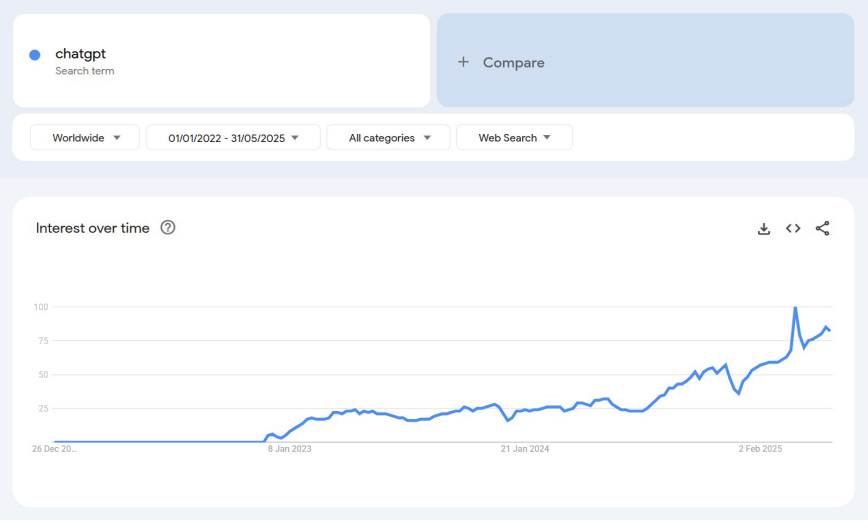

Abbildung 6: *Google Trends Statistik «chatgpt»*[374]

370 ROOS/WEITZ, S. 845.

371 HACKER, Rn. 6; siehe auch Beck KI-VO-WENDEHORST, Art. 3 N 16, m.w.H.

372 S. o., Rn. 88.

373 MOLAVI VASSE'I, S. 192.

374 Google Trends «chatgpt», abrufbar unter <https://trends.google.com/trends/explore?date=2022-01-01%202025-05-31&q=chatgpt&hl=en-GB>, zuletzt besucht am 31.05.2025. Die Zahlen geben das Suchinteresse im Verhältnis zum höchsten Punkt auf dem Diagramm für die jeweilige Region und Zeit an. Ein Wert von 100 entspricht der höchsten Beliebtheit des Begriffs. Ein Wert von 50 bedeutet, dass der Begriff halb so beliebt ist. Ein Wert von 0 bedeutet, dass nicht genügend Daten für diesen Begriff vorliegen.

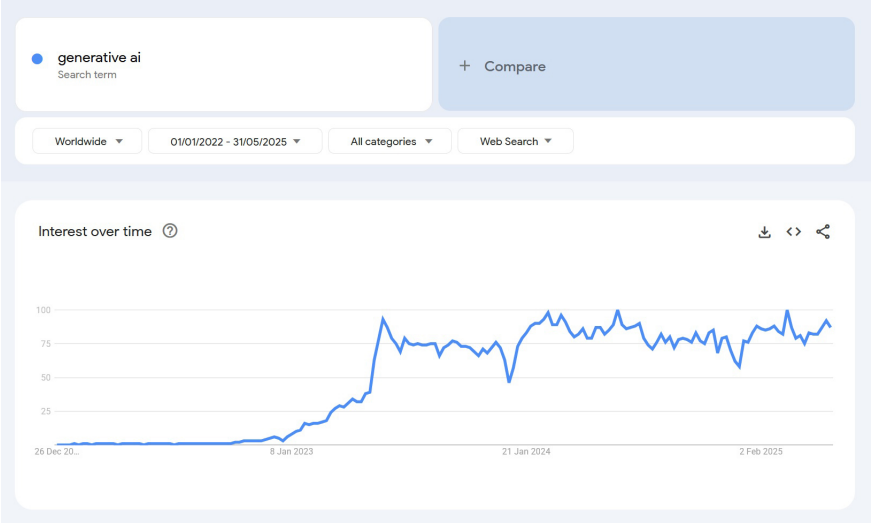

Abbildung 7: *Google Trends Statistik «generative AI»*[375]

Generative KI floss daraufhin ebenfalls in die Diskussionen um die Definition des KI-Systems mit ein.[376]

2.6. 2023: Einigung auf den Kompromisstext

Am 14. Juni 2023 einigte sich das Europäische Parlament[377] auf folgende Definition aus dem Kompromisstext vom 22. Mai 2023[378]: 121

> «‹System der künstlichen Intelligenz› (KI-System) [bezeichnet] ein *maschinengestütztes System*, das so konzipiert ist, dass es mit *unterschiedlichem Grad an Autonomie* operieren kann und das für explizite oder implizite *Ziele Ergebnisse*

375 Google Trends «generative AI», abrufbar unter <https://trends.google.com/trends/explore?date=2022-01-01%202025-05-31&q=generative%20ai&hl=en-GB>, zuletzt besucht am 31.05.2025.

376 Beck KI-VO-Wendehorst, Art. 3 N 15; Beck KI-VO-Martini, Art. 50 N 112.

377 Europäisches Parlament, Abänderung Gesetz über KI, Abänderung 165 Vorschlag für eine Verordnung Art. 3 Abs. 1 Ziff. 1; siehe auch Parlament bereit für Verhandlungen über Regeln für sichere und transparente KI, abrufbar unter <https://www.europarl.europa.eu/news/de/press-room/20230609IPR96212/parlament-bereit-fur-verhandlungen-uber-regeln-fur-sichere-und-transparente-ki>, zuletzt besucht am 31.05.2025.

378 Europäisches Parlament, Bericht Vorschlag KI-VO, Änderungsantrag 165 Vorschlag für eine Verordnung Art. 3, Abs. 1, Ziff. 1.

> wie Vorhersagen, Empfehlungen oder Entscheidungen *hervorbringen* kann, die das physische oder virtuelle *Umfeld beeinflussen*».

Diese Definition, welche an die Definition der OECD von 2019 angelehnt war, enthielt keine Einschränkungen mehr auf bestimmte Technologien.[379]

2.7. 2024: Finale Version der KI-VO

122 Da die OECD ihre Definition am 8. November 2023 aktualisierte,[380] wurde auch die Definition der KI-VO nochmals angepasst.[381] Die Definition der OECD und der KI-VO sind deshalb ähnlich.[382] Nach vielen Diskussionen[383] einigte man sich in der am 1. August 2024 in Kraft getretenen finalen Version der KI-VO endlich über eine Definition für den Begriff «KI-System». Gestützt auf Art. 96 Abs. 1 lit. f KI-VO hat die Europäische Kommission am 6. Februar 2025 Leitlinien, die der Erleichterung der «Anwendung der Definition eines KI-Systems» nach Art. 3 Ziff. 1 KI-VO dienen sollen, erlassen.[384] Die Leitlinien sind nicht rechtsverbindlich und dienen als Auslegungshilfe.[385] Aufgrund der relativ unscharfen[386] Definition des KI-Systems in der KI-VO wurde angenommen, dass der Anwendungsbereich faktisch in diesen Leitlinien definiert werden würde.[387] Obwohl die Leitlinien wenigstens einige Beispiele liefern, bleibt die Definition des KI-Systems weiterhin unscharf.[388] Im Folgenden wird anhand der nun geltenden Definition aufgezeigt, dass sich die Abgrenzung zu traditioneller Software weiterhin schwierig gestaltet.

---

379 Siehe auch Beck KI-VO-Wendehorst, Art. 3 N 16; sie enthielt jedoch weiterhin Verweise auf verschiedene Techniken, bspw. in Europäisches Parlament, Bericht Vorschlag KI-VO, ErwG 6a.

380 OECD, Explanatory Memorandum, S. 4.

381 Siehe auch Beck KI-VO-Wendehorst, Art. 3 N 17, m.w.H.; und Molavi Vasse'i, S. 193.

382 Rosenthal, Jusletter 05.08.2024, Rn. 17.

383 Zu den Schritten des Gesetzgebungsverfahrens siehe Europäisches Parlament, Gesetzgebungsverfahren KI-VO.

384 Die Kommission veröffentlicht Leitlinien zur Definition von KI-Systemen, um die Anwendung des ersten KI-Gesetzes zu erleichtern, abrufbar unter <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>, zuletzt besucht am 31.05.2025.

385 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 7; Beck KI-VO-Hartmann, Art. 96 N 1 f.; konkret zu Art. 3 Ziff. 1 Beck KI-VO-Wendehorst, Art. 3 N 13.

386 Rosenthal, Jusletter 05.08.2024, Rn. 17.

387 Beck KI-VO-Wendehorst, Art. 3 N 51.

388 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 6, 62; siehe auch Molavi Vasse'i, S. 190, 193 f.

a. Definition des KI-Systems nach der KI-VO

Die nun geltende KI-VO definiert das «KI-System» als 123

> «ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können».[389]

Die Leitlinien zur KI-Definition identifizieren daraus folgende sieben Hauptelemente, auf welche sogleich eingegangen wird: 1) maschinenbasiertes System, 2) Autonomie, 3) Anpassungs- bzw. Lernfähigkeit, 4) Ziele des KI-Systems, 5) Ableitungsfähigkeit, 6) Resultate die die Umwelt beeinflussen können und 7) Interaktion mit der Umwelt. Es müssen nicht alle Elemente der Definition gleichzeitig während der zwei Phasen (Lernphase / «building phase» vor der Inbetriebnahme und Anwendungsphase / «use phase» danach) des Lebenszyklus des KI-Systems vorhanden sein.[390]

Ein «maschinengestütztes System» hat immer eine technische Komponente.[391] 124
«Quantum computing systems», biologische und organische Systeme sind gem. Leitlinie ebenso mitgemeint.[392] Weggefallen ist in der Definition (leider) die Feststellung, dass es sich bei einem KI-System um Software handelt.[393] Da KI-Systeme nach der KI-VO immer Software sind,[394] gilt die KI-VO nicht für körperliche Produkte wie z.B. die Hardware,[395] in welche das KI-System integriert[396] ist oder

389 Art. 3 Ziff. 1 KI-VO.

390 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 10.

391 Beck KI-VO-Wendehorst, Art. 3 N 19; siehe auch ErwG 12 KI-VO: «Die Bezeichnung ‹maschinenbasiert› bezieht sich auf die Tatsache, dass KI-Systeme von Maschinen betrieben werden».

392 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 13; siehe auch Beck KI-VO-Wendehorst, Art. 3 N 20, mit gegenteiliger Interpretation vor Veröffentlichung der Leitlinie und entsprechender Kritik und weiteren Hinweisen.

393 Siehe im Detail Borges, Begriff, Rn. 28 ff., insbesondere Rn. 56; Borges, Teil 1, Rn. 74.

394 Borges, Teil 1, Rn. 74; Beck KI-VO-Ruschemeier, Art. 6 N 40; mit Bezug auf den KI-VO Vorschlag: Borges, Begriff, Rn. 48; Bomhard/Merkle, Rn. 5; gemäss verwendeter Beispiele wohl ebenso Rosenthal, Jusletter 05.08.2024, Rn. 15; a.A. Ritter/Schaa, S. 32. S. o., Rn. 91.

395 Borges, Teil 1, Rn. 75.

396 Nennt diese «embedded AI systems» Borges, Begriff, Rn. 46, m.w.H.

auf welcher das KI-System «läuft».[397] Das Produkt mit dem integrierten KI-System wird als Ganzes auch nicht zum KI-System.[398]

125 Obwohl die Leitlinien zur KI-Definition die Elemente «Autonomie» und «Ableiten» unabhängig voneinander behandeln, müssen diese zusammen gelesen werden.[399] Ein KI-System muss Ausgaben aufgrund von Eingaben ableiten können.[400] Es handelt sich dabei um eine zwingende Voraussetzung,[401] wobei aber begrenzt ableitungsfähige Systeme von der KI-Definition ausgeschlossen sein sollen aufgrund ihrer limitierten Fähigkeiten, Muster zu analysieren und ihren Output autonom anzupassen.[402] Ein grosser Teil der Lehre sprach sich vor Erscheinen der Leitlinie dafür aus, dass das KI-System die Regeln, *wie* es ableitet, selbst erzeugen muss.[403] Es sollte also «nicht nur die Ausgaben selbst ableite[n], sondern auch den Weg, wie es zu diesen Ausgaben kommt».[404] Diese Erzeugung der Ableitungsregeln erfolgt durch die Nutzung von maschinellem Lernen[405] in der «building phase».[406] Da jedoch auch logik- und wissensgestützte Ansätze als KI-Systeme erfasst sein sollen,[407] muss sich «Ableiten»

397 Die Hard- und Softwarekomponenten ermöglichen lediglich das Funktionieren des KI-Systems, Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 11.

398 Borges, Teil 1, Rn. 75; Borges, Begriff, Rn. 48; wohl ebenfalls Ritter/Schaa, S. 33; a.A. Beck KI-VO-Wendehorst, Art. 3 N 22 f.

399 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 15; siehe auch Vasella, EU-Kommission: Leitlinien zum Begriff des AI-Systems, abrufbar unter <https://datenrecht.ch/eu-kommission-leitlinien-zum-begriff-des-ai-systems/>, zuletzt besucht am 31.05.2025: «Die Kommission stellt klar, dass das Kriterium der Autonomie und der Ableitung von Output zusammenhängen, weil sich die Autonomie auf diese Ableitung bezieht. Entsprechend ist richtigerweise von einem und nicht zwei Kriterien auszugehen, aber klar wird dies bei der Kommission nicht».

400 Art. 3 Ziff. 1, ErwG 12 KI-VO; Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 26.

401 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 26.

402 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 41 und Beispiele in ErwG 42 ff.; siehe auch mit Kritik Molavi Vasse'i, S. 194 f.; Vasella hält fest, dass es sich bei den Ergänzungen durch die Leitlinie um eine Bagatellschwelle handelt, Vasella, EU-Kommission: Leitlinien zum Begriff des AI-Systems, abrufbar unter <https://datenrecht.ch/eu-kommission-leitlinien-zum-begriff-des-ai-systems/>, zuletzt besucht am 31.05.2025.

403 Ritter/Schaa, S. 35; Rosenthal, Jusletter 05.08.2024, Rn. 15; Thouvenin et al., Jusletter IT 04.07.2024, Rn. 25; Stiemerling, Rn. 27; Borges, Teil 1, Rn. 66 f.

404 Beck KI-VO-Wendehorst, Art. 3 N 44.

405 ErwG 12 KI-VO; Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 32 ff.; Rosenthal, Jusletter 05.08.2024, Rn. 14; Stiemerling, Rn. 23, 27; Borges, Teil 1, Rn. 65, 67.

406 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 30 f.

407 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 39.

auch auf die Anwendungsphase beziehen.[408] Ein KI-System muss gem. ErwG 12 KI-VO «zu einem gewissen Grad» ohne menschlichen Einfluss funktionieren.[409] Als «Autonomie» wird von einem Teil der Lehre die Eigenschaft des KI-Systems genannt, Output durch Ableitung zu generieren.[410] Anders als die zitierten Lehrmeinungen ist das Verständnis der Europäischen Kommission: Gem. der Leitlinien geht es bei «Autonomie» um die Fähigkeit, mit der Umwelt zu interagieren, und darum, inwieweit das KI-System unabhängig von einer menschlichen Interaktion agieren kann.[411, 412] Abhängig davon, wie Autonomie verstanden wird, sind bspw. reine «Expertensysteme», die komplett von Menschen programmiert wurden, von der KI-VO nicht[413] oder eben doch[414] als KI-System erfasst.

Art. 3 Ziff. 1 KI-VO hält weiter fest, dass ein KI-System «nach seiner Betriebsaufnahme anpassungsfähig sein kann». Diese Lernfähigkeit[415] muss jedoch während der Verwendung («use phase») nicht jederzeit möglich sein.[416] An- 126

408 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 31, «the concept of ‹inference› should be understood in a broader sense as encompassing the ‹building phase› of the AI system»; mit dem Hinweis, dass der Gesetzgeber nicht nur Anwendungen maschinellen Lernens erfassen wollte, obwohl sich die Erfassung von logik- und wissensgestützten Systemen nicht mehr mit der Formulierung vereinbaren lasse «wonach KI-Systeme ableiten, ‹wie› Ausgaben erstellt werden», Beck KI-VO-Wendehorst, Art. 3 N 46.

409 ErwG 12 KI-VO; Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 17; siehe dazu die Kritik (vor Publikation der Leitlinie) in Beck KI-VO-Wendehorst, Art. 3 N 29, weil «hier allerdings jedes algorithmische System darunterfallen» könne und «unterschiedlicher Grad» auch «den Grad Null» erfasse.

410 Borges, Teil 1, Rn. 66; Rosenthal, Jusletter 05.08.2024, Rn. 14 f., siehe auch den Hinweis auf Arioli, dass das Gleiche gemeint sei, aber nicht «Autonomie» genannt wird; im Ergebnis gleich, aber mit anderer Bezeichnung Arioli, Jusletter IT 04.07.2024, Rn. 7 Fn. 4.

411 ErwG 12 KI-VO, «sollte sich nicht auf Systeme beziehen, die auf ausschliesslich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen»; Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 16, 19; Ritter/Schaa, S. 33; siehe vor Erscheinen der Leitlinie auch Beck KI-VO-Wendehorst, Art. 3 N 29 f.

412 Die oben vertretene Definition von Autonomie in Rn. 100 entspricht somit nicht der Meinung der Europäischen Kommission.

413 Rosenthal, Jusletter 05.08.2024, Rn. 14; ebenso Feiler/Forgó, Art. 3 N 10; siehe auch das Beispiel von Stiemerling, Rn. 22.

414 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 18, 39; Beck KI-VO-Wendehorst, Art. 3 N 41, 58, welche sich zugunsten der Technologieneutralität allgemein für ein breites Verständnis von KI-System ausspricht, N 6.

415 ErwG 12 KI-VO.

416 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 10, 23; mit ausführlicher Diskussion Beck KI-VO-Wendehorst, Art. 3 N 32 ff.

sonsten wären KI-Systeme, mit Batch-Learning[417], die nach dem Lernen eingefroren werden, nicht von der Definition des KI-Systems erfasst.[418]

127 KI-Systeme sind so konzipiert, dass sie auf der Grundlage bestimmter Ziele arbeiten, die entweder explizit oder implizit festgelegt sind.[419] Explizite Ziele sind vom Entwickler klar definierte Vorgaben, wie z.B. die Optimierung einer Kostenfunktion.[420] Implizite Ziele lassen sich aus dem Verhalten oder den zugrundeliegenden Annahmen des Systems ermitteln, ohne dass diese ausdrücklich formuliert sind.[421] Die Ziele des KI-Systems können sich von der Zweckbestimmung nach Art. 3 Ziff. 12 KI-VO unterscheiden.[422]

128 Zudem muss das KI-System ein Resultat oder eine Ausgabe[423] («output») hervorbringen, welches einen Einfluss[424] auf die Umgebung[425] hat.[426] Diese Resultate können Einfluss auf eine physische Umgebung (z.B. die Erwärmung eines Ofens) oder Einfluss anhand von Ausgaben, die als Eingaben für ein anderes System verwendet werden,[427] haben, sowie die Beeinflussung eines Menschen[428] sein. Die Ausgaben werden in vier verschiedene Kategorien eingeteilt: Vorhersagen, Inhalte, Empfehlungen und Entscheidungen.[429] Diese sind nicht abschliessend.[430] Gem. Leitlinien zur Definition des KI-Systems handelt es sich bei der Generierung von Resultaten um eine fundamentale Fähigkeit von KI-Systemen und unterscheidet diese von herkömmlicher Software.[431] Dieser Ansicht kann nicht gefolgt werden.[432] Es handelt sich auch bei der Beeinflussung

417 S. o., Rn. 97.

418 Beck KI-VO-Wendehorst, Art. 3 N 33, m.w.H.; ebenso Rosenthal, Jusletter 05.08.2024, Rn. 13.

419 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 24.

420 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 24.

421 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 24.

422 ErwG 12 KI-VO; Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 25.

423 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 52.

424 Zum Begriff der «Beeinflussung» siehe Borges, Begriff, Rn. 92 ff.

425 Zum Begriff der «Umgebung» siehe Borges, Begriff, Rn. 91.

426 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 60; Borges, Begriff, Rn. 107; a.A. Beck KI-VO-Wendehorst, Art. 3 N 42, welche den Einfluss auf die Umgebung nicht für ein hilfreiches Abgrenzungskriterium hält.

427 Beck KI-VO-Wendehorst, Art. 3 N 40.

428 Beck KI-VO-Wendehorst, Art. 3 N 41; Borges, Begriff, Rn. 104, 107.

429 Art. 3 Ziff. 1 KI-VO; Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 53.

430 Beck KI-VO-Wendehorst, Art. 3 N 39.

431 Europäische Kommission, Leitlinien Definition KI-System (Stand 06.02.25), ErwG 52.

432 Wobei zumindest die Komplexität des Outputs ein Indiz dafür sein könne, ob es sich um ein KI-System handle oder nicht. Mit Verweis auf ErwG 59 der Leitlinie siehe Vasella,

der Umgebung nicht um ein nützliches Abgrenzungskriterium,[433] da jede Software immer einen Einfluss auf ihre Umgebung hat.[434]

Insgesamt ist noch immer nicht in jedem Fall klar, wie sich herkömmliche Software genau von einem KI-System abgrenzen lässt. Auf eine klare Abgrenzung zwischen «traditioneller» Software und einem KI-System im Sinne der KI-VO muss also weiterhin gewartet werden.[435] 129

b. Abgrenzung zum KI-Modell

Die in der KI-VO beschriebenen KI-Modelle sind das «Herzstück» des eigentlichen KI-Systems. Es wird auch als «Kern»[436] des KI-Systems bezeichnet, der den Lernmechanismus[437] bzw. die Anpassungsfähigkeit sowie die (Teil-)Autonomie[438] des KI-Systems ermöglicht. WENDEHORST hält fest, dass «ein KI-Modell sich auf einen spezifischen Algorithmus, der für die Durchführung einer bestimmten Aufgabe oder eine Gruppe von Aufgaben entwickelt wurde»[439] bezieht. Der Begriff «KI-Modell» wird in der KI-VO nicht definiert.[440] In ErwG 97 finden sich jedoch hilfreiche Anhaltspunkte. So wird festgehalten, dass «KI-Modelle wesentliche Komponenten von KI-Systemen sind» und in diese integriert werden.[441] Selbst sind sie aber keine KI-Systeme.[442] KI-Modelle können zu KI-Systemen werden, wenn weitere Komponenten wie bspw. Nutzerschnittstellen hinzugefügt werden.[443] Ein KI-System besteht häufig aus meh- 130

EU-Kommission: Leitlinien zum Begriff des AI-Systems, abrufbar unter <https://datenrecht.ch/eu-kommission-leitlinien-zum-begriff-des-ai-systems/>, zuletzt besucht am 31.05.2025; siehe auch (vor Publikation der Leitlinie) ROSENTHAL, Jusletter 05.08.2024, Rn. 12.

433 Beck KI-VO-WENDEHORST, Art. 3 N 42; a.A. BORGES, Begriff, Rn. 107.

434 ROSENTHAL, Jusletter 05.08.2024, Rn. 12.

435 Siehe auch BORGES, Teil 1, Rn. 65, welcher die Definition als «komplex und mehrdeutig» bezeichnet; ähnlich ROSENTHAL, Jusletter 05.08.2024, Rn. 11, 16; ebenso Beck KI-VO-WENDEHORST, Art. 3 N 50 ff. welche eine alternative Systematisierung vorschlägt; a.A. wohl STIEMERLING, Rn. 28, der die Definition als «eng» und «zielführend» bezeichnet.

436 Beck KI-VO-BERNSTEINER/SCHMITT, Art. 51 N 11; STIEMERLING, Rn. 12; KASPER, Jusletter 23.09.2024, Rn. 19.

437 STIEMERLING, Rn. 12.

438 Beck KI-VO-BERNSTEINER/SCHMITT, Art. 51 N 11.

439 Beck KI-VO-WENDEHORST, Art. 3 N 26.

440 Siehe auch Beck KI-VO-WENDEHORST, Art. 3 N 25; ebenso Beck KI-VO-BERNSTEINER/SCHMITT, Art. 51 N 11.

441 ErwG 97 KI-VO.

442 ErwG 97 KI-VO.

443 ErwG 97 KI-VO.

reren KI-Modellen und weiteren Komponenten.[444] Bekannte KI-Modelle können z.B. Texte generieren und analysieren (GPT von Open AI) oder Bilder (Midjourney von Open AI, Bing Image Creator von Microsoft) oder sogar Videos (Sora von Open AI) aufgrund von Texten generieren.[445]

131 Während das KI-System bspw. eine Nutzeroberfläche hat, damit ein Nutzer damit interagieren (bspw. einen «Prompt» eingeben) kann, liegt das KI-Modell normalerweise «versteckt» im Hintergrund und macht das, was sich wie «Intelligenz» anfühlt, erst möglich. Zum Beispiel ist ChatGPT ein KI-System und GPT[446] das KI-Modell dahinter, welches aufgrund der Eingaben des Nutzers (Prompts) Ausgaben generiert.[447]

c. *Abgrenzung zum KI-System und zum KI-Modell mit allgemeinem Verwendungszweck*

132 Die KI-VO regelt zudem KI-Systeme mit allgemeinem Verwendungszweck (engl. «General Purpose AI», kurz «GPAI»). Diese basieren gem. Art. 3 Ziff. 66 KI-VO auf KI-Modellen mit allgemeinem Verwendungszweck[448] (engl. «General Purpose AI Model», kurz «GPAIM»), auch «Basismodelle» (engl. «Foundation Models») genannt[449]. Es handelt sich bei GPAI um eine Unterkategorie von KI-Systemen.[450] Der Unterschied von KI-Systemen mit allgemeinem Verwendungszweck zu anderen KI-Systemen besteht darin, dass sie auf Basismodellen beruhen und «in der Lage [sind], einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen».[451] GPAI können generative KI beinhalten, müssen dies aber nicht.[452] Dies

444 Beck KI-VO-Wendehorst, Art. 3 N 26.

445 Siehe auch Beck KI-VO-Bernsteiner/Schmitt, Art. 51 N 12, m.w.H.

446 Website OpenAI Platform, abrufbar unter <https://platform.openai.com/docs/models>, zuletzt besucht am 31.05.2025.

447 Ähnlich Beck KI-VO-Bernsteiner/Schmitt, Art. 51 N 13.

448 Welches wiederum in Art. 3 Ziff. 63 KI-VO definiert ist als «ein KI-Modell – einschliesslich der Fälle, in denen ein solches KI-Modell mit einer grossen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden».

449 Beck KI-VO-Martini, Art. 50 N 59; siehe auch Borges, Begriff, Rn. 11 f.

450 Art. 3 Ziff. 66 KI-VO; siehe auch Beck KI-VO-Martini, Art. 50 N 61.

451 Art. 3 Ziff. 66 KI-VO; siehe auch Beck KI-VO-Hartmann, Art. 75 N 4.

452 In ErwG 99 KI-VO werden «grosse generative KI-Modelle» als «typisches Beispiel für ein KI-Modell mit allgemeinem Verwendungszweck» genannt; siehe auch Krönke, S. 529.

hängt von den Zielen und Anforderungen ab, die das GPAI-System erfüllen soll. GPT-4, welches übersetzen, Fragen beantworten und Texte generieren kann, ist bspw. ein KI-Modell mit allgemeinem Verwendungszweck.[453]

Werden «Modelle mit mindestens einer Milliarde Parametern, die mit einer grossen Datenmenge unter umfassender Selbstüberwachung trainiert», gelten sie als KI-Modelle mit allgemeinem Verwendungszweck.[454] Die Abgrenzung von GPAIM ist relevant, da für ihre Anbieter zusätzliche Pflichten[455] gelten und GPAIM in vielen verschiedenen Systemen zur Anwendung kommen und dadurch ein erhöhtes Risiko[456] darstellen können. Weitere zusätzliche Bestimmungen, insbesondere eine Meldepflicht für Informationen über schwerwiegende Vorfälle, bestehen für KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko.[457] 133

3. Diskussionen in der Schweiz auf Bundesebene um den Inhalt des Begriffs «KI»

Im Gegensatz zur EU hat die Schweiz KI bis anhin noch nicht spezifisch reguliert und es existiert deshalb noch keine rechtlich verbindliche Definition für KI-Systeme.[458] Die KI-VO und damit die darin enthaltene Definition sind für die Schweiz rechtlich nicht bindend.[459] Das schweizerische Recht ist grundsätzlich technologieneutral ausgestaltet, weshalb der geltende Rechtsrahmen auch auf KI-Systeme angewandt werden kann.[460] Trotzdem zeigen die vielen parlamentarischen Vorstösse zum Thema KI, dass es sich um ein intensiv dis- 134

453 Schwenke, S. 207.

454 ErwG 98 KI-VO.

455 Art. 53 KI-VO.

456 Weltersbach/Aslan, S. 52; Arioli, Jusletter IT 04.07.2024, Rn. 5.

457 Gem. Art. 55 Abs. 1 lit. c KI-VO s. u., Rn. 374. Ein «systemisches Risiko» wird definiert als «ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in grossem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können», Art. 3 Ziff. 65 KI-VO.

458 BJ, Rechtliche Basisanalyse KI, S. 19.

459 BJ, Rechtliche Basisanalyse KI, S. 90; wieso das BGer auf die KI-VO verweist, ist deshalb fraglich, BGer 1C_63/2023 vom 17.10.2024, E. 4.5.4 mit Hinweis auf die Definition des KI-Systems in E. 4.6.

460 BJ, Rechtliche Basisanalyse KI, S. 19; bereits Bundesrat, Leitlinien, S. 9.

kutiertes Thema handelt und Regulierung in verschiedenen Bereichen thematisiert wird.[461]

135 In der Schweiz veröffentlichte die interdepartementale Arbeitsgruppe «Künstliche Intelligenz» am 13. Dezember 2019 einen Bericht an den Bundesrat mit dem Titel «Herausforderungen der künstlichen Intelligenz».[462] Im Bericht wurde auf eine Definition von KI verzichtet, mit der Begründung, dass «eine allgemein gültige und akzeptierte Definition» nicht existiere.[463] Stattdessen wurde auf die Auswirkungen von KI-Anwendungen abgestellt, um herauszufinden, ob seitens Bund Handlungsbedarf aufgrund des vermehrten Einsatzes von KI besteht.[464] In den Leitlinien «Künstliche Intelligenz» für den Bund vom 25. November 2020, welche auf der Grundlage des Berichts «Herausforderungen der künstlichen Intelligenz» vom 13. Dezember 2019 erarbeitet wurden, wird KI lediglich als «Grundlagentechnologie» bezeichnet. Definiert wird KI ebenfalls nicht.[465] Das vom Kompetenznetzwerk für künstliche Intelligenz (CNAI) erstellte Dokument «Terminologie» vom 21. Dezember 2021 definierte KI, KI-System, KI-Entscheidungen und KI-Technologie jeweils separat.[466] Die Definition des KI-Systems deckte sich inhaltlich mit jener des Kompromissvorschlags vom 22. Mai 2023 für den KI-VO-Entwurf der EU. Die Definition des KI-Systems in der neueren Version 2.1 vom 21. Dezember 2023 orientiert sich hingegen an der finalen, in Kraft getretenen Version der KI-VO.[467] Diese Definitionen sind jedoch rechtlich nicht bindend, sondern dienen primär der erleichterten Kommunikation.[468]

136 Der Bundesrat beauftragte am 22. November 2023 das Bundesamt für Kommunikation und das EDA, «eine Auslegeordnung über mögliche Ansätze zur Regulierung des Einsatzes von KI auszuarbeiten».[469] Statt Ende 2024 lag diese Auslege-

461 Motion 25.3396 vom 21.03.2025, Arslan/Nationalrat, Massnahmen zum Schutz der Nachhaltigkeit in die Vernehmlassungsvorlage zur KI-Regulierung aufnehmen; Interpellation 24.4178 vom 27.09.2024, Chappuis/Nationalrat, Zulassung von KI-Systemen für den allgemeinen Gebrauch auf dem Schweizer Markt; Interpellation 24.4091 vom 26.09.2024, Blunschy/Nationalrat, Wo steht die Schweiz im Bereich Daten- und KI-Kompetenz?; Interpellation 15.3446 vom 06.05.2015, Markwalder/Nationalrat, Neue Technologien und autonome Apparate. Rechtliche Rahmenbedingungen für die Haftung.

462 SBFI, KI Bericht.

463 SBFI, KI Bericht, S. 7, 19.

464 SBFI, KI Bericht, S. 17, 20.

465 Bundesrat, Leitlinien, S. 2.

466 Geschäftsstelle CNAI, Terminologie Version 1.0, S. 7.

467 Geschäftsstelle CNAI, Terminologie Version 2.1, S. 7.

468 Geschäftsstelle CNAI, Terminologie Version 2.1, S. 3.

469 Bundesrat prüft Regulierungsansätze für Künstliche Intelligenz, abrufbar unter <https://www.news.admin.ch/de/nsb?id=98791>, zuletzt besucht am 31.05.2025.

ordnung am 12. Februar 2025 inklusive rechtlicher Basisanalyse[470], sektorieller Analyse[471] und Länderanalyse[472] der Öffentlichkeit vor.[473] Gestützt auf die Auslegeordnung entschied sich der Bundesrat für eine eigenständige schweizerische Herangehensweise an die Regulierung von KI. Dabei verfolgt er insbesondere drei Ziele: «Stärkung des Innovationsstandorts Schweiz, […] Wahrung des Grundrechtsschutzes inklusive der Wirtschaftsfreiheit sowie […] Stärkung des Vertrauens der Bevölkerung in KI».[474] Dazu soll die KI-Konvention des Europarates ratifiziert und – möglichst sektoriell – ins Schweizer Recht übernommen werden.[475] Zusätzlich werden freiwillig umzusetzende Massnahmen erarbeitet.[476] Für die Auslegeordnung wurde die KI-Definition des Europarates verwendet, welche fast mit der Definition der OECD vom 08. November 2023 übereinstimmt,[477] welche wiederum sehr ähnlich wie die Definition der KI-VO ist.[478] Die Schweiz ist ebenfalls Teil der OECD.[479] Die OECD bietet der Schweiz eine internationale Plattform, um ihre Interessen zu vertreten, und macht u.a. die Beteiligung an der Entwicklung von globalen Standards möglich.[480]

Am 17. Mai 2024 hat der Europarat ein Übereinkommen über KI verabschiedet. Die Schweiz ist Mitglied des Europarates[481] und hat an den Verhandlungen mitgewirkt.[482] Mit dem Übereinkommen wird ein rechtsverbindlicher Rahmen 137

470 BJ, Rechtliche Basisanalyse KI.

471 BAKOM, Überblick Sektorregulierung KI.

472 BAKOM, Länderanalyse KI.

473 KI-Regulierung: Bundesrat will Konvention des Europarats ratifizieren, abrufbar unter <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-104110.html>, zuletzt besucht am 31.05.2025.

474 BAKOM, Auslegeordnung KI, S. 20.

475 Künstliche Intelligenz, abrufbar unter <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/ki_leitlinien.html>, zuletzt besucht am 31.05.2025.

476 Künstliche Intelligenz, abrufbar unter <https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/ki_leitlinien.html>, zuletzt besucht am 31.05.2025.

477 BAKOM, Auslegeordnung KI, S. 6.

478 S. o., Rn. 122.

479 OECD member Switzerland, abrufbar unter <https://www.oecd.org/en/countries/switzerland.html>, zuletzt besucht am 31.05.2025.

480 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), abrufbar unter <https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/internationale_organisationen/oecd.html>, zuletzt besucht am 31.05.2025.

481 Europarat, abrufbar unter <https://www.eda.admin.ch/eda/de/home/aussenpolitik/internationale-organisationen/europarat.html>, zuletzt besucht am 31.05.2025.

482 Europaratskonvention zu KI unter Mitarbeit der Schweiz verabschiedet, abrufbar unter <https://www.news.admin.ch/de/nsb?id=101063>, zuletzt besucht am 31.05.2025.

für KI-Systeme festgelegt. Dieser gewährleistet insbesondere die Einhaltung der menschenrechtlichen, demokratischen und rechtsstaatlichen Normen des Europarates sowie weiterer relevanter internationaler Standards bei der Entwicklung und Anwendung von KI-Systemen.[483] Die Schweiz hat die Konvention am 27. März 2025 unterzeichnet und bereitet nun die nötigen Anpassungen verschiedener Gesetze vor.[484] Bis Ende 2026 soll diesbezüglich eine Vernehmlassungsvorlage vorliegen und ein Umsetzungsplan für die freiwilligen Massnahmen ausgearbeitet werden.[485]

4. Fazit

138 Da es bis auf die Definition im CRA keine rechtliche Definition für Software gibt, wird vorliegend davon ausgegangen, dass Software eine Folge von Befehlen bezeichnet, welche nach Speicherung auf einem maschinenlesbaren Träger bewirkt, dass eine informationsverarbeitende Maschine eine bestimmte Funktion oder Aufgabe ausführt oder ein definiertes Ergebnis erzielt oder anzeigt.[486]

139 Der sachliche Geltungsbereich der KI-VO umfasst KI-Systeme und KI-Modelle. Davon abgegrenzt werden KI-Systeme mit allgemeinem Verwendungszweck sowie KI-Modelle mit allgemeinem Verwendungszweck. Zusätzlich werden KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko reguliert.

140 Im Rahmen der Erarbeitung der KI-VO wurde intensiv über die Definition des KI-Systems diskutiert. Während die Definition für KI anfangs sehr weit war und entsprechend fast jede Software darunter gefallen wäre,[487] fand man letztlich einen Konsens über eine engere Bezeichnung.[488] Die KI-VO definiert nicht «KI» an sich, sondern enthält in Art. 3 Ziff. 1 KI-VO eine Definition für «KI-System». Die Abgrenzung von traditioneller Software zu KI-Systemen kann sich jedoch – je nach Fall – immer noch schwierig gestalten. Die Diskussionen und vielen Änderungen der Definition zeigen, dass es komplex ist, KI von her-

483 Europaratskonvention zu KI unter Mitarbeit der Schweiz verabschiedet, abrufbar unter <https://www.news.admin.ch/de/nsb?id=101063>, zuletzt besucht am 31.05.2025.

484 Schweiz unterzeichnet Europaratskonvention zu KI, abrufbar unter <https://www.news.admin.ch/de/nsb?id=104646>, zuletzt besucht am 31.05.2025.

485 Schweiz unterzeichnet Europaratskonvention zu KI, abrufbar unter <https://www.news.admin.ch/de/nsb?id=104646>, zuletzt besucht am 31.05.2025.

486 Angelehnt an Oster, s. o., Rn. 110.

487 S. o., Rn. 119.

488 S. o., Rn. 123.

kömmlicher Software zu unterscheiden. Die Grenzen sind nicht immer scharf.[489] Das bedeutet, dass es sich bei der Definition des KI-Systems in der KI-VO nicht um die einzige Möglichkeit handeln muss, KI zu definieren.[490] Obwohl noch unklar ist, ob die EU künftig weiter auf die Definition des KI-Systems gem. Art. 3 Ziff. 1 KI-VO abstellt,[491] scheint sich jene Definition i.V.m. den Definitionen der OECD und des Europarates trotzdem bereits jetzt durchzusetzen.[492] Während sich die Definitionen des KI-Systems der KI-VO, der OECD und des Europarates sehr ähnlich sind, entfernt sich die Leitlinie der Europäischen Kommission davon und engt sie ein.[493] Dies kann negativ als Einschränkung der internationalen Kohärenz[494] wie auch positiv als willkommene Bagatellschwelle[495] empfunden werden. Es ist naheliegend, die Definition des KI-Systems der drei ähnlichen internationalen Definitionen der KI-VO, der OECD und des Europarates als Anhaltspunkt zu verwenden, wenn davon ausgegangen wird, dass die Schweiz ein europakompatibles Produktsicherheitsrecht verfolgen möchte. Die Schweiz befindet sich mitten im Regulierungsprozess für KI. Die Regulierung von KI soll in der Schweiz – wo möglich – technologieneutral ausgestaltet werden.[496] Es wird vor zu umfassender Regulierung gewarnt und als Chance gesehen, dass bislang nicht reguliert wurde und allein in der Schweiz tätige Unternehmen momentan nicht gezwungen sind, Änderungen an ihrer Geschäftstätigkeit vorzunehmen.[497]

489 S. o., Rn. 87.

490 Siehe auch: Anhang I, Teil A, Ziff. 5 und 6 MVO, wo auf Sicherheitsbauteile und Maschinen eingegangen wird, die mit «selbstentwickelndem Verhalten unter Verwendung von Ansätzen des maschinellen Lernens» ausgestattet sind; ErwG 13 PLD 2024, welche KI-Systeme schlicht zu Software zählt; im Detail Beck KI-VO-Wendehorst, Art. 3 N 8 f.

491 Beck KI-VO-Wendehorst, Art. 3 N 7.

492 Siehe auch Thouvenin et al., Jusletter IT 04.07.2024, Rn. 24.

493 Molavi Vasse'i, S. 195 f.

494 Molavi Vasse'i, S. 196.

495 Vasella, EU-Kommission: Leitlinien zum Begriff des AI-Systems, abrufbar unter <https://datenrecht.ch/eu-kommission-leitlinien-zum-begriff-des-ai-systems/>, zuletzt besucht am 31.05.2025.

496 Bundesrat, Leitlinien, S. 4; Braun Binder et al., Jusletter 28.06.2021, Rn. 56.

497 Kasper, Jusletter 23.09.2024, Rn. 47; Rosenthal, Jusletter 05.08.2024, Rn. 90; siehe auch Braun Binder et al., Jusletter 28.06.2021, Rn. 4, welche darauf hinweisen, dass der Zugang zum europäischen Binnenmarkt für schweizerische Unternehmen allenfalls gefährdet sein könnte, wenn KI stark unterschiedlich reguliert würde. Gleichzeitig wird aber auch auf Chancen einer innovationsfreundlichen (Nicht-)Regulierung hingewiesen.

B. Einführung in die relevanten Rechtsquellen der produktsicherheitsrechtlichen Nachmarktpflichten

141 In diesem Kapitel wird eine Übersicht über die Rechtsquellen der Produktsicherheit in der Schweiz und der EU gegeben, um die Grundlagen für die Behandlung der produktsicherheitsrechtlichen Nachmarktpflichten für KI-Produkte zu schaffen.

142 Vorab ist festzuhalten, dass die Terminologie der verschiedenen Erlasse uneinheitlich ist.[498] In der Schweiz wird im Kontext der Produktregulierung jeweils der Begriff des Produktes im Plural verwendet.[499] In der EU sind die Regulierungen im Singular benannt.[500] Wie bei BÜHLER und PFENNINGER/SCHILD werden auch in diesem Werk die Termini «Produktsicherheit» bzw. «Produkthaftpflicht» im Singular benutzt, wobei die Gesetze entsprechend ihrer offiziellen Bezeichnung im Plural benannt bleiben.

I. Horizontale Rechtsquellen in der Schweiz

143 Dieses Kapitel zeigt eine Übersicht über einige für Software und KI relevante Rechtsquellen für die produktsicherheitsrechtlichen Nachmarktpflichten.

1. STEG – Gesetz über die Sicherheit von technischen Einrichtungen und Geräten

144 Das Gesetz über die Sicherheit von technischen Einrichtungen und Geräten (STEG)[501] vom 19. März 1976 regelte in der Schweiz erstmals alle technischen

498 PFENNINGER/SCHILD, in: Fellmann/Furrer, Herausforderungen, S. 23 Fn. 1; BÜHLER, Bestandteil, V, welcher die Schreibweise im Plural zu Recht kritisiert; siehe auch DRITTENBASS, Rn. 358 Fn. 1291, welcher sich jedoch für die Schreibweise im Plural entschieden hat.

499 So die Bundesgesetze über die Produktesicherheit (SR 930.11) und die Produktehaftpflicht (SR 221.112.944) sowie die Verordnung über die Produktesicherheit (SR 930.111). Wobei in der Vernehmlassung noch vom «Produktsicherheitsgesetz (PSG)» im Singular die Rede war: Bericht Vernehmlassungsverfahren STEG, passim.

500 So die Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine *Produktsicherheit* und die Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates vom 10. Mai 2023 über die allgemeine *Produktsicherheit* […].

501 Bundesgesetz über die Sicherheit von technischen Einrichtungen und Geräten vom 19. März 1976, ausser Kraft, SR 819.1 (zit. STEG).

Einrichtungen und Geräte, solange diese nicht durch einen Spezialerlass geregelt wurden[502]. Das wichtigste Ziel war – wie der Name sagt – die Sicherheit von technischen Einrichtungen und Geräten.[503] Auch eine nachträgliche Marktüberwachung wurde im STEG – analog zur Europäischen Gemeinschaft (EG) – geregelt.[504] Somit musste die Sicherheit nicht nur beim Inverkehrbringen und Anpreisen, «sondern auch während des bestimmungsgemässen Gebrauchs» gewährleistet werden.[505]

Damit technischen Handelshemmnissen zwischen der damaligen EG und der Schweiz entgegengewirkt werden konnte, war eine Revision des STEG nötig.[506] Nach einem ersten Revisionsversuch 1992, welcher mit Ablehnung des EWR-Abkommens durch die Schweizer Stimmbevölkerung scheiterte,[507] trat am 1. Juli 1995 doch noch ein revidiertes STEG in Kraft.[508] Mit dieser Revision wurde eine Anpassung an die EG-Richtlinie 92/59/EWG über die allgemeine Produktsicherheit[509] und somit eine Angleichung an den «Global and New Approach» angestrebt.[510] Zudem wurden mehrere EG-Richtlinien ins Schweizer Recht übernommen.[511] Die EG-Richtlinie 92/59/EWG wurde 2002 durch die Produktsicherheitsrichtlinie revidiert.[512] Diese wurde wiederum 2023 durch die GPSR ersetzt.[513] 145

2. PrSG – Produktesicherheitsgesetz und PrSV – Produktesicherheitsverordnung

Das schweizerische Produktesicherheitsgesetz (PrSG) ist seit 1. Juli 2010 in Kraft und ersetzte[514] das STEG. Während das STEG lediglich auf technische Einrichtungen und Geräte anwendbar war, wurde der Geltungsbereich des 146

502 Art. 1 Abs. 2 STEG.
503 SHK PrSG-Hess, Einleitung N 48.
504 Art. 6 ff. STEG; SHK PrSG-Hess, Einleitung N 42.
505 SHK PrSG-Hess, Einleitung N 34.
506 SHK PrSG-Hess, Einleitung N 48 ff.
507 Diebold/Rütsche, Rn. 452.
508 Ausführlich SHK PrSG-Hess, Einleitung N 7 ff., 44 ff. m.w.H.
509 Richtlinie 92/59/EWG des Rates vom 29. Juni 1992 über die allgemeine Produktsicherheit, ABl. L 228/24 (zit. RL 92/59/EWG).
510 Botschaft PrSG, S. 7411, 7413.
511 Botschaft PrSG, S. 7414.
512 SHK PrSG-Hess, Einleitung N 10.
513 S. u., Rn. 156.
514 Siehe auch Art. 20 Abs. 1 PrSG.

PrSG auf Produkte allgemein ausgeweitet.[515] Das PrSG vollzieht die Europäische Richtlinie 2001/95/EG über die allgemeine Produktsicherheit nach und gleicht so die schweizerische Regulierung der Produktsicherheit an die europäische an.[516] Im Gegensatz zu den Mitgliedstaaten der EU hat die Schweiz keine Pflicht, Europäische Richtlinien in nationales Recht zu übernehmen. Aus wirtschaftlicher Perspektive ergab die Übernahme jedoch auch in der Schweiz Sinn.[517] Ziel war es, wirtschaftlich kompatibel zu sein[518] und überall das gleiche Sicherheitsniveau zu erhalten.[519] Gem. Art. 4 Abs. 1 und Abs. 2 PrSG werden bspw. die grundlegenden Sicherheits- und Gesundheitsanforderungen vom Bundesrat unter Berücksichtigung des internationalen Rechts festgelegt.[520] Zudem wurde mit dem Wechsel vom STEG zum PrSG die Umstellung «von einer präventiven Kontrolle zu einer Marktkontrolle» vollzogen.[521]

147 Das PrSG verfolgt zwei Ziele: Erstens soll es die Sicherheit und Gesundheit der Bevölkerung und somit die körperliche Integrität von Personen schützen.[522] Zweitens soll – wie beim THG[523] – der freie Warenverkehr[524] mit der EU[525] erleichtert werden. Dazu mussten die Anforderungen an die Sicherheit von Konsumentenprodukten in der Schweiz an das Niveau der EU – damals geregelt in der Produktsicherheitsrichtlinie – angeglichen werden.[526] Dazu dürfen nur Produkte in Verkehr gebracht werden und auf dem Markt verfügbar bleiben, welche für Menschen sicher sind.[527] Um das erste Ziel zu erreichen, regelt das PrSG im 2. Abschnitt Voraussetzungen für das Inverkehrbringen und im 3. Ab-

515 Botschaft PrSG, S. 7417 f., 7431; zuletzt Urteil des Obergerichts des Kantons Zürich UE140296 vom 03.08.2015, E. 7.4; BVGer C-914/2013 vom 06.10.2016, E. 2.1.4; BVGer C-4660/2013 vom 28.05.2015, E. 3.3; ebenso Gerster, Rn. 27, m.w.H.

516 Fellmann, Jusletter 25.10.2010, Rn. 1 f.; Wey, in: Fellmann/Furrer, Schonzeit, S. 30; Bühler, Bestandteil, S. 8 f.; SHK PrHG-Hess, Art. 4 N 4; IK-EUDP, Schweiz, S. 61; Fornage, Sécurité, Rn. 11.

517 Siehe dazu die parlamentarische Diskussion, AB S 2009, insbesondere S. 70; und AB N 2009, S. 709 ff.

518 S. o., Rn. 64.

519 S. u., Fn. 632.

520 Siehe auch SHK PrSG-Hess, Art. 3 N 21, m.w.H.

521 BVGer C-1177/2012 vom 12.06.2014, E. 5.1.3.

522 BGE 143 II 518, 529 E. 5.6.1; Urteil des Obergerichts des Kantons Zürich UE140296 vom 03.08.2015, E. 7.2; Gerster, Rn. 385, welcher das PrSG als eine «dem Allgemeinwohl verpflichtete staatliche Sicherheitsvorschrift» bezeichnet; Bühler/Tobler, S. 127.

523 Zum Verhältnis zwischen dem THG und dem PrSG: SHK PrSG-Hess, Einleitung N 88 f.

524 Art. 1 Abs. 1 PrSG; BGE 143 II 518, 523 E. 5.1; BVGer C-3805/2020 vom 09.05.2022, E. 3.1.

525 Fellmann, Jusletter 25.10.2010, Rn. 2.

526 Botschaft PrSG, S. 7408; siehe auch Wey, in: Fellmann/Furrer, Schonzeit, S. 37, m.w.H.

527 Fellmann, Jusletter 25.10.2010, Rn. 2; Kellerhals, in: Dürr/Lardi/Rouiller S. 304.

schnitt Pflichten nach dem Inverkehrbringen.[528] Das PrSG legt in Art. 8 Nachmarktpflichten fest, welche u.a. für Hersteller gelten. Weiter werden auch den Importeuren, Händlern, anderen Inverkehrbringern und weiteren Wirtschaftsteilnehmern Pflichten auferlegt. Diese werden vorliegend jedoch nicht näher betrachtet. Im Gegensatz zu den übrigen Bestimmungen des PrSG gelten die Nachmarktpflichten nur für Konsumentenprodukte.[529] Neben den produktsicherheitsrechtlichen Nachmarktpflichten aus dem PrSG sind die Bestimmungen der PrSV zu beachten. Die PrSV enthält jedoch keine zusätzlichen Nachmarktpflichten für Hersteller, sondern nur Spezifizierungen zu den existierenden Regeln. Die PrSV spezifiziert u.a. die Marktüberwachung durch die Behörden.[530] Als Orientierungshilfe für die Anwendung des PrSG und der PrSV können die FAQ des Staatssekretariats für Wirtschaft (SECO) zu den genannten Regulatorien beigezogen werden. Die FAQ sind jedoch rechtlich nicht massgebend.[531]

Das PrSG hat einen präventiven Charakter.[532] Wichtig ist, dass zwischen dem Produktsicherheitsrecht und dem Produkthaftpflichtrecht[533] unterschieden wird. Es handelt sich beim Produktsicherheitsrecht um Verwaltungsrecht[534] mit den obengenannten Zielen. Das Produkthaftpflichtrecht hingegen schafft – zusammen mit dem Obligationenrecht (OR)[535] – die Haftungsgrundlagen (u.a. auch aus Versäumnissen von Pflichten aus der Produktsicherheit[536]) für fehlerhafte Produkte.[537] Dennoch sind das Produktsicherheitsrecht und das Produkthaftpflichtrecht eng miteinander verbunden.[538] Während das Produktsicherheitsrecht darauf abzielt, präventiv Schäden zu verhindern, lassen sich 148

528 Bereits vor dem Inkrafttreten des PrSG wurden Produktbeobachtungspflichten aus dem Zivilrecht anerkannt, Fornage, in: Chappuis/Winiger/Campi S. 209; Röthlisberger, S. 29 f.

529 Botschaft PrSG, S. 7431, 7441.

530 Art. 1 lit. d PrSV.

531 SECO, FAQ, S. 1.

532 Roberto, Rn. 09.36; Gerster, Rn. 372.

533 In erster Linie geregelt im Bundesgesetz über die Produktehaftpflicht (Produktehaftpflichtgesetz) vom 18. Juni 1993, SR 221.112.944 (zit. PrHG).

534 Roberto, Rn. 09.37.

535 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220 (zit. OR).

536 Wildhaber/Rey, Rn. 1496; SHK PrHG-Hess, Art. 4 N 8 f.

537 Wildhaber/Rey, Rn. 1406; Roberto, Rn. 09.01; Bühler, Bestandteil, S. 11 f. m.w.H.

538 Produktsicherheitsrecht und Produkthaftpflichtrecht werden auch als «two sides of the same coin» bezeichnet, Lohsse/Schulze/Staudenmayer, in: Lohsse/Schulze/Staudenmayer, Liability for AI, S. 10; mit Bezug zur europäischen KI-Regulierung übernommen von Wildhaber, Jusletter IT 04.07.2024, Rn. 19; siehe auch Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 163.

durch das Produkthaftungsrecht nachträglich Schäden ausgleichen.[539] Das PrSG hat das Schutzniveau von Produkten jenem des PrHGs angepasst, welches bereits mit der Produktsicherheitsrichtlinie deckungsgleich war.[540] Das Bundesgericht stellte zu Recht fest, dass im Produktsicherheits- und Produkthaftpflichtrecht «teilweise analoge Begriffe» verwendet werden und beide «grundsätzlich auf das gleiche Sicherheitsniveau» abstellen.[541] Es rechtfertigte aufgrund dieser Feststellung, «die Überlegungen zum Produkthaftpflichtgesetz analog auch auf das Produktsicherheitsrecht anzuwenden».[542] Die vom Bundesgericht gezogene Analogie zwischen den zwei Rechtsgebieten ist jedoch mit Zurückhaltung anzuwenden, da das PrSG und das PrHG verschiedene Ziele verfolgen. Da allerdings viel zum Produkthaftpflichtrecht bzw. in der EU zum Produkthaftungsrecht und wenig zum Produktsicherheitsrecht geschrieben wurde, wird – wo sinnvoll – die Literatur zur Produkthaftpflicht bzw. zur Produkthaftung einbezogen.[543] Das PrHG wurde von der Schweiz ebenfalls nach der Produkthaftungsrichtlinie 85/374/EWG (PLD 1985)[544] autonom nachvollzogen.[545] Es ist auch europakonform auszulegen.[546]

149 Die verfassungsrechtlichen Grundlagen für das PrSG finden sich in Art. 95 Abs. 1 BV[547] zur Ausübung der privatwirtschaftlichen Erwerbstätigkeit, Art. 97

539 Zugleich hat das Produkthaftpflichtrecht auch eine präventive Komponente, indem Anreize geschaffen werden, die Pflichten des Produktsicherheitsrechts einzuhalten, um nicht für allfällige Schäden aufkommen zu müssen, Lohsse/Schulze/Staudenmayer, in: Lohsse/Schulze/Staudenmayer, Liability for AI, S. 10 f.; ebenso Wildhaber, Jusletter IT 04.07.2024, S. 19.

540 Fellmann, Jusletter 25.10.2010, Rn. 3.

541 BGE 139 II 534, 540f. E. 4.5, m.w.H.

542 BGE 139 II 534, 541 E. 4.5, wobei das BGer seine Meinung mit dem Verweis auf eine Quelle zum deutschen ProdSG unterstreicht; gl.M. wie das BGer mit Verweis auf ebendiesen Entscheid ist Gerster, Rn. 92, wobei dieser unterstreicht, dass «keine Kongruenz angenommen werden» dürfe; ohne Meinung, aber ebenfalls mit Verweis auf diesen Entscheid Damian, in: Praxishandbuch Produktregulierung, § 19 Rn. 2335.

543 Zur Möglichkeit von «disziplinübergreifenden» Analogieschlüssen zwischen Privat- und Verwaltungsrecht siehe Kramer/Arnet, S. 232, m.w.H.; umgekehrt das PrSG und die europäische Produktsicherheitsrichtlinie zur Auslegung des PrHG verwendend SHK PrHG-Hess, Art. 4 N 6.

544 Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (Product Liability Directive), ABl. L 210/29 (zit. PLD 1985).

545 IK-EUDP, Schweiz, S. 61; Roberto, Rn. 09.01; Wildhaber/Rey, Rn. 1408; zum autonomen Nachvollzug ins PrHG siehe auch Kramer/Arnet, S. 355 Fn. 1101.

546 Konkret zum PrHG: BGE 133 III 81, 83 f. E. 3.1; BGE 137 III 226, 229 E. 2.2; Wildhaber/Rey, Rn. 1408; Fellmann, in: Fellmann S. 116; allgemein zur europarechtskonformen Auslegung BGE 129 III 335, 350 E. 6.

547 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999, SR 101 (zit. BV).

Abs. 1 BV zum Schutz der Konsumentinnen und Konsumenten und Art. 110 Abs. 1 lit. a BV zum Schutz der Arbeitnehmerinnen und Arbeitnehmer.[548] Zudem stützt sich das PrSG auf Art. 118 BV zum Schutz der Gesundheit.[549] Es handelt sich beim PrSG – im Gegensatz zu den Sektorrechten[550] – um einen horizontalen Rahmenerlass.[551] Es wird auch als Auffanggesetz bezeichnet, da es jeweils dann angewandt wird, wenn mit den sektorrechtlichen Regeln nicht das gleiche Ziel wie mit den Regeln des PrSG verfolgt wird.[552] Das PrSG regelt primär «potenziell gefährliche Produkte».[553] Es nennt seinen räumlichen Geltungsbereich nicht ausdrücklich. Die Pflichten des PrSG gelten für Hersteller mit Schweizer «Sitz, Wohnsitz oder Aufenthalt».[554] Befindet sich der Hersteller nicht in der Schweiz, wird bspw. im Falle der Nachmarktpflichten nach Art. 8 PrSG der Importeur subsidiär verpflichtet.[555]

3. Exkurs: THG – Gesetz über die technischen Handelshemmnisse

Das schweizerische Bundesgesetz über die technischen Handelshemmnisse (THG)[556] trat am 1. Juli 1996 in Kraft. Ziel des Gesetzes ist es, einheitliche Grundlagen zu schaffen, «damit im Regelungsbereich des Bundes technische Handelshemmnisse vermieden, beseitigt oder abgebaut werden».[557] Während der Hauptzweck das THGs der Abbau von Handelshemmnissen ist, ist der Hauptzweck des PrSG die Gewährleistung der Sicherheit von Produkten.[558] Das THG und das PrSG sind «komplementäre Rahmenerlasse».[559] 150

[548] Ingress PrSG; Botschaft PrSG, S. 7450.

[549] Ingress PrSG; Botschaft PrSG, S. 7450; siehe auch: BSK BV-Gächter/Renold-Burch, Art. 118 N 20; SGK BV-Tomas/Bernhard, Art. 118 N 33, welche bei den erfassten Gegenständen nach Art. 118 BV auf von Art. 2 Abs. 1 PrSG erfasste Produkte verweisen.

[550] S. u., Rn. 161.

[551] Botschaft PrSG, S. 7426; siehe auch Wey, in: Fellmann/Furrer, Schonzeit, S. 30 f.

[552] Das PrSG ist lex generalis zum Sektorrecht BVGer A-4413/2021 vom 20.09.2023, E. 4.3.3; Roberto, Rn. 09.37; Gerster, Rn. 12; Wey, in: Fellmann/Furrer, Schonzeit, S. 34.

[553] Daneben gehören auch Unternehmen zu den Regelungsgegenständen des PrSG, da mit den Nachmarktpflichten eine «Sicherheits- und Notfallorganisation» nötig wurde, SHK PrSG-Hess, Art. 8 N 3.

[554] SHK PrSG-Hess, Art. 2 N 23.

[555] SHK PrSG-Hess, Art. 2 N 23.

[556] Bundesgesetz über die technischen Handelshemmnisse vom 6. Oktober 1995, SR 946.51 (zit. THG).

[557] Art. 1 Abs. 1 THG.

[558] BGE 143 II 518, 529 E. 5.6.1.

[559] Botschaft PrSG, S. 7426; die Botschaft zitierend: BGE 143 II 518, 525 f. E. 5.3; BVGer C-1177/2012 vom 12.06.2014, E. 4.2.

151 Mit dem THG wurde das Cassis-de-Dijon-Prinzip[560] im Schweizer Recht verankert, wodurch der Zugang zum Schweizer Markt auch für Produkte geöffnet wurde, die nicht den nationalen technischen Vorschriften entsprechen, aber im EU/EWR-Raum rechtmässig auf dem Markt sind.[561] Das Cassis-de-Dijon-Prinzip wird nur einseitig durch die Schweiz gegenüber den EU- und EWR-Mitgliedern angewandt, aber nicht umgekehrt.[562] Sind Produkte durch das MRA abgedeckt, können diese problemlos in die Schweiz eingeführt werden, da die in der EU durchgeführte Konformitätsbewertung anerkannt wird – eine Anwendung des Cassis-de-Dijon-Prinzips ist daher nicht erforderlich.[563]

152 Das THG regelt die Marktüberwachung.[564] Art. 3 lit. p THG definiert den Begriff «Marktüberwachung» wie folgt: «die hoheitliche Tätigkeit von Vollzugsorganen, mit der durchgesetzt werden soll, dass angebotene, in Verkehr gebrachte oder in Betrieb genommene Produkte den technischen Vorschriften entsprechen». Während Behörden nach dem PrSG nur bei der Gefährdung der Sicherheit und Gesundheit der Verwender eingreifen dürfen, gilt diese Interventionsbefugnis gem. dem THG auch zum Schutz «anderer öffentlicher Interessen».[565] Es enthält keine Nachmarktpflichten für Hersteller.

II. Horizontale Rechtsquellen in der EU

153 Die Produktsicherheit in der EU ist in verschiedenen sektorrechtlichen Richtlinien und Verordnungen geregelt. Seit 2024 ist die Produktsicherheitsverordnung in Kraft. Zuvor wurde die Produktsicherheit in der EU neben den sektorrechtlichen Erlassen durch die RL 92/59/EWG über die allgemeine Produktsicherheit geregelt. EU-Richtlinien und Verordnungen dienen der Harmonisierung von Anforderungen für den freien Verkehr von Waren und Dienstleistungen im Europäischen Binnenmarkt. Es wird zwischen einem harmonisierten und einem nicht-harmonisierten Bereich unterschieden.[566] Der harmonisierte Bereich ist jener Bereich des Europäischen Binnenmarktes, in dem durch EU-rechtliche Harmonisierungsvorschriften ein einheitlicher Rechtsrahmen geschaffen wurde. Ein

560 Zum ursprünglichen Entscheid siehe EuGH vom 20.02.1979, 120/78, Rewe-Zentral (Cassis de Dijon), ECLI:EU:C:1979:42.
561 Art. 16a Abs. 1 THG; SHK PrSG-Hess, Einleitung N 88; Diebold/Rütsche, Rn. 531.
562 Bühler, Sicherheit, Rn. 12; Diebold/Rütsche, Rn. 521.
563 Diebold/Rütsche, Rn. 533.
564 Art. 19 ff. THG.
565 SHK PrSG-Hess, Einleitung N 89; Hess zitierend BVGer C-1177/2012 vom 12.06.2014, E. 4.3.
566 SHK PrSG-Hess, Einleitung N 85 Fn. 321, m.w.H.

Harmonisierungsrechtsakt ist bspw. die Niederspannungsrichtlinie (LVD)[567] [568]. Befindet sich ein Produkt im nichtharmonisierten Bereich – bestehen also keine Harmonisierungsvorschriften[569] –, sind Art. 28 bis 30 AEUV[570] anwendbar.[571] Auch im nichtharmonisierten Bereich müssen Produkte von den EU-Mitgliedstaaten gegenseitig anerkannt werden.[572] Diese Anerkennung wird einseitig auch von der Schweiz beachtet.[573]

1. Produktsicherheitsrichtlinie RL 2001/95/EG

Die RL 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit forderte, «dass Verbraucherprodukte sicher sein müssen und dass die Marktüberwachungsbehörden der Mitgliedstaaten gegen gefährliche Produkte vorgehen und diesbezüglich Informationen über das Unionssystem zum raschen Informationstausch (RAPEX) austauschen müssen».[574] Die Produktsicherheitsrichtlinie hatte den Zweck, die menschliche Gesundheit und Sicherheit zu schützen,[575] indem innerhalb der EU die «Mindestanforderungen an die Sicherheit von Produkten für Verbraucher» harmonisiert sowie verantwortliche Wirtschaftsakteure bestimmt und verpflichtet wurden.[576] Sie war subsidiär zum spezifischen Sektorrecht[577] und nur auf Verbraucherprodukte anwendbar[578]. Die Produktsicherheitsrichtlinie war 154

567 Richtlinie 2014/35/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen auf dem Markt (Niederspannungsrichtlinie, Low Voltage Directive), ABl. L 96/357 (zit. LVD).

568 Anhang I Ziff. 54 MÜVO.

569 Wobei das allgemeine Produktsicherheitsrecht nicht-harmonisierte Konsumentenprodukte regelt und es sich deshalb nicht um einen völlig «unharmonisierten» Bereich handelt. Siehe dazu SCHUCHT, Produktkrisen, S. 313.

570 Konsolidierte Fassungen vom 15.03.2025 des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union, ABl. C 202/1 (zit. AEUV).

571 SHK PrSG-HESS, Einleitung N 85 Fn. 321, m.w.H.; u.U. ist auch die MÜVO anwendbar, siehe ErwG 39, Art. 16 Abs. 1 GPSR i.V.m. Art. 4 Abs. 3 MÜVO.

572 EuGH vom 20.02.1979, 120/78, Rewe-Zentral (Cassis de Dijon), ECLI:EU:C:1979:42, S. 652 f.; ausführlich auf den Entscheid bezugnehmend SHK PrSG-HESS, Einleitung N 85 Fn. 321, m.w.H.

573 S. o., Rn. 151.

574 ErwG 1 GPSR.

575 BAUER, Rn. 78.

576 LITTBARSKI, in: Taeger/Pohle, Teil 18 Rn. 170.

577 Art. 1 Abs. 2 Produktsicherheitsrichtlinie; LITTBARSKI, in: Taeger/Pohle, Teil 18 Rn. 170; PFENNINGER, S. 1159; WEY, in: Fellmann/Furrer, Schonzeit, S. 32.

578 Art. 2 lit. a Produktsicherheitsrichtlinie.

das öffentlich-rechtliche Pendant zum Produkthaftungsrecht in der EU.[579] Die Nachmarktpflichten wurden in Art. 5 der Produktsicherheitsrichtlinie geregelt.

155 Im Gegensatz zu heute gab es zum Zeitpunkt der Verabschiedung der Richtlinie nur wenige Verbraucherprodukte, die neue Technologien wie IoT oder KI enthielten.[580] Die Produktsicherheitsrichtlinie wurde deshalb aufgrund von Entwicklungen in den Bereichen neuer Technologien und Onlineverkäufe aktualisiert und überarbeitet. Dadurch sollte u.a. sichergestellt werden, dass Produktsicherheitsrückrufe besser funktionieren, und «um für Kohärenz mit den Entwicklungen der Harmonisierungsrechtsvorschriften und Normungsrechtsvorschriften der Union zu sorgen». Die Produktsicherheitsrichtlinie sowie die RL 87/357/EWG[581] wurden aufgehoben und durch die GPSR ersetzt.[582]

2. GPSR – Produktsicherheitsverordnung VO (EU) 2023/988

156 Am 10. Mai 2023 wurde die neue Produktsicherheitsverordnung im Amtsblatt der Europäischen Union veröffentlicht. Diese gilt gem. ihrem Art. 52 seit dem 13. Dezember 2024. Im Übergangszeitraum durften Produkte, die gem. Produktsicherheitsrichtlinie konform waren, noch in Verkehr gebracht werden.[583] Durch die Regulierung in Form einer Verordnung mit «klare[n] und ausführliche[n] Vorschriften» statt einer oder mehrerer Richtlinien wird den Mitgliedstaaten der EU kein «Raum für eine abweichende Umsetzung» gelassen.[584] Die Marktüberwachung von Produkten innerhalb der EU soll damit kohärent geregelt und der Aufwand für einheitlich angewandte Produktsicherheitsvorschriften minimiert werden.[585] Die GPSR gilt als EU-Verordnung nur für die europäischen Mitgliedstaaten und ist in der Schweiz nicht anwendbar.

579 WAGNER, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 163.

580 Europäische Kommission, Impact Assessment GPSR, S. 12.

581 Richtlinie 87/357/EWG des Rates vom 25. Juni 1987 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten für Erzeugnisse, deren tatsächliche Beschaffenheit nicht erkennbar ist und die die Gesundheit oder die Sicherheit der Verbraucher gefährden, ABl. L 192/49 (zit. RL 87/357/EWG).

582 ErwG 2 GPSR.

583 ErwG 105 GPSR.

584 ErwG 3 GPSR; Verordnungen der EU sind für die Mitgliedstaaten nach Art. 288 Abs. 2 AEUV direkt anwendbar. Richtlinien hingegen müssen gem. Art. 288 Abs. 3 AEUV zuerst ins nationale Recht umgesetzt werden, wodurch Abweichungen entstehen können.

585 ErwG 3 GPSR; siehe auch NP GPSR-SCHUCHT/WIEBE, § 1 N 13.

Die Verordnung legt «wesentliche Vorschriften für die Sicherheit von Verbraucherprodukten» fest.[586] Sie hat das Ziel, das Funktionieren des Europäischen Binnenmarktes zu verbessern und gleichzeitig ein hohes Niveau an Verbraucherschutz sicherzustellen.[587] Explizit genannt wird das Ziel, die Gesundheit und Sicherheit von Verbrauchern zu gewährleisten.[588] Es handelt sich bei der Verordnung um einen «bereichsübergreifenden Rechtsrahmen», da die Regelung von Sicherheitsaspekten aller Produktkategorien unmöglich ist.[589] Wie bereits bei der allgemeinen Produktsicherheitsrichtlinie handelt es sich auch bei der GPSR um einen horizontalen Rechtsakt, da sie für alle Verbraucherprodukte gilt.[590] Sie wird auch als «allgemeiner Teil» des europäischen Produktsicherheitsrechts bezeichnet.[591] Die Nachmarktpflichten sind in Art. 9, 20 und 35 bis 37 GPSR geregelt. 157

3. KI-VO – Verordnung über künstliche Intelligenz VO (EU) 2024/1689

Die KI-VO ist ein horizontaler, risikobasierter Erlass und stellt in erster Linie Produktsicherheitsrecht für KI-Systeme dar.[592] Sie ergänzt das bestehende Produktsicherheitsrecht der EU und schliesst Lücken in Bezug auf KI-Systeme.[593] Die KI-VO wird als «eine Art ‹Pilotprojekt›» bezeichnet.[594] Sie gilt für alle KI-Systeme, unabhängig davon, ob diese an Verbraucher gerichtet sind oder nicht (B2B, nicht nur B2C).[595] Sie trat am 1. August 2024 in Kraft,[596] wobei die enthaltenen Vorschriften gem. Art. 113 KI-VO gestaffelt zu gelten beginnen.[597] Die ersten Regelungen hatten ihren Geltungsbeginn am 2. Februar 2025,[598] währen der späteste Geltungsbeginn am 2. August 2027 sein wird.[599] 158

586 Art. 1 Abs. 2 GPSR.
587 Art. 1 Abs. 1 GPSR.
588 ErwG 4 GPSR.
589 ErwG 6 GPSR.
590 NP GPSR-Schucht/Wiebe, § 1 N 11, 16.
591 NP GPSR-Schucht/Wiebe, § 3 N 66.
592 ErwG 9, 26 KI-VO; Buchalik/Gehrmann, Rn. 5; Voigt/Hullen, S. 1; Borges, Teil 1, Rn. 7, m.w.H.; Krönke, S. 533; Wagner, Rauch, S. 128.
593 ErwG 9 KI-VO; Buchalik/Gehrmann, Rn. 1.
594 Beck KI-VO-Hartmann, Art. 96 N 3.
595 Art. 3 Ziff. 1 KI-VO unterscheidet nicht zwischen KI-Systemen für Verbraucher oder andere; siehe auch Beck KI-VO-Wendehorst, Art. 1 N 59.
596 Beck KI-VO-Wendehorst, Art. 113 N 1; Rosenthal, Jusletter 05.08.2024, Rn. 1; Borges, Teil 1, Rn. 1.
597 Siehe auch Beck KI-VO-Wendehorst, Art. 113 N 1.
598 Art. 113 lit. a KI-VO; siehe auch Beck KI-VO-Wendehorst, Art. 113 N 2.
599 Art. 113 lit. c KI-VO; siehe auch Beck KI-VO-Wendehorst, Art. 113 N 11.

Bis spätestens 31. Dezember 2030 müssen die letzten KI-Systeme mit der KI-VO in Einklang gebracht werden.[600]

159 Zweck der KI-VO sind die Verbesserung des Funktionierens des EU-Binnenmarktes und die Förderung der «Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen KI».[601] «Gleichzeitig [soll] ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der [EU-]Charta verankerten Grundrechte, einschliesslich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von KI-Systemen in der Union» gewährleistet und Innovation unterstützt werden.[602] Dies soll mittels eines einheitlichen Rechtsrahmens, welcher insbesondere «die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von» KI-Systemen in der EU regelt, erreicht werden. Ausserdem soll die KI-VO «den grenzüberschreitenden freien Verkehr KI-gestützter Waren und Dienstleistungen» in der EU sicherstellen.[603] Die KI-VO regelt hauptsächlich den Umgang mit KI-Systemen, die ein hohes Risiko für die Gesundheit, Sicherheit und Grundrechte von Personen in der EU verursachen können.[604]

160 Die KI-VO ist vorliegend aus zwei Gründen relevant: Erstens kann sie zwecks Kompatibilität mit dem übrigen Produktsicherheitsrecht der EU in der Schweiz einen grossen Einfluss auf die Regulierung von KI-Systemen haben.[605] Zweitens kann die KI-VO für Schweizer Hersteller aufgrund ihrer extraterritorialen Wirkung[606] unter Umständen direkt anwendbar sein.[607] Art. 2 Abs. 1 KI-VO regelt den persönlichen sowie den internationalen Anwendungsbereich der KI-VO.[608] Der räumliche Anwendungsbereich der KI-VO knüpft für Anbieter am Marktortprinzip an.[609] Die KI-VO gilt für Anbieter, wenn diese ein KI-System oder KI-Modell mit allgemeinem Verwendungszweck in der EU in Verkehr bringen oder ein KI-System in Betrieb nehmen.[610] Dies gilt auch, wenn

600 Art. 111 Abs. 1 KI-VO.
601 Art. 1 Abs. 1 KI-VO.
602 Art. 1 Abs. 1 KI-VO.
603 ErwG 1 KI-VO.
604 ErwG 7, 65, 66 KI-VO; siehe auch Buchalik/Gehrmann, Rn. 5.
605 S. o., Rn. 4.
606 Beck KI-VO-Wendehorst, Art. 2 N 6, m.w.H.
607 IK-EUDP, Schweiz, S. 20; Kasper, Jusletter 23.09.2024, Rn. 25.
608 Siehe auch Beck KI-VO-Wendehorst, Art. 2 N 1.
609 Für Anbieter, Beck KI-VO-Wendehorst, Art. 2 N 12 aber anders für Betreiber, wo sie am Niederlassungsprinzip anknüpft, siehe N 20; Voigt/Hullen, S. 20; Schopper/Raschner, S. 97.
610 S. u., Rn. 294 f.

diese Anbieter in einem Drittland,[611] wie z.B. der Schweiz, niedergelassen sind. Des Weiteren gilt die KI-VO auch für Anbieter in Drittländern, wenn die Ausgabe des KI-Systems «in der Union[612] verwendet wird».[613] Der Anwendungsbereich kann hier sehr weit sein, ist zurzeit aber noch nicht ganz klar[614] und sollte durch Leitlinien konkretisiert werden[615]. In der Literatur wird die Bestimmung eng ausgelegt und es sollen nur absehbare bzw. bestimmungsgemässe Verwendungen der Ausgaben des KI-Systems in der EU als erfasst gelten, da Art. 2 Abs. 1 lit. c KI-VO eigentlich nur zur Verhinderung von Umgehungen der Verordnung gedacht war.[616] Beabsichtigen Anbieter in der Schweiz (wenn sie keine Niederlassung in der EU haben) nicht, dass die Ausgaben ihrer KI-Systeme in der EU verwendet werden, unterliegen sie auch nicht den Vorschriften der KI-VO. Zuletzt ist die KI-VO für Einführer, Händler, Bevollmächtigte und betroffene Personen in der EU anwendbar.[617] Auf diese soll hier aber nicht eingegangen werden. Die Bestimmungen über die Nachmarktpflichten sind in Art. 9, 18, 19, 20, 72 und 73 KI-VO geregelt. Sie alle gelten ab dem 2. August 2026.[618]

III. Vorrang des Sektorrechts in der Schweiz

Zusätzlich zum THG, PrSG und zur PrSV existieren zahlreiche sektorspezifische Erlasse, die die Produktsicherheit in der Schweiz regeln.[619] Art. 1 Abs. 3 PrSG hält fest, dass das PrSG nur anwendbar ist, «soweit nicht andere bundesrechtliche Bestimmungen bestehen, mit denen dasselbe Ziel verfolgt wird». 161

611 Art. 2 Abs. 1 lit. a und ErwG 21 KI-VO.

612 Damit sind die 27 EU-Mitgliedstaaten sowie Norwegen, Liechtenstein und Island als EWR-EFTA-Staaten gemeint. Die Schweiz ist deshalb nicht mitgemeint, Beck KI-VO-Wendehorst, Art. 2 N 9, 11.

613 Art. 2 Abs. 1 lit. c und ErwG 22 KI-VO.

614 Schopper/Raschner, S. 97; Voigt/Hullen, S. 20; siehe auch Rosenthal, Jusletter 05.08.2024, Rn. 24, m.w.H.

615 Schopper/Raschner, S. 98; Arioli, Jusletter IT 04.07.2024, Rn. 51.

616 Schopper/Raschner, S. 97 f.; Beck KI-VO-Wendehorst, Art. 2 N 24; Voigt/Hullen, S. 21; Krönke, S. 530; Rosenthal, Jusletter 05.08.2024, Rn. 24; siehe auch das Beispiel in ErwG 22 KI-VO; ebenfalls die Anwendbarkeit der KI-VO nur bei einer absichtlichen Verwendung der Ausgabe des KI-Systems im EWR bejahend mit Verweis auf ErwG 22 KI-VO Kasper, Jusletter 23.09.2024, Rn. 27; a.A. wohl: BJ, Rechtliche Basisanalyse KI, S. 123; Arioli, Jusletter IT 04.07.2024, Rn. 51.

617 Art. 2 Abs. 1 lit. d, f und g KI-VO.

618 Art. 113 lit. c KI-VO; Beck KI-VO-Wendehorst, Art. 113 N 13.

619 Wey, in: Fellmann/Furrer, Schonzeit, S. 35; SHK PrSG-Hess, Einleitung N 88; siehe bspw. die vom MRA erfassten Produktbereiche mit einer Auflistung der Regelungen der EU mit den entsprechenden Regelungen der Schweiz in Art. 3 Abs. 2 i.V.m. Anhang 1 MRA. Zum Sektorrecht mit Relevanz für Software und KI s. u., Rn. 169.

Die «anderen bundesrechtlichen Bestimmungen» sind die sektoriellen Erlasse, welche dem PrSG grundsätzlich vorgehen.[620] Es handelt sich bei den sektoriellen Erlassen um leges speciales zum PrSG. Vorliegend ist es wichtig, zu klären, wann das PrSG und wann Sektorrecht zur Anwendung kommt, da sich die Nachmarktpflichten nach Art. 8 PrSG nicht überall mit den Nachmarktpflichten in den Sektorerlassen decken.[621] Mit den Nachmarktpflichten gem. Art. 8 PrSG sollte eine Angleichung des Schutzniveaus in der Schweiz an jenes der EU in Bezug auf den Schutz der Gesundheit und Sicherheit (bzw. der körperlichen Integrität) von Menschen vor sich auf dem Markt befindenden, unsicheren Konsumentenprodukten erfolgen. Als das PrSG in Kraft trat, waren die sektoriellen Erlasse noch nicht an das höhere, europäische Schutzniveau angepasst[622] und damit auf einem tieferen Schutzniveau als das PrSG.[623] Obwohl das Sektorrecht dem PrSG grundsätzlich vorgeht, bestehen drei Ausnahmen.

1. Ausnahme 1: Gesetzesstufe nicht genügend hoch

162 Ein sektorieller Erlass, der sich unterhalb der Gesetzesstufe befindet, muss «sich im Rahmen des übergeordneten Gesetzes» halten.[624] Eine vom PrSG abweichende Regelung muss also «auf einer hinreichenden gesetzlichen Grundlage beruhen».[625] Ist diese Voraussetzung nicht erfüllt, darf der sektorielle Erlass nicht angewandt werden und das PrSG ist stattdessen anwendbar.[626]

2. Ausnahme 2: Enthält das Sektorrecht keine Regelung, gilt das PrSG

163 Enthält das Sektorrecht für Produkte, die auch vom PrSG erfasst sind, zu gewissen Themen keine Regelung, wird das PrSG ergänzend angewandt.[627] Sind

620 SHK PrSG-Hess, Einleitung N 88 mit Verweis auf Ausnahmen.

621 S. u., Rn. 387.

622 Produktsicherheit, Änderung des Bundesgesetzes über die Sicherheit von technischen Einrichtungen und Geräten (STEG), Bericht über die Ergebnisse des Vernehmlassungsverfahrens, S. 6 f.; SHK PrSG-Hess, Einleitung N 88 Fn. 335; siehe auch Motion 09.3008 vom 29.01.2009, Kommission für Wirtschaft und Abgaben Ständerat/Ständerat, Bereinigung der Spezialgesetzgebung im Bereich der Produktesicherheit.

623 Botschaft PrSG, S. 7433; siehe auch Wey, in: Fellmann/Furrer, Schonzeit, S. 61.

624 Botschaft PrSG, S. 7433.

625 Botschaft PrSG, S. 7433.

626 Botschaft PrSG, S. 7433.

627 Art. 1 Abs. 3 PrSG; Botschaft PrSG, S. 7433; siehe auch ausführlich Wey, in: Fellmann/Furrer, Schonzeit, S. 35.

also keine Nachmarktpflichten im spezifischen Sektorrecht aufgeführt, gelten jene nach Art. 8 PrSG.[628] Ist ein Produkt überhaupt nicht durch Sektorrecht geregelt, gelten ebenfalls die Bestimmungen des PrSG.[629]

3. Ausnahme 3: Höchstes Schutzniveau geht (meistens) vor

Der Vorrang des Sektorrechts gilt jeweils unter dem Vorbehalt, dass mit einer Regelung *dasselbe Ziel*[630] verfolgt wird. Strittig ist, was mit «Ziel» gemeint ist. Vorliegend wird vertreten, dass es sich beim «gleichen Ziel» um das Sicherheits- bzw. Schutzniveau und nicht etwa um «den Umfang bzw. de[n] Anwendungsbereich der Sicherheit»[631] handelt. Mit Erlass des PrSG sollte eine Anpassung an das Schutzniveau der EU (bzw. damals der EG) stattfinden.[632] Das Sicherheitsniveau des angewendeten Produktsicherheitsrechts darf also nicht tiefer sein, als mit der EU vereinbart.[633] Deshalb geht auch das Sektorrecht nicht vor, wenn dessen Schutzniveau tiefer ist als jenes des PrSG. Trotz Lex-specialis-Eigenschaft des Sektorrechts tritt dieses hinter dem höheren Schutzniveau der Regelung im PrSG zurück.[634] Konkret heisst das: Enthält das Sektorrecht für ein bestimmtes Produkt, welches auch vom PrSG erfasst ist, eine Regelung, mit der dasselbe Ziel verfolgt wird, dann kommt gem. der Botschaft[635] und der h.L.[636] der Erlass mit dem höheren Schutz- bzw. Sicherheitsniveau zum fraglichen Gegenstand zur Anwendung. 164

628 Ebenso SECO, FAQ, S. 2.

629 Art. 1 Abs. 3 PrSG; Wey, in: Fellmann/Furrer, Schonzeit, S. 35.

630 Art. 1 Abs. 3 PrSG.

631 Pfenninger/Schild haben ein von der – hier gefolgten – h.L. abweichendes Verständnis vom «selben Ziel» gem. Art. 1 Abs. 3 PrSG, was zu einer abweichenden Meinung bezüglich des Vorrangs der Sektorrechte führt, Pfenninger/Schild, in: Fellmann/Furrer, Herausforderungen, S. 31; überzeugend diskutiert in Wey, in: Fellmann/Furrer, Schonzeit, S. 37.

632 Botschaft PrSG, S. 7408, 7433; siehe ausführliche Diskussion in Wey, in: Fellmann/Furrer, Schonzeit, S. 37 f.; zuletzt ebenso Hess, in: Häner/Waldmann S. 222; a.A. Pfenninger/Schild, in: Fellmann/Furrer, Herausforderungen, S. 31. S. o., Rn. 148.

633 Botschaft PrSG, S. 7433.

634 SHK PrSG-Hess, Einleitung N 88 Fn. 335, m.w.H.

635 Botschaft PrSG, S. 7433.

636 Wildhaber/Rey, Rn. 1498; Fornage, in: Chappuis/Winiger/Campi S. 212; Wey, in: Fellmann/Furrer, Schonzeit, S. 37 f. m.w.H. und ausführlicher Diskussion; Bühler/Tobler, S. 368; SHK PrSG-Hess, Art. 1 N 8 und Einleitung N 88 Fn. 335; Holliger-Hagmann, Fallstricke, S. 97 f.

165 Der kleinere, aber neuere Teil der Lehre und das SECO[637] vertreten die Meinung, dass die sektoriellen Erlasse dem PrSG in jedem Fall – also auch bei einem tieferen Schutzniveau – vorgehen, wenn mit einer Regelung dasselbe Ziel verfolgt wird.[638] GERSTER hält fest, dass diese Interpretation der Absicht des PrSG zwar widerspreche, eine andere Ansicht jedoch «einen gesetzestechnischen Fehler offenbaren» würde.[639] Zieht man die Kritik am PrSG in Betracht, ist diese Annahme nicht unbegründet.[640] PFENNINGER spricht sich zudem dagegen aus, «dass die Inverkehrbringer neben der Beachtung der einschlägigen Sektorrechte jedes Mal noch die unzähligen nationalen Umsetzungsgesetze auf ‹weiter gehende› Sicherheitsanforderungen hin überprüfen müssen».[641] Mit dem Erlass der Produktsicherheitsverordnung, welche in den EU-Mitgliedstaaten direkt anwendbar ist (im Gegensatz zur alten Produktsicherheitsrichtlinie), fällt die Prüfung nationaler Umsetzungsgesetze nun weg.[642] Beachtet werden muss in der Schweiz weiterhin das PrSG, da die Verordnung auf die Schweiz als Nicht-EU-Staat keine direkte Wirkung hat.

166 Die verschiedenen Argumente der neueren Lehre überzeugen, wie soeben dargelegt, nicht. Die Bestimmung mit dem höheren Schutzniveau muss jeweils vorgehen. Ein gemeinsames Schutzniveau bezüglich der Sicherheit und Gesundheit von natürlichen Personen vor gefährlichen Konsumentenprodukten sowie die wirtschaftliche Kompatibilität mit der EU sind die Hauptziele des PrSG.[643] Würde im Sektorrecht nun ein tieferes Schutzniveau verankert und ginge dieses dem PrSG vor, könnten beide Ziele nicht mehr adäquat erreicht werden: Der Sicherheitsstandard in der Schweiz wäre gegenüber jenem der EU tiefer[644] und die wirtschaftliche Kompatibilität wäre deshalb nicht mehr gegeben. Die einzige Ausnahme wäre, wenn auch das EU-Sektorrecht, welches im MRA ein Schweizer Pendant hat, ein tieferes Schutzniveau als das PrSG vor-

637 SECO, FAQ, S. 1.

638 Mit Ausnahme von WILDHABER/REY, Rn. 1498; PFENNINGER/SCHILD folgend, BSK OR I-FELLMANN, Vorbemerkungen zum PrHG 4d; GERSTER, Rn. 17 mit ausführlicher Diskussion in Rn. 13 ff.; PFENNINGER, S. 1166; PFENNINGER/SCHILD, in: Fellmann/Furrer, Herausforderungen, S. 30 spezifisch bezogen auf die Nachmarktpflichten gem. Art. 8 PrSG S. 31.

639 GERSTER, Rn. 18.

640 Bspw. die «unsorgfältige Gesetzesredaktion» kritisierend FURRER, in: Fellmann/Furrer, Schonzeit, S. 90.

641 PFENNINGER, S. 1167.

642 HARTMANN/KLINDT, S. 73.

643 S. o., Rn. 146.

644 WEY, in: Fellmann/Furrer, Schonzeit, S. 37 f. m.w.H.

schreiben würde.[645] Würde dann das Schweizer Sektorrecht dem Schutzniveau des EU-Sektorrechts folgen, wäre die wirtschaftliche Kompatibilität mit der EU weiterhin gegeben, ohne das hohe Schutzniveau des PrSG zu beachten.

IV. Vorrang des Sektorrechts in der EU

Die GPSR gilt immer dann, wenn die Sicherheit eines Produktes nicht in einem anderen EU-Sektorerlass, der dasselbe Ziel verfolgt, speziell geregelt ist.[646] Die GPSR ist im Verhältnis zu den EU-Harmonisierungsvorschriften und anderen spezifischeren Sicherheitsvorschriften Lex generalis.[647] Hat ein Produkt bereits spezielle EU-Vorschriften, haben diese somit Vorrang vor der GPSR – der Meinung von SCHUCHT/WIEBE nach – unabhängig davon, ob sie ein höheres oder niedrigeres Schutzniveau bieten.[648] Besteht also eine Regelung und ist ihr Schutzniveau geringer als jenes der GPSR, findet nicht die GPSR, sondern die entsprechende Harmonisierungsvorschrift Anwendung.[649] Ergänzend kommt die GPSR dort zur Anwendung, wo die speziellen Vorschriften Regelungslücken aufweisen.[650] 167

Gem. Art. 2 Abs. 1 Uabs. 3 lit. b GPSR sind Produkte, die spezifischen Anforderungen der Harmonisierungsrechtsvorschriften der Union im Sinne des Art. 3 Ziff. 27 GPSR unterliegen, von Kapitel III Abschnitt 1 ausgenommen. Art. 3 Ziff. 27 GPSR umfasst als «Harmonisierungsrechtsvorschriften der Union» die in Anhang I der MÜVO aufgeführten Rechtsvorschriften der Union sowie alle sonstigen Rechtsvorschriften der Union zur Harmonisierung der Bedingungen für die Vermarktung von Produkten, auf die jene Verordnung Anwendung findet. Das ist bspw. die LVD (gem. Anhang I Ziff. 54 MÜVO). In Kapitel III Abschnitt 1 GPSR sind die Pflichten der Wirtschaftsakteure geregelt (z.B. Art. 9 GPSR). Enthält die LVD somit spezifische Nachmarktpflichten für Hersteller mit dem gleichen Ziel wie jene in Art. 9 GPSR, sind die GPSR-Pflichten nicht anwendbar (gem. SCHUCHT/WIEBE sogar, wenn sie ein tieferes Schutzniveau 168

645 Siehe auch BGE 143 II 518, 548 E. 9.4 (jedoch mit Bezug zur Konformität) feststellend, dass in der Schweiz bei gleichwertiger Rechtsgrundlage kein höheres Schutzniveau verlangt werden darf als in der EU.

646 Art. 2 Abs. 1 Uabs. 1, ErwG 8 GPSR.

647 NHK GPSR-WILRICH, Art. 2 N 19.

648 NHK GPSR-SCHUCHT/WIEBE, Einleitung N 33 mit Verweis auf sich selbst; NP GPSR-SCHUCHT/WIEBE, § 3 N 66.

649 NP GPSR-SCHUCHT/WIEBE, § 3 N 66.

650 Art. 2 Abs. 1 Uabs. 2 und 3, ErwG 6 GPSR; siehe auch NP GPSR-SCHUCHT/WIEBE, § 3 N 66.

verlangen).[651] Hierbei muss aber jede einzelne Pflicht geprüft werden.[652] Die KI-VO ist in Anhang I MÜVO nicht aufgeführt. Art. 74 Abs. 1 KI-VO erklärt die MÜVO jedoch auf KI-Systeme, die unter die KI-VO fallen, anwendbar.

V. Sektorrecht mit Relevanz für KI-Produkte

169 In Kapitel Teil 1:D.I wurden einige gefährliche Produkte beschrieben. Komplex ist, dass diese Produkte unter viele verschiedene Sektorerlasse fallen. Rasenmähroboter etwa fallen in der Schweiz unter die Maschinenverordnung[653] (Art. 1 Abs. 2 MaschV i.V.m. Art. 3 Ziff. 1 MRL[654])[655] und als Funkanlagen unter die Verordnung über Fernmeldeanlagen (FAV)[656], wenn sie bspw. mit einer Ladestation oder einem Smartphone über Funkwellen Informationen austauschen. Sie werden nicht als Haushaltsgeräte klassifiziert.[657] Küchenroboter, Katzentoiletten und Staubsaugerroboter fallen in der Schweiz als Haushaltsgeräte (je nach Spannung) gem. Art. 1 Abs. 1 NEV[658] aufgrund des Ausschlusses nach Art. 1 Abs. 2 MaschV i.V.m. Art. 1 Abs. 2 lit. k MRL[659] auch unter die Verordnung für elektrische Niederspannungserzeugnisse (NEV). Auch in der EU fallen Smart Home Devices grundsätzlich in den harmonisierten Bereich, da auf sie verschiedene EU-Harmonisierungsvorschriften anwendbar sind.[660] Der Hersteller des Moley-Küchenroboters gibt bspw. an, dass er u.a. die MRL und die EMV-RL[661] einhält.[662] Aufgrund des

651 NP GPSR-Schucht/Wiebe, § 9 N 21.
652 NP GPSR-Schucht/Wiebe, § 9 N 21.
653 Verordnung über die Sicherheit von Maschinen (Maschinenverordnung) vom 2. April 2008, SR 819.14 (zit. MaschV).
654 Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung), (Maschinenrichtlinie), ABl. L 157/24 (zit. MRL).
655 Ein enstprechender Hinweis findet sich in Leitlinie LVD, S. 80.
656 Verordnung über Fernmeldeanlagen vom 25. November 2015, SR 784.101.2, Art. 2 Abs. 1 lit. a (zit. FAV).
657 Leitlinie LVD, S. 80.
658 Verordnung über elektrische Niederspannungserzeugnisse (Niederspannungsverordnung) vom 25. November 2015, SR 734.26 (zit. NEV).
659 Art. 1 Abs. 2 lit. k MRL verweist auf die Richtlinie 73/23/EWG des Rates vom 19. Februar 1973 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen, ABl. L 77/29, welche mittlerweile durch die LVD ersetzt wurde.
660 Piovano/Schucht/Wiebe, S. 9.
661 Richtlinie 2014/30/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit (Neufassung), ABl. L 96/79 (zit. EMV-RL).
662 Safety Standards and Certification, FAQ – Moley Robotics, abrufbar unter <https://www.moley.com/faq/>, zuletzt besucht am 31.05.2025.

MRA hat die Schweiz eine Reihe von Sektorerlassen, die jeweils gleichwertig wie die europäischen Sektorerlasse sind.[663]

Es liegt nahe, dass Produkte mit Software- und KI-Komponenten im Zusammenhang mit elektrischen Erzeugnissen geregelt sein könnten. Die Sicherheit elektrischer Erzeugnisse wird grundsätzlich durch die Vorschriften der Elektrizitätsgesetzgebung bestimmt.[664] Dazu gehören verschiedene Verordnungen, die gestützt auf das EleG[665] erlassen wurden, und das EleG selbst. Die Botschaft zum PrSG hielt 2008 noch fest, dass die auf das Elektrizitätsgesetz gestützten Verordnungen «im Allgemeinen» keine Nachmarktpflichten für Hersteller beinhalten, somit das PrSG zur Anwendung komme und deshalb keine Änderung der «Gesetzgebung über die Sicherheit von elektrischen Erzeugnissen» nötig sei.[666] Mittlerweile wurden viele Verordnungen trotzdem angepasst, sodass sie nun Nachmarktpflichten für Hersteller enthalten. Da Software und damit KI in mehreren Verordnungen gleichzeitig geregelt sein können, soll im Folgenden auf die relevantesten Verordnungen eingegangen werden. In Bezug auf Smart Home Devices sind in der Schweiz vorwiegend die NEV und die FAV (welche jedoch teilweise auf die NEV verweist) anwendbar, weshalb genauer auf diese Verordnungen eingegangen wird. In der Schweiz und der EU existieren zahlreiche sektorielle Erlasse, weshalb beispielhaft einige ausgewählte Kategorien aus dem MRA ebenfalls angesprochen werden, die für Smart Home Devices gelten könnten. 170

1. Elektrische Betriebsmittel und elektromagnetische Verträglichkeit

Die Niederspannungsverordnung (NEV) regelt Sicherheitsanforderungen für elektrische Niederspannungserzeugnisse. Die Ziele der NEV sind die Gewährleistung der Sicherheit von Personen, Haustieren und Sachen[667] sowie die Förderung des freien Warenverkehrs zwischen der Schweiz und der EU[668]. Die NEV betrifft also die Sicherheit elektrischer Geräte und Komponenten, die bei 171

663 S. o., Rn. 64.

664 Botschaft PrSG, S. 7424.

665 Bundesgesetz betreffend die elektrischen Schwach- und Starkstromanlagen (Elektrizitätsgesetz) vom 24. Juni 1902, SR 734.0 (zit. EleG).

666 Botschaft PrSG, S. 7424; siehe auch Holliger-Hagmann, Fallstricke, S. 98.

667 Art. 3 NEV lautet: «Niederspannungserzeugnisse dürfen nur auf dem Markt bereitgestellt werden, wenn sie den anerkannten Regeln der Technik entsprechen und bei bestimmungsgemässem Aufbau, Unterhalt und Gebrauch die Sicherheit von Personen, Haustieren und Sachen nicht gefährden».

668 UVEK, Erläuternder Bericht Revision NEV, S. 1 f.

Niederspannung betrieben werden. Die NEV wurde gestützt auf das EleG, das PrSG und das THG erlassen.[669] Die NEV setzte die LVD ins Schweizer Recht um.[670]

172 Die NEV erfasst gem. Art. 1 Abs. 1 NEV elektrische Niederspannungserzeugnisse zur Verwendung mit einer Nennspannung von 50 V bis 1000 V Wechselspannung[671] oder von 75 V bis 1500 V Gleichspannung[672] im Sinne der LVD. Weiter gilt sie nach Art. 1 Abs. 2 NEV für Niederspannungserzeugnisse mit einer Betriebsspannung unter 50 V Wechselspannung und 75 V Gleichspannung (lit. a) und für jene, die in Anhang II der EU-LVD aufgelistet sind, ausser wenn deren elektrische Sicherheit in Spezialerlassen[673] geregelt ist (lit. b).[674] Dies können z.B. Smart Home Devices wie Smartspeaker, Überwachungskameras und Alarmanlagen sein. Nicht unter die NEV fällt Software. Software kann aber in verschiedenen Niederspannungserzeugnissen eingesetzt werden, die in den Anwendungsbereich der NEV fallen. Auch wenn sie durch die Integration in ein Smartphone oder einen PC «verkörperlicht» wird,[675] handelt es sich bei Software nicht um ein Niederspannungserzeugnis. Ist Software in ein Niederspannungserzeugnis integriert und das Produkt insgesamt gefährlich, handelt es sich um ein gefährliches Niederspannungserzeugnis. Wenn das Gefahrenpotenzial in diesem Fall allein in der Software liegt, ist jedoch nicht die NEV für die Softwarekomponente anwendbar, sondern das PrSG als Auffanggesetz. Dies ist bspw. der Fall, wenn die Ursache der Gefahr in der fehlerhaften automatischen Bilderkennung liegt.[676] Die NEV findet bei Produkten mit Software und KI nur da Anwendung, wo die Ursache der Gefahr in einer physischen Komponente (also dem Niederspannungserzeugnis selbst) liegt (z.B. ein

669 Ingress NEV.

670 UVEK, Erläuternder Bericht Revision NEV, S. 1; siehe auch BVGer A-727/2016 vom 13.07.2016, E. 6.

671 Z.B. Waschmaschinen und Kühlschränke, siehe dazu Vorsicht vor billigen elektrischen Geräten aus dem Ausland, abrufbar unter <https://energeiaplus.com/2024/02/14/vorsicht-vor-billigen-elektrischen-geraeten-aus-dem-ausland/>, zuletzt besucht am 31.05.2025.

672 Z.B. Radios, Computer, Spielkonsolen, siehe dazu Vorsicht vor billigen elektrischen Geräten aus dem Ausland, abrufbar unter <https://energeiaplus.com/2024/02/14/vorsicht-vor-billigen-elektrischen-geraeten-aus-dem-ausland/>, zuletzt besucht am 31.05.2025.

673 Das wäre z.B. bei Maschinen, die unter die MaschV fallen, der Fall.

674 Weitere Beispiele für elektrische Niederspannungserzeugnisse sind: Mobiltelefone und Powerbanks BVGer A-4413/2021 vom 20.09.2023, A.; Haushaltssteckvorrichtungen BVGer A-727/2016 vom 13.07.2016, E .5.1.1; automatische Rasenmäher mit entsprechendem Navigationssystem BVGer A-5814/2009 vom 24.08.2010, A. i.V.m E. 4.9.

675 S. o., Rn. 79.

676 Siehe dazu das Beispiel unten, Rn. 335.

Stromschlag oder ein Überhitzen eines Produktes aufgrund einer unsicheren Isolierung eines Kabels).[677]

Smart Home Devices können elektromagnetische Störungen verursachen und ihr Betrieb kann durch solche beeinträchtigt werden. Sie sind deshalb gem. Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 lit. a und lit. b VEMV[678] von der Verordnung über die elektromagnetische Verträglichkeit (VEMV) erfasst. Die VEMV dient nicht primär der Produktsicherheit, sondern der Verhinderung von elektromagnetischen Störungen.[679] Ihr fehlt bspw. ein Verweis auf die Sicherheit und Gesundheit von Personen. Sie stützt sich dementsprechend lediglich auf das EleG, das FMG und das THG, jedoch nicht auf das PrSG und wird vorliegend nicht näher betrachtet. 173

Die NEV, die VEMV und die LVD sind Teil des MRA.[680] 174

2. Funkanlagen und Telekommunikationsendgeräte

Die Verordnung über Fernmeldeanlagen verlangt in Art. 7 Abs. 1 FAV, dass Funkanlagen «den Schutz der Gesundheit und der Sicherheit von Menschen und Haus- und Nutztieren sowie den Schutz von Gütern, einschliesslich der in der [...] NEV enthaltenen Ziele in Bezug auf die Sicherheitsanforderungen, aber ohne Spannungsgrenze» (lit. a) und «ein angemessenes Niveau an elektromagnetischer Verträglichkeit nach der Verordnung [...] über die elektromagnetische Verträglichkeit (VEMV)» (lit. b) gewährleisten müssen. Die FAV wurde gestützt auf das FMG und das THG erlassen.[681] Fernmeldeanlagen sind Teil des MRA.[682] Während das BAKOM die zuständige Behörde für die Kontrolle der in der FAV[683] (Art. 41 FAV) und dem FMG (Art. 33 Abs. 1 FMG) festgelegten Vorschriften ist, liegt «die Kontrolle der Aspekte betreffend den Schutz der 175

677 Siehe auch die Abkehr von Produkt zu Niederspannungserzeugnis bei der Teilrevision der NEV in UVEK, Erläuternder Bericht Revision NEV, S. 2.

678 Verordnung über die elektromagnetische Verträglichkeit vom 25. November 2015, SR 734.5 (zit. VEMV).

679 Art. 1 Abs. 1 VEMV.

680 Anhang 1, Kapitel 9, Abschnitt I MRA; siehe auch UVEK, Erläuternder Bericht Revision NEV, S. 2.

681 Ingress FAV.

682 Anhang 1, Kapitel 9, Abschnitt 1 und Kapitel 7, Abschnitt I MRA; siehe auch Botschaft FMG, S. 6640 f.

683 Art. 41 FAV.

Gesundheit und Sicherheit» nach Art. 7 Abs. 1 lit. a FAV bei der Vollzugsbehörde der NEV,[684] also dem ESTI[685].

176 Eine Funkanlage ist gem. Art. 2 Abs. 1 lit. a FAV «ein elektrisches oder elektronisches Erzeugnis, das per Funkwellen bewusst Informationen sendet oder empfängt, oder ein elektrisches oder elektronisches Erzeugnis, das Zubehör, wie eine Antenne, benötigt, damit es per Funkwellen bewusst Informationen senden oder empfangen kann». Dies trifft auf IoT-Geräte und damit wohl auf die allermeisten Smart Home Devices zu, solange diese mittels Funkwellen (z.B. Wi-Fi, Bluetooth) mit anderen Geräten kommunizieren.[686] Unterschieden wird in Art. 10 Abs. 1 FAV zwischen «Herstellerinnen von Funkanlagen» und «Herausgeberinnen von Software, die die bestimmungsgemässe Nutzung dieser Anlagen ermöglicht». Die Software für den Betrieb der Funkanlage wird gem. Art. 19 Abs. 1 FAV als «Bestandteil» der Funkanlage verstanden. Die Software selbst ist aber keine Funkanlage nach Art. 2 Abs. 1 lit. a FAV, da sie kein elektrisches oder elektronisches Erzeugnis ist.

177 Die Funkanlagenrichtlinie 2014/53/EU (RED)[687] verweist in Art. 3 Abs. 1 lit. a RED darauf, dass Funkanlagen so gebaut sein müssen, dass der Schutz der Gesundheit und Sicherheit von Menschen, Haus- und Nutztieren sowie von Gütern gewährleistet ist. Zudem müssen die in der LVD enthaltenen Ziele in Bezug auf die Sicherheitsanforderungen (ohne Anwendung der Spannungsgrenze) gewährleistet sein.[688] In diesem Zusammenhang hält Art. 1 Abs. 4 RED fest, dass Funkanlagen, die in den Anwendungsbereich der RED fallen, nicht von der LVD erfasst sind – mit Ausnahme der obengenannten Fälle nach Art. 3 Abs. 1 lit. a RED. Funkanlagen fallen in der EU also in erster Linie unter die RED und nicht unter die LVD.[689] Art. 3 Abs. 1 lit. i RED hält fest, dass Funkanlagen so gebaut sein müssen, dass sie

684 Art. 36 Abs. 1 FAV.

685 S. u., Rn. 381.

686 Denkbar sind Smart Home Devices, welche zwar Software oder sogar ein trainiertes KI-System enthalten, aber nicht mit anderen Geräten verbunden sind. Die momentan auf dem Markt erhältlichen Geräte können jedoch zumeist via App auf einem Smartphone gesteuert werden und senden deshalb Funkwellen aus und fallen damit unter die FAV. Weitere Beispiele für Funkanlagen sind: Funkgeräte, BVGer A-5896/2023 vom 05.11.2024, A. i.V.m. E. 5.4.1; automatische Rasenmäher mit entsprechendem Navigationssystem, BVGer A-5814/2009 vom 24.08.2010, A. i.V.m E. 4.9.

687 Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (Radio Equipment Directive), ABl. L 153/62 (zit. RED).

688 Art. 3 Abs. 1 lit. a RED.

689 Siehe auch: Leitlinie LVD, S. 83; Europäische Kommission, Blue Guide, S. 25 Fn. 72 f.

bestimmte Funktionen unterstützen, «mit denen sichergestellt werden soll, dass nur solche Software geladen werden kann, für die die Konformität ihrer Kombination mit der Funkanlage nachgewiesen wurde». Art. 4 Abs. 1 RED verlangt, dass Informationen über die Konformität von Kombinationen aus Funkanlagen und Software, die die bestimmungsgemässe Nutzung von Funkanlagen ermöglichen, bereitgestellt werden müssen. Sie geht somit zwar auf Software ein, definiert diese aber nicht als Funkanlage oder eigenständiges Produkt.[690]

3. Maschinen

Die MaschV wurde u.a. gestützt auf das PrSG und das EleG erlassen und stützt sich weitgehend auf die MRL[691].[692] Seit dem 20. Januar 2024 stützt sich die Schweizer MaschV in einem Fall auf die neue MVO. Diese hält in Art. 3 Abs. 3 MVO fest, dass Sicherheitsbauteile auch Software sein können. Die MaschV ist gem. Art. 1 Abs. 1 MaschV i.V.m. Art. 1 Abs. 2 lit. k MRL nicht auf Haushaltsgeräte anwendbar,[693] weshalb sie für die vorliegend genauer untersuchten Smart Home Devices nicht relevant ist. Auch die MVO ist gem. Art. 2 Abs. 2 lit. p Ziff. i MVO nicht auf elektrische Haushaltsgeräte anwendbar, sofern diese unter den Anwendungsbereich der LVD oder der RED fallen. 178

4. Medizinprodukte

Die MepV[694] wurde u.a. gestützt auf das PrSG und das EleG erlassen.[695] Sie ist Teil des MRA.[696] Gem. Art. 3 Abs. 1 MepV kann explizit auch Software als ein Medizinprodukt gelten. Dies entspricht der Regelung in der EU, wo die MDR in 179

690 A.A. Beck KI-VO-Ruschemeier, Art. 6 N 70, mit Verweis auf Martini, in: Hilgendorf/Roth-Isigkeit, § 4 Rn. 41 Fn. 68.

691 Gem. Art. 1 Abs. 1 Fn. 6 MaschV ist die MRL in der Fassung «Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung), ABl. L 157 vom 9.6.2006, S. 24; zuletzt geändert durch Richtlinie 2014/33/EU, ABl. L 96 vom 29.3.2014, S. 251» massgebend.

692 Siehe auch Freytag, S. 25.

693 Als Haushaltsgeräte sind Geräte für typische Haushaltsfunktionen wie Waschen, Reinigen, Heizen, Kühlen, Kochen usw. bestimmt. Als Beispiele werden Waschmaschinen, Geschirrspüler, Staubsauger und Kochgeräte genannt. Elektrische Gartengeräte oder Elektrowerkzeuge fallen jedoch nicht unter diesen Ausschluss, weshalb Rasenmäher als Maschinen zu klassifizieren sind, Leitlinie LVD, S. 80.

694 Medizinprodukteverordnung vom 1. Juli 2020, SR 812.213 (zit. MepV).

695 Ingress, MepV.

696 Anhang 1, Kapitel 4, Abschnitt 1 MRA.

Art. 2 Ziff. 4 Software ebenfalls als eigenständiges Produkt erfasst.[697] Die Produktbeobachtung ist in Kapitel 7, Art. 56 ff. MepV geregelt. Medizinprodukte werden vorliegend nicht genauer untersucht. Smart Home Devices sind üblicherweise keine Medizinprodukte, weil sie nicht dazu bestimmt sind, Krankheiten zu erkennen, zu verhüten, zu überwachen, vorherzusagen, zu behandeln oder zu lindern.[698]

5. Spielzeug

180 Die Verordnung des EDI über die Sicherheit von Spielzeug (VSS)[699] wurde gestützt auf die Lebensmittel- und Gebrauchsgegenständeverordnung (LGV)[700] erlassen.[701] Sie gilt für Spielzeug nach Art. 65 LGV.[702] Art. 65 LGV hält fest, dass als Spielzeug alle Gegenstände gelten, die dazu bestimmt oder gestaltet sind, von Kindern bis vierzehn Jahren zum Spielen verwendet zu werden. Um als Spielzeug zu gelten, muss ein Gegenstand nicht ausschliesslich für den Zweck des Spielens vorgesehen sein. Gem. Art. 1 Abs. 2 VSS gelten Gegenstände nach Anhang 1 Ziff. I nicht als Spielzeug. Dazu gehören nach Anhang 1 Ziff. 1 Ziff. 12 VSS bspw. «funktionelle Lernprodukte wie Kochherde, Bügeleisen und andere funktionelle Produkte, die mit einer Nennspannung von mehr als 24 Volt betrieben und ausschliesslich für didaktische Zwecke zur Verwendung unter Aufsicht einer erwachsenen Person verkauft werden». Smart Home Devices sind i.d.R. nicht für Kinder gedacht und fallen somit nicht unter die VSS.

181 Das Bundesgesetz über Lebensmittel und Gebrauchsgegenstände (LMG)[703] und die LGV sind in Bezug auf Spielzeug Teil des MRA.[704] Lebensmittel und Gebrauchsgegenstände werden ebenfalls in Spezialgesetzen reguliert. Das LMG bezweckt primär, die Gesundheit von Konsumenten vor unsicheren Lebens-

697 Siehe im Detail auch WAGNER, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 164.

698 Art. 3 Abs. 1 lit. c Ziff. 1 MepV. Die Nennung dieser Bestimmung ist als Veranschaulichungsbeispiel gedacht. Auch die übrigen in Art. 3 MepV genannten Voraussetzungen treffen nicht auf Smart Home Devices zu.

699 Verordnung des EDI über die Sicherheit von Spielzeug (Spielzeugverordnung) vom 15. August 2012, SR 817.023.11 (zit. VSS).

700 Lebensmittel- und Gebrauchsgegenständeverordnung vom 16. Dezember 2016, SR 817.02 (zit. LGV).

701 Ingress VSS.

702 Art. 1 Abs. 1 VSS.

703 Bundesgesetz über Lebensmittel und Gebrauchsgegenstände (Lebensmittelgesetz) vom 20. Juni 2014, SR 817.0 (zit. LMG).

704 Anhang 1, Kapitel 3, Abschnitt 2 MRA.

mitteln und Gebrauchsgegenständen zu schützen.[705] Es wurde gestützt auf Art. 91 Abs. 1, Art. 105 und Art. 118 Abs. 2 lit. a BV erlassen.[706] Das Herstellen von Lebensmitteln und Gebrauchsgegenständen wird in der LGV geregelt.[707] Diese wurde gestützt auf das LMG, USG[708], GTG[709], PrSG und das THG erlassen.[710] Gebrauchsgegenstände sind insbesondere Erzeugnisse, die typischerweise unmittelbar mit dem menschlichen Körper in Kontakt kommen.[711] Art. 5 lit. a Ziff. 1 LMG hält fest, dass Gegenstände, die dazu bestimmt sind, mit Lebensmitteln in Berührung zu kommen, unter die Kategorie der Gebrauchsgegenstände (als sog. Bedarfsgegenstände) fallen. Denkbar wäre also, dass Smart Home Devices wie Backöfen oder Wasserkocher unter das LMG fallen. Die Anforderungen in Art. 49 Abs. 1 LGV bestimmen, dass Bedarfsgegenstände direkt oder indirekt Stoffe nur in Mengen an Lebensmittel abgeben dürfen, die gesundheitlich unbedenklich (lit. a), technisch unvermeidbar (lit. b) sind und keine unvertretbare Veränderung der Zusammensetzung oder Beeinträchtigung der organoleptischen[712] Eigenschaften der Lebensmittel herbeiführen (lit. c). Die oben beschriebenen Gefahren durch Software und KI in Smart Home Devices könnten zwar die gerade beschriebenen Gefahren mittelbar auslösen (z.B. durch Überhitzung), werden aber durch die LGV primär nicht erfasst, da sich deren Regelungsziel auf die stoffliche Sicherheit und physikalisch-chemische Eigenschaften bezieht, nicht aber auf funktionale Risiken, die etwa durch Software entstehen können. Es wird deshalb vorliegend nicht weiter auf die Bestimmungen des LMG und der LGV eingegangen.

VI. Fazit

Das schweizerische und europäische Produktsicherheitsrecht haben zwei Hauptaufgaben: Erstens soll die Sicherheit und Gesundheit von Menschen geschützt werden, indem die Gefahren, die von Produkten ausgehen, abgewen- 182

705 Art. 1 lit. a LMG; Botschaft LMG, S. 5594.

706 Ingress LMG.

707 Art. 1 lit. a LGV.

708 Bundesgesetz über den Umweltschutz (Umweltschutzgesetz) vom 7. Oktober 1983, SR 814.01 (zit. USG).

709 Bundesgesetz über die Gentechnik im Ausserhumanbereich (Gentechnikgesetz) vom 21. März 2003, SR 814.91 (zit. GTG).

710 Ingress LGV.

711 Art. 5 LMG; BÜHLER, Sicherheit, Rn. 22.

712 Organoleptisch bedeutet «Lebensmittel nach einem bestimmten Bewertungsschema in Bezug auf Eigenschaften wie Geschmack, Aussehen, Geruch, Farbe ohne Hilfsmittel, nur mit den Sinnen prüfend», Organoleptisch, abrufbar unter <https://www.duden.de/rechtschreibung/organoleptisch>, zuletzt besucht am 31.05.2025.

det werden, und zweitens sollen Handelshemmnisse zwischen der EU und der Schweiz bzw. innerhalb der EU beseitigt werden. Die Beseitigung von technischen Handelshemmnissen ist für die Schweiz aus wirtschaftlicher Sicht essenziell.[713] Exporte und Importe werden massiv erleichtert und die Schweiz bleibt dadurch wettbewerbsfähig.[714] Viele Regelungen befinden sich in sektorrechtlichen Erlassen, weil die Produktsicherheitsanforderungen vom Produkttyp abhängig und einheitliche Regelungen nicht immer zweckmässig sind. Für Smart Home Devices sind in der Schweiz vor allem die NEV und die FAV relevant, welche beide Teil des MRA sind und nicht nur natürliche Personen schützen. Wo einheitliche Regelungen doch sinnvoll sind, wird die Produktsicherheit horizontal geregelt. In der Schweiz findet dies im PrSG und in der EU in der GPSR statt. Beide Erlasse sind Auffanggesetze und lediglich subsidiär anwendbar mit einigen Ausnahmen. In der Schweiz muss die gesetzliche Grundlage für eine vom PrSG abweichende Regelung im Sektorrecht genügend sein. Des Weiteren geht das PrSG vor, wenn das Sektorrecht keine Regelung enthält. Beinhaltet das PrSG Bestimmungen, die ein höheres Schutzniveau als das Sektorrecht vorgeben, geht ebenfalls das PrSG vor. Eine Ausnahme könnte in Betracht gezogen werden, wenn EU-Sektorrecht, welches vom MRA erfasst ist, ein tieferes Schutzniveau vorgeben würde als das PrSG. Dann könnte auch in der Schweiz am tieferen Schutzniveau des entsprechenden Schweizer Sektorerlasses festgehalten werden, weil die wirtschaftliche Kompatibilität gewahrt bleiben würde. Fraglich ist dann, welches Ziel des PrSG höher gewertet wird. In der EU geht ebenfalls das spezifischere Produktsicherheitsrecht vor. Wenn das spezifische Sektorrecht jedoch keine Regelung enthält, kommt die GPSR ergänzend zur Anwendung. Gem. SCHUCHT/WIEBE gibt die GPSR kein Mindestschutzniveau vor, weshalb in der EU sektorrechtliche Bestimmungen der GPSR wohl vorgehen, auch bei einem niedrigeren Schutzniveau.

183 Die Nachmarktpflichten des PrSG sind demnach immer anwendbar, wenn das Sektorrecht weniger weitgehende Nachmarktpflichten vorsieht als jene aus dem PrSG.[715] Verlangt der Sektorerlass jedoch gleich weitgehende oder weitergehende Nachmarktpflichten als das PrSG, geht der Sektorerlass vor. In der EU gehen die Nachmarktpflichten des Sektorrechts vorbehaltlos der GPSR vor. Enthält die GPSR jedoch Bestimmungen, die im Sektorrecht fehlen, wird die GPSR ergänzend angewandt. Somit sind in der EU für KI-Systeme primär die Nachmarktpflichten der KI-VO anzuwenden und nicht jene der GPSR. Enthält

713 Siehe auch HÄNSENBERGER, Drohnen, S. 229.
714 S. o., Rn. 64.
715 WEY, in: Fellmann/Furrer, Schonzeit, S. 36 f., 60.

die GPSR aber ergänzende Nachmarktpflichten, müssen diese (mindestens, wenn KI-Systeme als Produkte anerkannt werden) ebenfalls beachtet werden.

184 Im Gegensatz zur GPSR erstrecken sich die Sicherheitsanforderungen des PrSG grundsätzlich auf alle Produkte und nicht nur auf Konsumentenprodukte. Eine Ausnahme sind die Nachmarktpflichten nach Art. 8 PrSG. Auch die KI-VO erstreckt sich auf alle KI-Systeme und enthält keine Einschränkung auf Konsumentenprodukte. Die Nachmarktpflichten der KI-VO sind also auch auf B2B-KI-Systeme anwendbar.

Teil 3: Produktsicherheitsrechtliche Nachmarktpflichten für Hersteller (bzw. Anbieter) von Software und KI

In diesem Kapitel wird dargestellt, inwiefern Smart Home Devices und Software inklusive KI als Produkte im Produktsicherheitsrecht erfasst sind, was der Schutzumfang ist und wer als Hersteller gilt, der Nachmarktpflichten erfüllen muss. Weiter wird geklärt, was überhaupt eine Inverkehrbringung ist, da es sich hier um die zeitliche Abgrenzung zum Beginn der Nachmarktpflichten handelt. Danach wird dargelegt, was die Nachmarktpflichten beinhalten. Zuletzt wird geklärt, wie lange die Nachmarktpflichten beachtet werden müssen. 185

A. Smart Home Devices und Software als Produkte

186 Ziel dieses Kapitels ist es, zu klären, inwiefern Smart Home Devices sowie Software und KI als Produkte i.S.d. PrSG und der GPSR klassifiziert werden können. Bereits vorweggenommen wurde, dass in der Schweiz auf Smart Home Devices die NEV und die FAV anwendbar sein können. Smart Home Devices können Niederspannungserzeugnisse sowie Funkanlagen sein. Reine Software ist jedoch weder ein Niederspannungserzeugnis noch eine Funkanlage, weshalb sie «stand-alone» nicht unter die NEV und die FAV fallen kann. Zu prüfen ist daher, ob Software unter das PrSG fällt. Dafür wird der Produktbegriff des PrSG genauer untersucht und mit dem europäischen produktsicherheitsrechtlichen Produktbegriff verglichen. Da die EU mit der KI-VO eine eigenständige Regulierung für KI-Systeme hat, wird diese miteinbezogen.

I. Vorbemerkung zu Konsumenten- und Migrationsprodukten

187 Im Gegensatz zur ehemaligen Produktsicherheitsrichtlinie[716] und der GPSR[717] sind in der Schweiz nicht nur Konsumentenprodukte vom allgemeinen Produktsicherheitsrecht erfasst.[718] Während das schweizerische Produktsicherheitsrecht also grundsätzlich auch für gewerbliche Produkte (B2B) gilt, gelten die Nachmarktpflichten gem. Art. 8 Abs. 1 PrSG nur für Konsumenten- und Migrationsprodukte (B2C).[719] Dies entsprach zum Zeitpunkt der Publikation der Botschaft auch dem europäischen Recht.[720] Da auch die GPSR lediglich Verbraucherprodukte erfasst, gelten auch deren Nachmarktpflichten nur für Konsumentenprodukte (B2C)[721]. Begründet wurde die Einschränkung der Nach-

716 Art. 2 Abs. 1 lit. a Produktsicherheitsrichtlinie.

717 ErwG 8 f., Art. 1 Abs. 2 und Art. 3 Ziff. 1 GPSR.

718 S. o., Rn. 147.

719 Es ist unbestritten, dass die Nachmarktpflichten nach Art. 8 PrSG nur für Konsumentenprodukte gelten, siehe bspw.: Heiss/Loacker, in: Heiss/Loacker, § 2 Rn. 2.24; Gerster, Rn. 268; Furrer, in: Fellmann/Furrer, Schonzeit, S. 83; Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 46 f.; SHK PrSG-Hess, Art. 8 N 4.

720 Konkret dem damaligen Recht der EG in der Produktsicherheitsrichtlinie, Botschaft PrSG, S. 7441 in Art. 5 Produktsicherheitsrichtlinie; siehe auch: Bühler/Tobler, S. 394; SHK PrSG-Hess, Art. 8 N 7.

721 Schucht, Informationspflichten, S. 397.

marktpflichten auf Konsumentenprodukte in der Schweiz mit dem generellen Bedürfnis nach besonderem Schutz für Konsumenten, der Angleichung der Regeln an das EU-Recht[722] und damit, dass Fachpersonen im Gegensatz zu «Normalverbrauchern» mehr Wissen und Erfahrung im Umgang mit «ihren» Produkten haben.[723] Produkte, die für Konsumenten sowie auch für Fachpersonen bestimmt sind oder durch Produktmigration von beiden Gruppen verwendet werden, werden Dual-Use-Produkte genannt und unterstehen ebenfalls den Nachmarktpflichten nach Art. 8 PrSG.[724] Auch die GPSR erfasst Migrations-[725] und Dual-Use[726]-Produkte.

188 Das PrSG enthält keine Legaldefinition des Begriffs «Konsument»[727] und in der Schweiz gibt es auch keinen einheitlichen Konsumentenbegriff[728]. Es handelt sich dabei aber immer nur um natürliche Personen.[729] Genauer um den letzten privaten Käufer (oder z.B. auch Mieter, Beschenkten etc.), welcher das Produkt nicht für gewerbliche oder berufliche Zwecke nutzt.[730] Mit Konsumentenprodukten sind also alle Produkte, die (auch) privat verwendet werden, gemeint.[731] In der Lehre werden die Begriffe «Konsum-» oder «Konsumentenprodukte» sowie «Konsumgüter» mehrheitlich synonym verwendet.[732] Ob ein Produkt für Konsumenten bestimmt ist, entscheidet in erster Linie der Hersteller. Er hat ein sog. Definitionsmonopol und kann das Produkt dem Konsum «widmen».[733] Hinweise auf die Eigenschaft als Konsumentenprodukt können neben konkreten Angaben auch die Bezeichnung des Produktes, die Art des Vertriebs und

722 Bühler/Tobler, S. 394.

723 Holliger-Hagmann, Fallstricke, S. 130; siehe auch Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 11.

724 SECO, FAQ, S. 6; Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 46 f.

725 NHK GPSR-Wilrich, Art. 3 N 30.

726 NHK GPSR-Wilrich, Art. 3 N 24.

727 Siehe auch Bühler/Tobler, S. 394.

728 Heiss, in: Heiss/Loacker, § 3 Rn. 3.1, m.w.H.

729 Brunner, in: Fellmann/Furrer, Schonzeit, S. 74; siehe auch Heiss, in: Heiss/Loacker, § 3 Rn. 3.2.

730 Fellmann, Jusletter 25.10.2010, Rn. 16 f.

731 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 2.

732 «Konsumprodukt»: Botschaft PrSG, S. 7408, 7419; «Konsumgüter»: Heiss/Loacker, in: Heiss/Loacker, § 2 Rn. 2.24; SHK PrSG-Hess, Art. 8 N 7; «Konsumentenprodukte»: Kellerhals, in: Dürr/Lardi/Rouiller S. 307; bezeichnet den Begriff «Konsumprodukt» als irreführend und spricht sich für die Verwendung von «Konsumentenprodukt» aus Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 2; verwendet den Begriff «Konsumgut», verweist aber auch auf den Ausdruck «Konsumentenprodukt» Fellmann, Jusletter 25.10.2010, 12 ff.

733 Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 10; Fellmann, Jusletter 25.10.2010, Rn. 20 ff.; in Bezug auf die GPSR siehe NHK GPSR-Wilrich, Art. 3 N 25.

Informationen in der Werbung sein.[734] Ein ursprünglich nur gewerblich genutztes Produkt wird durch Produktmigration zum Konsumentenprodukt, wenn es *vorhersehbar* auch durch Private genutzt wird.[735] Im schweizerischen Produktsicherheitsrecht finden sich zum Kriterium der Vorhersehbarkeit verschiedene Ansichten: Laut FELLMANN ergibt sich der vorhersehbare Gebrauch eines Produktes aus dem «realen Nutzerverhalten».[736] Wie unten zu zeigen sein wird, ist das reale Nutzerverhalten indes nicht einfach vorherzusagen und das Abstellen auf die vernünftige Vorhersehbarkeit aufgrund des «hindsight bias» problematisch.[737] GERSTER macht deutlich, dass sich aufgrund der Formulierung in Art. 8 Abs. 1 PrSG «unter vernünftigerweise vorhersehbaren Bedingungen [...] benutzt werden *könnten*» rückblickend schwierig argumentieren lässt, dass «die Benutzung [...] durch den Verwender nicht *vernünftigerweise vorhersehbar* war».[738] Auch HOLLIGER-HAGMANN äussert sich zu dieser Problematik und stellt fest, «dass die meisten für die Verwendung durch Fachleute bestimmten Erzeugnisse irgendwann in die Hände von Konsumenten gelangen».[739] BRUNNER nennt die eigentliche *Vorhersehbarkeit* des Gebrauchs durch Konsumenten als entscheidendes Kriterium, statt des realen Nutzerverhaltens.[740] Dieser Meinung ist unter Berücksichtigung der Gefahr des «hindsight bias» zuzustimmen. WILRICH geht in Bezug auf die GPSR einen Schritt weiter und macht die vernünftige vorhersehbare Verwendung abhängig von der Komplexität und Grösse eines Produktes[741] und von der «Klugheit der Nutzer»[742]. Zusammengefasst sind die Nachmarktpflichten des PrSG und der GPSR auf die gleichen Konsumentenprodukte anwendbar.[743]

---

734 FELLMANN, Jusletter 25.10.2010, Rn. 20.

735 Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 10; FELLMANN, Jusletter 25.10.2010, Rn. 22; für das EU-Recht: Art. 3 Ziff. 2 GPSR; siehe auch NHK GPSR-WILRICH, Art. 3 N 27.

736 FELLMANN, Jusletter 25.10.2010, Rn. 22; siehe auch GERSTER, Rn. 37 f. mit Kritik.

737 S. u., Rn. 264.

738 GERSTER, Rn. 38, 268 mit übernommenen Hervorhebungen.

739 Als Ausnahme davon nennt sie gewisse besonders risikobehaftete und teure Produkte, HOLLIGER-HAGMANN, Produktsicherheit und Haftpflicht, S. 46.

740 BRUNNER, in: Fellmann/Furrer, Schonzeit, S. 75, mit Verweis auf die Botschaft PrSG, S. 7437; ähnlich, aber noch einschränkender SHK PrSG-HESS, Art. 3 N 38: «Es handelt sich also dabei um Produkte, die *vorhersehbar* aus dem gewerblich bestimmten Nutzungsbereich in denjenigen der Konsumentin oder des Konsumenten geraten. [...] Dies muss jedoch im Blickwinkel einer objektivierten Betrachtungsweise auf die vom Hersteller in seiner Einflusssphäre gewollten oder jedenfalls zugelassenen Vertriebsströme erfolgen».

741 Zur Vorhersehbarkeit NHK GPSR-WILRICH, Art. 3 N 31.

742 Zur Vernünftigkeit NHK GPSR-WILRICH, Art. 3 N 32.

743 Auch die Nachmarktpflichten der Produktsicherheitsrichtlinie galten ausschliesslich für Konsumgüter, SHK PrSG-HESS, Art. 8 N 7.

Der Konsumentenschutz ist in der Schweiz und der EU unterschiedlich ausgeprägt. Während der Konsumentenschutz in der EU grundsätzlich höher[744] ist als in der Schweiz, ist die Schweiz nicht dazu verpflichtet, die europäischen Konsumentenschutzvorschriften generell zu übernehmen.[745] In Bezug auf die Produktsicherheit hat die Schweiz jedoch die Konsumentenschutzvorschriften der EU autonom nachvollzogen.[746] 189

II. Hardware als Produkt in der Schweiz

Smart Home Devices bestehen immer aus Hardware und Software. Ein Produkt ist gem. Art. 2 Abs. 1 PrSG eine «verwendungsbereite bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder unbeweglichen Sache bildet». Hardware kann eine verwendungsbereite bewegliche Sache sein und ist somit unbestritten ein Produkt i.S.v. Art. 2 Abs. 1 PrSG.[747] Je nachdem, wofür die Hardware benutzt wird, kann sie unter verschiedenes Sektorrecht fallen. In Bezug auf Smart Home Devices handelt es sich bei der Hardware in den allermeisten Fällen um ein Niederspannungserzeugnis i.S.v. Art. 1 Abs. 1 oder 2 NEV und in Kombination mit Software, die die kabellose Verbindung mit anderen Geräten ermöglicht, um eine Funkanlage i.S.v. Art. 2 Abs. 1 lit. a FAV. 190

Hardware ist selbst nicht Teil der Software oder des KI-Systems. Es handelt sich dabei um verschiedene Produkte, welche jedoch miteinander verbunden sind. Die Vorschriften des PrSG werden auch auf eingearbeitete Produkte angewandt.[748] Die Botschaft hielt explizit fest, dass es weiterhin möglich sein müsse, «die produktsicherheitsrelevanten Vorschriften auch auf eine eingearbeitete oder vermischte Sache anzuwenden».[749] Der Produktbegriff richtet sich zwar nach der beweglichen körperlichen Sache gem. Art. 713 ZGB[750], wird im Produktsicherheitsrecht jedoch ausgeweitet.[751] Ein eingearbeitetes Produkt geht im Produktsicherheitsrecht nicht in der anderen Sache auf, in die es in- 191

744 Heiss/Loacker, in: Heiss/Loacker, Einführung S. 5.
745 IK-EUDP, Schweiz, S. 60 f.
746 IK-EUDP, Schweiz, S. 61.
747 SHK PrSG-Hess, Art. 2 N 11, m.w.H.
748 Botschaft PrSG, S. 7434; siehe auch Bühler/Tobler, S. 372; Fellmann, Tragweite, S. 4; siehe auch Gerster, Rn. 30, m.w.H.; SHK PrSG-Hess, Art. 2 N 8, m.w.H.
749 Botschaft PrSG, S. 7434.
750 Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210 (zit. ZGB).
751 Botschaft PrSG, S. 7434; Bühler, Bestandteil, S. 29; SHK PrSG-Hess, Art. 2 N 3; siehe auch mit Bezug zum PrHG Damian, in: Praxishandbuch Produktregulierung, § 19 Rn. 2347; Lohmann, Haftungsrahmen, S. 115.

tegriert wurde.[752] Selbst Produkte, die zuerst zusammengebaut werden müssen und vom Hersteller in Einzelteilen abgegeben werden, gelten gem. Art. 2 Abs. 2 PrSG bereits als verwendungsbereit.[753] Werden dem Empfänger somit Einzelteile zum Zusammenbauen übergeben, sind das zusammengebaute Produkt sowie die Einzelteile als solche ebenfalls als verwendungsbereite Produkte anzusehen.[754] Auch elektronische Geräte, welche noch mit einer (auch wenn nicht mitgelieferten) Batterie bestückt werden müssen, gelten als verwendungsbereit.[755] Somit sind auch Verbindungs- (z.B. Klebstoff und Schrauben[756]), Ersatz-[757] (z.B. ein Ersatz für einen kaputt gegangenen Staubsaugeraufsatz) oder Zusatzteile (z.B. ein neuer, zusätzlicher Staubsaugeraufsatz) verwendungsbereite Produkte. Das heisst, dass die verschiedenen Teile eines Smart Home Devices wie bspw. die Hardware inklusive Plastikgehäuse, Platine, Kabel usw. und die Software alle für sich selbst Produkte sind und allein oder in Kombination sicher sein müssen, sofern man – wie vorliegend – Stand-alone-Software als Produkt anerkennt.[758] Auch Plugins und Softwareupdates können dann als verwendungsbereite Produkte gelten.[759]

III. Software und KI als Produkte in der Schweiz

192 In diesem Kapitel wird geklärt, ob und inwiefern Software nach geltendem Recht als eigenständiges Produkt vom PrSG erfasst wird. Trotz der veralteten Trennung zwischen Embedded und Stand-alone-Software wird aufgrund der verschiedenen Lehrmeinungen beides getrennt untersucht. Wie bereits festgestellt wurde, fällt Software in Bezug auf Smart Home Devices nicht unter bestehendes Sektorrecht.[760] Um zu untersuchen, ob und inwiefern Software

752 BVGer C-4789/2015 vom 29.01.2016, E. 2.2; BVGer C-6342/2013 vom 23.02.2015, E. 2.2; dies im Gegensatz zum Sachenrecht, in welchem die bewegliche Sache in der Sache aufgeht, in die sie integriert wurde, Botschaft PrSG, S. 7434; Gerster, Rn. 30.

753 Bühler/Tobler, S. 372.

754 Die Botschaft zählt bpsw. Haushaltsgeräte und -maschinen sowie Computerkonfigurationen auf, Botschaft PrSG, S. 7434; Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 9; Hess, in: Häner/Waldmann S. 221; Bühler/Tobler, S. 374.

755 Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 9.

756 Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 9.

757 Bühler/Tobler, S. 374.

758 S. u., Rn. 197 ff.

759 Siehe zumindest für Softwareupdates im deutschen Recht Beurskens, in: Bomhard et al., § 16 Rn. 144.

760 Software ist weder ein Niederspannungserzeugnis (Rn. 172) noch eine Funkanlage (Rn. 176). Software kann ein Medizinprodukt sein (Rn. 179) und zudem u.U. unter die MaschV fallen (Rn. 178).

ein Produkt ist, muss deshalb von den Definitionen im allgemeinen Produktsicherheitsrecht ausgegangen werden.

193 Inwiefern Software und somit auch KI als Produkt im Produktsicherheitsrecht erfasst sind, ist sowohl in der Schweiz als auch in der EU umstritten. In der Schweiz wurde bislang weder im Kontext des PrSG noch des PrHG gerichtlich entschieden, ob Software (und erst recht ein KI-System) als Produkt erfasst ist.[761] Software an sich ist keine körperliche Sache. Es kann sich also um eine Art von digitaler Dienstleistung oder um ein «unkörperliches» Produkt handeln.[762] Im Folgenden soll geklärt werden, ob Software als Produkt i.S.d. PrSG de lege lata erfasst werden kann. Die Frage ist relevant, da Rechtsgutverletzungen auch auf Stand-alone-Software basieren können.[763] Reine Software ohne eine «eigene» physische Ausprägung kann erhebliche Risiken bergen und ein gefährliches «Produkt» darstellen. Dies gilt nicht nur für klassische «Steuerungssoftware» in Fahrzeugen,[764] sondern bspw. auch für Software in Konsumentenprodukten. Bspw. könnte durch die Software in einer VR-Brille das Licht so hell eingestellt werden, dass die Augen beschädigt werden. Oder ein Kopfhörer wird so laut, dass er das Gehör schädigt. Argumentiert man dahingehend, dass die Hardware des Kopfhörers bereits entsprechend limitiert werden soll, können Funktionen wie «find-my-earbuds»[765] nicht mehr eingesetzt werden.[766] Es ist für das Gefährdungspotenzial von Software unerheblich, wie diese zur Verfügung gestellt wird, also ob sich Software bereits auf einem Gerät befindet oder zuerst heruntergeladen werden muss.[767]

761 Ebenfalls zum PrHG: BJ, Rechtliche Basisanalyse KI, S. 148; Koch/Pichonnaz, S. 638.

762 Zu dieser Unklarheit siehe bspw. Centre for Strategy and Evaluation Services, Study on the Impact of Artificial Intelligence on Product Safety, S. 61 f., abrufbar unter <https://www.gov.uk/government/publications/study-on-the-impact-of-artificial-intelligence-on-product-safety>, zuletzt besucht am 31.05.2025.

763 Braun Binder et al., Jusletter 28.06.2021, Rn. 43, mit Verweis auf Lohmann, Fahrzeuge, S. 316; SHK PrHG-Hess, Art. 3 PrHG N 30, m.w.H.; Haftpflichtkommentar-Holliger-Hagmann, Art. 3 PrHG N 34; bezogen auf das deutsche Produkthaftungsrecht Wittbrodt, S. 76.

764 Siehe bspw. Lohmann, Haftungsrahmen, S. 115, mit Verweis auf Zech, Gutachten, A 68.

765 Dabei spielen die Kopfhörer einen lauten Ton ab, falls sie nicht mehr auffindbar sind, How to find your lost Samsung Galaxy Buds, abrufbar unter <https://www.androidauthority.com/how-to-find-lost-galaxy-buds-3318610/>, zuletzt besucht am 31.05.2025.

766 Ausführliche Beispiele s. o., Rn. 22 ff.

767 Mit Bezug auf das PrHG: Koch/Pichonnaz, S. 638, m.w.H.; Werro, Rn. 627; SHK PrHG-Hess, Art. 3 N 34; mit Bezug auf das deutsche Produkthaftungsrecht Wittbrodt, S. 76; zur Unabhängigkeit der Zurverfügungstellung von Software mit Verweis auf den «UsedSoft»-Entscheid Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 167 f.; siehe EuGH vom 03.07.2012, C-128/11, UsedSoft, ECLI:EU:C:2012:407, Rn. 47; siehe bereits Wagner, Produkthaftung, S. 719.

1. Embedded Software

194 In Bezug auf das PrSG wird Embedded Software einheitlich als Produkt angesehen, solange sie unteilbar mit der Hardware verbunden ist. BÜHLER hat diese Frage nur in Bezug auf den Produktbegriff nach PrHG[768], nicht aber nach PrSG[769] behandelt. Zusammengefasst stellt er auf die Möglichkeit der Trennung von Hard- und Software ab: Nur die untrennbar mit der Hardware verbundene Software soll – dann zusammen mit der entsprechenden Hardware – als Produkt gelten.[770] Er spricht sich somit für die Erfassung von Embedded Software als Produkt aus, jedoch nicht für deren Eigenständigkeit als Produkt unabhängig von Hardware. HESS stellt fest, dass sich «in letzter Zeit die Meinung durchgesetzt» habe, es spiele für die Produkteigenschaft keine Rolle, ob das Produkt über ein physisches Produkt oder online übertragen wird.[771] HOLLIGER-HAGMANN anerkennt Software unbeschränkt als Produkt.[772]

195 Embedded Software war bereits in der Produktsicherheitsrichtlinie als Produkt erfasst.[773] Sie ist im europäischen[774] und deutschen[775] Produktsicherheitsrecht sowie im schweizerischen Produktehaftpflichtgesetz[776] und im deutschen[777] sowie im neuen europäischen[778] Produkthaftungsrecht als Produkt erfasst.

768 BÜHLER, Bestandteil, S. 30 ff.

769 BÜHLER, Bestandteil, S. 34 ff.

770 BÜHLER, Bestandteil, S. 33 f., wobei er integrierte Software der Individualsoftware entgegenstellt, was jedoch keine entgegengesetzten Kategorien sind; ähnlich in BÜHLER/TOBLER, S. 119 f.

771 SHK PrSG-HESS, Art. 2 N 12.

772 Wobei sie nicht zwischen Embedded und Stand-alone-Software unterscheidet: Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG 9; HOLLIGER-HAGMANN, Produktsicherheit und Haftpflicht, S. 8; HOLLIGER-HAGMANN, Fallstricke, S. 106.

773 Europäische Kommission, Weissbuch KI, S. 16; a.A. Europäische Kommission, Impact Assessment GPSR, S. 14.

774 S. u., Rn. 222.

775 Für das deutsche ProdSG: WIEBE, Pflichten, S. 66, m.w.H.; Beck ProdSG-KLINDT/SCHUCHT, § 2 Rn. 164a.

776 Alle mit Bezug auf das PrHG: BATACHE, Rn. 408; MORIN, in: Canapa/Richa S. 120; DAMIAN, in: Praxishandbuch Produktregulierung, § 19 Rn. 2347; KOCH/PICHONNAZ, S. 638; LOHMANN, Haftungsrahmen, S. 115; SHK PrHG-HESS, Art. 3 PrHG N 34; zumindest in Bezug auf Standardsoftware ebenfalls ROBERTO, Rn. 9.10.

777 WIEBE, Pflichten, S. 66, m.w.H.; WITTBRODT, S. 75, m.w.H.; WAGNER, Produkthaftung, S. 714.

778 S. u., Rn. 234.

2. Stand-alone-Software

Es ist umstritten, ob Stand-alone-Software als Produkt im Sinne des PrSG erfasst ist. In der Schweiz wird Stand-alone-Software mehrheitlich als Produkt nach Art. 2 Abs. 1 PrSG qualifiziert.[779] Es wird jedoch auch vertreten, dass Stand-alone-Software nach dem PrSG kein Produkt sei.[780] Weitere Autoren diskutieren diese Frage, legen sich aber nicht fest.[781] 196

2.1. Auslegung von Art. 2 Abs. 1 PrSG – Ist Software ein Produkt?

Unter Zuhilfenahme der klassischen Auslegungselemente[782] und dem pragmatischen Methodenpluralismus des BGers[783] folgend, wird in diesem Kapitel beurteilt, ob Software als Produkt von Art. 2 Abs. 1 PrSG erfasst wird. Art. 2 Abs. 1 PrSG lautet: 197

> «Als Produkt im Sinne dieses Gesetzes gilt eine verwendungsbereite bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet».

a. Literalinterpretation

Art. 2 Abs. 1 PrSG hält fest, dass Produkte «verwendungsbereite bewegliche Sachen» sind. Da die «Sache» im PrSG weiter zu verstehen ist als im ZGB,[784] fragt sich, ob sich der Begriff der Sache im Produktsicherheitsrecht nicht auch für Software öffnen lässt.[785] Für eine abweichende Bedeutung vom Sachbegriff des ZGB spricht auch der Wortlaut des französischen Gesetzestextes, da die 198

779 Morin, in: Canapa/Richa S. 120, 127; Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 9; Klett/Verde, S. 50; Kasper/Dal Molin, EU Cyber Resilience Act's Impact on Swiss Companies, abrufbar unter <https://www.homburger.ch/de/insights/eu-cyber-resilience-acts-impact-on-swiss-companies?>, zuletzt besucht am 31.05.2025, ohne Unterscheidung zwischen Embedded und Stand-alone-Software.

780 Bühler, Bestandteil, S. 33 f.; Bühler/Tobler, S. 119.

781 Zustimmend bezogen auf das PrHG, legt sich bezogen auf das PrSG indes nicht fest Nosetti, in: Hürlimann-Kaup et al. S. 226 ff.; verwendet den Begriff «Softwareprodukt», hält aber nur fest, dass es umstritten sei, ob «das PrSG auf alle Formen von Software Anwendung findet» Fröhlich-Bleuler, Rn. 2097; eher zustimmend SHK PrSG-Hess, Art. 2 N 12.

782 Kramer/Arnet, S. 66.

783 Siehe bspw. BGE 146 III 169, 172 f. E. 4.2.2; BGE 145 III 63, 64 f. E. 2.1; siehe mit weiteren Ausführungen und Kritik auch Kramer/Arnet, S. 143.

784 S. o., Rn. 191.

785 Zur Relativität der Rechtsbegriffe siehe auch Kramer/Arnet, S. 75 f.

«Sache» im PrSG auf Französisch als «bien» und im ZGB als «chose» bezeichnet wird.[786] Gem. dem Gesetzgeber soll mit dem Ausdruck «bewegliche Sache» klargestellt werden, dass Gebäude und Bauwerke nicht unter das PrSG fallen.[787] Zudem müsse es möglich sein, eingearbeitete Sachen in anderen beweglichen Sachen oder Immobilien nach deren Integration weiterhin als Produkte zu erfassen.[788] Beide Argumente sprechen nicht dagegen, Software als Produkt zu erfassen.

199 Das Kriterium der Beweglichkeit setzt also nicht explizit auch eine Körperlichkeit des Produktes voraus. Auch ohne Körperlichkeit lässt sich Software ohne weiteres «bewegen», z.B. als Download von einer Website auf einen Computer. Stand-alone-Software kann somit eine bewegliche Sache sein, auch wenn es sich dabei um die nichtphysischen Teile eines Computers handelt.

200 Software ist zwar immer Teil einer anderen beweglichen Sache, da sie Hardware benötigt, um darauf ausgeführt zu werden (dies gilt auch für SaaS), dies macht Software selbst aber nicht zu einer beweglichen, *körperlichen* Sache. Dementsprechend ist genau diese Argumentation bezüglich Embedded Software nicht nachvollziehbar. Obwohl Software keine Körperlichkeit hat, wurde sie in der älteren Lehre schon als Produkt anerkannt, wenn sie mit einer körperlichen Sache «verbunden», bspw. auf einem Datenträger gespeichert, war. Es wurde also auf das physische Speichermedium ausgewichen.[789] Dies ist der Grund, weshalb Embedded Software von der h.L. sowohl in der Produktsicherheit als auch in der Produkthaftung als Produkt anerkannt ist.[790] Dieser Argumentation folgend müssten auch Informationen in einem Buch (das ja auch ein beweglicher, körperlicher «Datenträger» ist) als Produkt anerkannt werden. Logischer ist deshalb, wenn auf die Voraussetzung der «Körperlichkeit» des Produktes verzichtet wird, zumal diese im Wortlaut auch nicht gefordert ist.

201 Die Verwendungsbereitschaft ist unproblematisch, da Software nach fertiger Entwicklung immer «benutzbar» sein kann. Das Kriterium der «Verwendungsbereitschaft» wurde gewählt, damit das PrSG nicht auf Produkte, die noch im Entstehungsprozess sind, angewandt wird.[791] Nach reiner Betrachtung des Wortlauts kann Software demnach eine verwendungsbereite bewegliche Sa-

786 Demgegenüber heisst es in dem italienischen Art. 2 Abs. 1 PrSG respektive Art. 713 ZGB jeweils «cosa».

787 Botschaft PrSG, S. 7434.

788 S. o., Rn. 191.

789 Batache, S. 408, m.w.H.; mit Bezug auf das deutsche Recht Wagner, Produkthaftung, S. 717.

790 S. o., Rn. 194.

791 Botschaft PrSG, S. 7434; siehe auch SHK PrSG-Hess, Art. 2 N 15.

che i.S.d. PrSG und damit ein Produkt nach Art. 2 Abs. 1 PrSG sein. Der Begriff «Sache» ist jedoch weiter als in Art. 713 ZGB zu verstehen.

b. Systematische Interpretation

Wegen der Interpendenz des Öffentlichen Rechts und des Privatrechts,[792] vorliegend konkret des Produktsicherheitsrechts und des Produkthaftpflichtrechts,[793] sollten die Produktbegriffe möglichst deckungsgleich ausgelegt werden. Weil sich nur wenige Autoren zum Produktbegriff im PrSG geäussert haben, soll der Meinungsstand in Bezug auf das PrHG herangezogen werden. Auch im Produkthaftpflichtrecht ist umstritten, ob Stand-alone-Software ein Produkt ist.[794] Die h.L. geht jedoch von der Erfassung von Stand-alone-Software als Produkt gem. Art. 3 Abs. 1 lit. a PrHG aus.[795] Einige Autoren sehen Stand-alone-Software nach dem PrHG weiterhin nicht als Produkt erfasst.[796] 202

Produktsicherheitsrechtliches Sektorrecht ist lex specialis zum PrSG.[797] Neueres Sektorrecht tendiert dazu, Software als Produkt zu erfassen. Analog zur EU[798] erfassen in der Schweiz das HMG[799] und die MepV[800] Software explizit als Medizinprodukt, ohne zwischen Embedded und Stand-alone-Software zu unterscheiden.[801] Während die MaschV Software nicht direkt erfasst, verweist sie in Art. 4 Abs. 1bis MaschV auf die europäische MVO, welche in Art. 3 Abs. 3 festhält, dass Sicherheitsbauteile auch Software sein können. 203

792 Siehe dazu Kramer/Arnet, S. 101.

793 S. o., Rn. 148.

794 Statt vieler Büyüksagis, S. 18 f. spezifisch mit Bezug auf Software und KI-Systeme; Koch/Pichonnaz, S. 638.

795 Müller, Rn. 443; Batache, Rn. 408; Wildhaber/Rey, Rn. 1427; Koch/Pichonnaz, S. 638, welche festhalten, dass «die aktuelle Definition des Produktes im PrHG […] es dennoch schwierig [macht], die wohl unkörperliche Software unter den Begriff ‹bewegliche Sache› zu subsumieren», sich aber dennoch für eine Anerkennung von Stand-alone-Software und eine Anwendung des PrHG aussprechen; CHK-Märki/Sommer, Art. 3 PrHG N 5; Braun Binder et al., Jusletter 28.06.2021, Rn. 43; Fellmann, Haftpflichtrecht, S. 107; Lohmann, Haftungsrahmen, S. 115; Wildhaber, Einführung, S. 40; BSK OR I-Fellmann, Art. 3 PrHG N 10; Schwenzer/Fountoulakis, Rn. 53.35; Nosetti, in: Hürlimann-Kaup et al. S. 226 ff.; Hänsenberger, Jusletter 26.11.2018, Rn. 14; Klett, Digitalisierte, S. 112; Werro, Rn. 627; SHK PrHG-Hess, Art. 3 N 34; Straub, Jusletter 18.03.2002, Rn. 16.

796 Huguenin, Rn. 2110; Honsell/Isenring/Kessler, § 21 Rn. 30 f.

797 Im Detail und zu den Ausnahmen s. o., Rn. 161 ff.

798 Art. 2 Ziff. 1 MDR; siehe auch Europäische Kommission, Weissbuch KI, S. 16 Fn. 45.

799 Art. 4 Abs. 1 lit. b Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz) vom 15. Dezember 2000, SR 812.21 (zit. HMG).

800 Art. 3 Abs. 1 MepV.

801 Batache, S. 67, m.w.H.

204 Werden die verfassungsrechtlichen Grundlagen des PrSG für eine verfassungskonforme Auslegung[802] zugezogen, kann festgestellt werden, dass sich das PrSG in drei von vier Fällen auf Artikel stützt, die dem Schutz der Bevölkerung dienen.[803] Da es für das Gefahrenpotenzial von Software keinen Unterschied macht, ob diese embedded oder stand-alone ist,[804] dient eine Anerkennung von Software als Produkt ebenfalls dem Schutz der Bevölkerung.

c. *Historische Interpretation*

205 Die europäische Produkthaftungsrichtlinie ist der Ursprung der Produktregulierung, wie sie heute existiert. Als die PLD 1985 erlassen wurde, hatte Software vor allem im Konsumbereich keine so hohe Relevanz wie heute und wurde in der Richtlinie deshalb nicht berücksichtigt.[805] Dennoch scheint mehrheitlich Konsens[806] darüber zu herrschen, dass Software in der PLD 1985 als Produkt erfasst ist.[807]

206 Nach der Produkthaftungsrichtlinie wurde die Produktsicherheitsrichtlinie erlassen. Unter der Produktsicherheitsrichtlinie war umstritten, ob Software ein Produkt ist.[808] Die Produktsicherheitsrichtlinie erfasste Software nicht explizit als Produkt.[809] Sie schränkte den Produktbegriff jedoch auch nicht auf bewegliche Sachen ein. Die Produktsicherheitsrichtlinie hielt in Art. 2 lit. a fest, dass der Ausdruck «Produkt» «jedes Produkt [bezeichnet], das – auch im Rahmen der Erbringung einer Dienstleistung – für Verbraucher bestimmt ist oder unter vernünftigerweise vorhersehbaren Bedingungen von Verbrauchern benutzt werden könnte, selbst wenn es nicht für diese bestimmt ist, und entgeltlich oder unentgeltlich im Rahmen einer Geschäftstätigkeit geliefert oder zur Verfügung gestellt wird, unabhängig davon, ob es neu, gebraucht oder wie-

802 Was vorliegend nicht nötig wäre, aber der Vollständigkeit halber einbezogen wird. Siehe auch Kramer/Arnet, S. 117.

803 S. o., Rn. 149.

804 S. o., Rn. 193.

805 Oster, in: Foerste/Westphalen, § 57 Rn. 43; Joggerst/Wendt, S. 13; Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 170.

806 A.a. Karner, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 119.

807 Oster, in: Foerste/Westphalen, § 57 Rn. 44; bereits zustimmend auf die schriftliche Anfrage Nr. 2613/85 von Herrn William Newton Dunn an die Kommission der EG vom 24.01.1986 (89/C 114/01), Antwort, S. 42; mit Verweis auf ebendiese Antwort: Lohmann, Haftungsrahmen, S. 115; Wittbrodt, S. 76; Koch, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 106; nur bezogen auf Standardsoftware Wagner, Produkthaftung, S. 718; a.A. Spindler, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 128, m.w.H.

808 Europäische Kommission, Weissbuch KI, S. 16.

809 Siehe auch Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 163.

deraufgearbeitet ist». OSTER stellt in Bezug auf das deutsche ProdSG – welches wie das PrSG auf der Produktsicherheitsrichtlinie beruht – fest, dass sich eine Subsumtion von Software als Produkt «noch besser vertreten lässt» als im Produkthaftpflichtrecht[810], weil in der Produktsicherheitsrichtlinie im Gegensatz zur PLD 1985 kein Bezug zu beweglichen Sachen gemacht werde.[811]

Die Schweiz hat beide Richtlinien in das PrHG respektive das PrSG autonom nachvollzogen.[812] Dass das Produkt im PrSG als «bewegliche Sache» definiert wurde (statt dies wie in der Produktsicherheitsrichtlinie offenzulassen), ist vermutlich auf den Versuch zurückzuführen, den Produktbegriff möglichst nahe an die Definition im PrHG anzugleichen. Einer richtlinienkonformen Interpretation[813] folgend, verliert die Voraussetzung der «beweglichen Sache» für den Produktbegriff nach dem PrSG somit an Relevanz. 207

Software wird weder in der Botschaft über das Folgeprogramm nach der Ablehnung des EWR-Abkommens noch in jener zum PrSG erwähnt. Auch in den parlamentarischen Diskussionen zum PrSG finden sich keine Hinweise auf den Umgang mit Software. Sie wurde während beider Gesetzgebungsprozesse schlichtweg nicht berücksichtigt. Die gestiegene Relevanz von Software seit Erlass der erwähnten Produktregulierungen spricht dafür, auch Stand-alone-Software als Produkt anzuerkennen. Zudem ist darauf hinzuweisen, dass die Materialien bei der historischen Auslegung bei älteren Gesetzen weniger stark zu berücksichtigen sind als bei neueren Gesetzen.[814] Wenn also Software in den über 15-jährigen Materialien zum PrSG nicht erwähnt wird, heisst das nicht, dass sie nicht als Produkt gelten kann. 208

810 OSTER, in: Foerste/Westphalen, § 57 Rn. 43 f.; die Erfassung von reiner Software als Produkt nach dem deutschen ProdHaftG ist ebenfalls umstritten, bejahend: MCGUIRE, in: Foerste/Westphalen, § 58 Rn. 44; WITTBRODT, S. 76; feststellend, dass Standardsoftware (nicht aber Individualsoftware) «wie körperliche Gegenstände zu behandeln» seien, WAGNER, Produkthaftung, S. 717 f.; a.A. Beck ProdSG-KLINDT/SCHUCHT, § 2 N 165.

811 OSTER, in: Foerste/Westphalen, § 57 Rn. 37; siehe auch WIEBE, Pflichten, S. 66; a.A. jedoch: WITTBRODT, S. 75; Beck ProdSG-KLINDT/SCHUCHT, § 2 N 165; PIOVANO/SCHUCHT/WIEBE, S. 78 f.; siehe auch PIOVANO, Hersteller, S. 19, welcher nichts über die Produkteigenschaft von Software sagt, jedoch davon ausgeht, dass ein Fahrassistent gem. Art. 3 ProdSG sicher sein muss. Beim Fahrassistenten handelt es sich um Software.

812 S. o., Rn. 148.

813 KRAMER/ARNET, S. 355 f.

814 BGE 124 III 350, 352 E. 2.b; BGE 116 II 525, 527 E. 2.b.

d. Teleologische Interpretation

209 Einer der wichtigsten Gründe für den Erlass des PrSG war, dass Produkte sicher sein müssen. Die Gefährdungslage für Nutzer von Software kann sich gleich gestalten wie bei körperlichen Gegenständen und ist unabhängig davon, ob sich die Software bereits auf dem Gerät befindet oder zuerst heruntergeladen werden muss. Dies darf deshalb auch keine Rolle für die Produkteigenschaft spielen.[815] Die Unterscheidung zwischen Embedded und Stand-alone-Software ergibt unter den heutigen Begebenheiten keinen Sinn. Früher wurde Software oft für spezifische Hardware entwickelt, da keine standardisierten Plattformen existierten. Sie war daher häufig hardwaregebunden und «embedded». Heute wird Software modular und plattformunabhängig entwickelt, kann auf verschiedenen Geräten installiert werden und ist teilweise sogar installationsfrei nutzbar, wie etwa bei Web-Apps.[816]

210 Embedded und Stand-alone-Software können als (Teil-)Produkte betrachtet werden, z.B. vergleichbar mit physischen Komponenten wie Schrauben.[817] Diese Komponenten sind i.d.R. nur in Verbindung mit einem anderen Produkt potenziell gefährlich,[818] werden aber dennoch als eigenständige Produkte anerkannt, wenn sie verwendungsbereit sind. Es wird deshalb auch vorgeschlagen, dass Software nur ein Produkt sein soll, wenn sie fähig ist, körperliche Produkte zu beeinflussen oder zu steuern, um vor allem dem «Robotikrisiko» entgegenzuwirken.[819] Dieser Meinung kann nicht gefolgt werden. Die Interaktion mit der Hardware unterscheidet Software bereits von der «blossen Information».[820] Im Gegensatz zur Information, die zuerst befolgt werden muss, bedarf es bei Software keiner menschlichen Umsetzung mehr, um Schäden auszulösen.[821] Straub hielt bereits 2002 fest, dass Software «zumindest dann produktetypische Funktionalität» habe, «wenn sie direkt Prozesse» steuert.[822] Es handelt sich auch um einen Prozess, wenn Software etwas auf einem Bildschirm anzeigt. Analog zu einer speziell konstruierten Schraube kann Software ein Produkt sein, solange sie verwendungsbereit ist. Unabhängig davon, ob sie

815 S. o., Rn. 193.
816 S. o., Rn. 34.
817 S. o., Rn. 191.
818 S. o., Rn. 33.
819 Zech, Regelungen, S. 37.
820 Straub, Produktehaftung, Rn. 4.
821 McGuire, in: Foerste/Westphalen, § 58 Rn. 45, mit Verweis auf den Entscheid; EuGH vom 10.06.2021, C-65/20, KRONE – Verlag, ECLI:EU:C:2021:471, Rn. 2.
822 Straub, Produktehaftung, Rn. 4.

spezifisch angepasst (Individualsoftware) oder allgemein einsetzbar ist (Standardsoftware).[823]

2.2. Ergebnis der Interpretation

Stand-alone-Software ist ein Produkt nach Art. 2 Abs. 1 PrSG. Der Wortlaut des Gesetzes spricht nicht dagegen, da der Begriff der «Sache» im PrSG weiter als nach Art. 713 ZGB ist. Für eine Erfassung als Produkt spricht auch, dass der Produktbegriff im PrSG möglichst jenem des PrHG entsprechen soll, die sektorrechtlichen Erlasse dazu tendieren, Software explizit als Produkt zu erfassen, und die verfassungsrechtlichen Grundlagen des PrSG mehrheitlich dem Schutz der Bevölkerung dienen. Da das Gefahrenpotenzial von Software unabhängig davon besteht, ob sie «embedded» oder «stand-alone» ist, trägt auch deren beider Anerkennung als Produkt zum Schutz der Bevölkerung bei. Die Ursprünge des Produktbegriffs im PrSG finden sich in der PLD 1985 und der Produktsicherheitsrichtlinie, unter welchen sich Software ebenfalls als Produkt erfassen lässt. Im Gesetzgebungsprozess wurde die Erfassung von Software als Produkt soweit ersichtlich nie diskutiert und es kann daher nicht davon ausgegangen werden, dass Software vom Produktbegriff ausgeschlossen werden sollte. Im Gegenteil muss Software aufgrund ihrer gestiegenen Relevanz als Produkt erfasst sein.[824] Software kann genauso gefährlich sein wie andere Produkte auch. Dies gilt unabhängig davon, ob sie «embedded» ist oder nicht. Da die Produktsicherheit eines der wichtigsten Ziele des PrSG ist und die Erfassung von Software als Produkt diesem Ziel dient, steht die Erfassung von Software als Produkt im Einklang mit dem Sinn und Zweck des PrSG. Auch wenn Software stets auf Hardware läuft, ist sie ein eigenständiges Produkt, solange sie verwendungsbereit ist. Das PrSG und seine Nachmarktpflichten sind somit auf Software – unabhängig davon, ob «embedded» oder «stand-alone» – anwendbar. 211

823 S. u., Rn. 214.

824 Interessant ist zudem die Antwort des ESTI vom November 2024 auf die Frage der Autorin «Gibt es Unterschiede zwischen Post-Market-Monitoring bei ‹Hardware›-Produkten und Software?»: «Ein Produkt muss als Ganzes die minimalen Anforderungen betreffend elektrische Sicherheit erfüllen: Wird eine sicherheitsrelevante Komponenten verändert (zum Beispiel eine Erdungsschraube oder eine Überwachungssoftware), so handelt es sich um ein neues Produkt und die Sicherheit muss neu bewertet werden». Dies zeigt, dass sicherheitsrelevante Software in der Schweizer Praxis bereits als (Teil-)Produkt angesehen wird.

2.3. Software als Dienstleistung

212 Konsequenterweise muss SaaS ebenso wie andere Stand-alone-Software behandelt und als Produkt erfasst werden.[825] Bei SaaS wird Software als Dienstleistung zur Verfügung gestellt. Auch die Verwendung eines Produktes im Rahmen des Erbringens einer Dienstleistung gilt als Inverkehrbringung eines Produktes nach Art. 2 Abs. 3 lit. b PrSG.[826] Die Dienstleistung selbst ist jedoch kein Produkt nach Art. 2 Abs. 1 PrSG.[827] Die Grenze zwischen Produkten und digitalen Dienstleistungen wird immer mehr verwischt.[828] Immer mehr Produkte werden zusammen mit Dienstleistungen verkauft oder im Zusammenhang mit einer Dienstleistung angeboten. Fernüberwachung und Updates sind bspw. laufende Dienstleistungen in Smart Home Devices. Diese Herausforderungen werfen u.a. Fragen nach der Definition des Begriffs «Produkt» auf.[829] Digitale Dienstleistungen können für die Sicherheit von Produkten genauso wichtig sein wie andere Komponenten.[830] Im Einzelnen können bspw. digitale Karten für Drohnen,[831] das kontinuierliche Zurverfügungstellen von Verkehrsdaten für ein Navigationssystem[832] und Temperaturüberwachungsmechanismen, die die Temperatur eines intelligenten Kühlschranks überwachen und regulieren,[833] die Sicherheit ihres zugehörigen Gerätes beeinträchtigen.

213 Aufgrund dieser Unklarheiten wird verlangt, dass klare Kriterien entwickelt werden, um eine Abgrenzung zwischen Dienstleistungen und Produkten zu ermöglichen.[834] Nachdem der EuGH entschieden hatte, dass Dienstleistungen

825 So auch ErwG 13 PLD 2024.

826 Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 17.

827 Botschaft PrSG, S. 7427, wobei die Erfassung von Dienstleistungen mindestens diskutiert wurde, S. 7416, 7419; siehe auch SHK PrSG-Hess, Art. 2 N 4; etwas zurückhaltender Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 20.

828 Zuletzt Batache, Rn. 408; Wildhaber, Einführung, S. 40, m.w.H.; Expert Group on Liability and New Technologies, Liability, S. 28; Wagner, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 27.

829 Alle zum europäischen Recht: Centre for Strategy and Evaluation Services, Study on the Impact of Artificial Intelligence on Product Safety, S. 55, abrufbar unter <https://www.gov.uk/government/publications/study-on-the-impact-of-artificial-intelligence-on-product-safety>, zuletzt besucht am 31.05.2025; Joggerst/Wendt, S. 13; Europäische Kommission, Weissbuch KI, S. 16; siehe auch Wagner, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 29.

830 ErwG 17 PLD 2024, wobei sie dort «digitale Dienste» heissen; ähnlich Europäische Kommission, Weissbuch KI, S. 17; Wildhaber, Einführung, S. 40, m.w.H.

831 Hänsenberger, Drohnen, S. 225 f.

832 Europäische Kommission, Vorschlag PLD 2024, ErwG 15; ErwG 17 PLD 2024.

833 Europäische Kommission, Vorschlag PLD 2024, ErwG 15; ErwG 17 PLD 2024.

834 Wildhaber, Einführung, S. 40; siehe auch Büyüksagis, S. 18.

nach der PLD 1985 keine Produkte sind,[835] werden in der neuen PLD 2024 «verbundene Dienste» erfasst.[836] Es handelt sich dabei gem. Art. 4 Ziff. 3 PLD 2024 um «einen digitalen Dienst, der so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte». Der verbundene Dienst ist eine Komponente des Produktes, wenn er in dieses integriert oder mit diesem verbunden ist.[837]

3. Individual- und Standardsoftware

In der Literatur wird zwischen Individual- und Standardsoftware[838] unterschieden und es ist umstritten, ob auch Individualsoftware als Produkt erfasst sein soll.[839] Individuell hergestellte Einzelprodukte sind im PrSG genauso als Produkt erfasst wie in Serie hergestellte Produkte.[840] Der von BÜHLER/TOBLER vertretenen Meinung, dass nur seriell hergestellte Produkte unter Art. 8 Abs. 1 PrSG fallen, da für Einzelprodukte die vertragsrechtlichen Normen zur Verfügung stünden,[841] kann nicht gefolgt werden. Erstens haben die vertragsrechtlichen Normen nicht den Schutz der Gesundheit und Sicherheit von Menschen zum Zweck. Zweitens können nicht nur seriell hergestellte Produkte unentdeckte Gefahren für potenziell viele Personen darstellen. In Bezug auf Software gilt dies bspw. für Individualsoftware, die nicht in Serie hergestellt, sondern bspw. für ein einzelnes Unternehmen entwickelt wird. So kann etwa Individualsoftware zur Steuerung einer vernetzten Brandmelde- und Evakuationsanlage in einem Mehrfamilienhaus eingesetzt werden, wobei die Software spezifisch auf die baulichen Gegebenheiten und technischen Einrichtungen zugeschnitten ist. Individualsoftware kann die Sicherheit und Gesundheit, der sich im Gebäude befindlichen Personen gefährden, etwa wenn Brandmeldungen nicht korrekt verarbeitet oder Fluchtwege nicht freigegeben werden. Die Vielzahl potenziell betroffener Personen ergibt sich dabei nicht aus der Seri- 214

835 EuGH vom 10.06.2021, C-65/20, KRONE – Verlag, ECLI:EU:C:2021:471, Rn. 27, 32, 37 f.

836 Dienstleistungen sind weiterhin nicht als Produkte erfasst, ErwG 17 PLD 2024.

837 Art. 3 Ziff. 4 PLD 2024; siehe jedoch KOCH/PICHONNAZ, S. 638, welche in Bezug auf den Entwurf festhalten, dass auch dann nicht ganz klar ist, welche digitalen Dienstleistungen eine genügend enge Verbindung mit einem Produkt haben, um als Komponenten zu gelten.

838 S. o., Rn. 78.

839 In Bezug auf das deutsche ProdHaftG: WAGNER, Produkthaftung, S. 717 f., anerkennt nur Standard- nicht aber Individualsoftware als Produkt.; a.A. BEURSKENS, in: Bomhard et al., § 16 Rn. 153.

840 GERSTER, Rn. 27; HOLLIGER-HAGMANN, Fallstricke, S. 28, 92, 102 f.; ebenso in Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 1; gl.M. mit Bezug auf das PrHG: FELLMANN/BÜREN-VON MOOS, Rn. 143; a.A. BÜHLER/TOBLER, S. 394.

841 BÜHLER/TOBLER, S. 394.

enmässigkeit oder der Vervielfältigung der Software, sondern aus ihrer zentralen Steuerungsfunktion innerhalb eines sicherheitsrelevanten Systems. Vor diesem Hintergrund kann es für die Qualifikation als Produkt im Sinne des Produktsicherheitsrechts nicht darauf ankommen, ob Software für viele oder einen Einzelnen entwickelt wurde. Die Qualifizierung von Individualsoftware als Produkt ist sinnvoll, da das Gefährdungspotenzial eines Produktes dasselbe ist wie bei Standardsoftware.[842] Aus diesen Gründen müssen sowohl Individual- als auch Standardsoftware als Produkt im Produktsicherheitsrecht gelten.[843] Somit sind die Nachmarktpflichten des PrSG auch auf einzeln angefertigte Produkte wie z.B. auf Individualsoftware und nicht nur auf Standardsoftware anwendbar.

4. KI als Produkt

215 Da es sich bei KI um eine Art von Software handelt, gelten die obigen Ausführungen zu Software entsprechend für KI. KI-Systeme sind demnach – unabhängig davon, ob sie in ein körperliches Gerät integriert sind – als Produkt vom PrSG erfasst. Für sie gelten deshalb die gleichen Regeln wie für «herkömmliche» Software ohne Lernfähigkeit und Autonomie.[844] In einer Stellungnahme auf eine Interpellation hielt der Bundesrat im November 2024 fest, dass die Schweiz «derzeit über keine spezifische Regelung über die Zulassung von Allzweck-KI-Systemen (General Purpose AI Systems, GPAI-Systeme)» verfüge.[845] In der gleichen Stellungnahme werden das PrSG «sowie die einschlägigen sektoriellen Gesetze» als für KI-Systeme «ebenfalls relevant» bezeichnet.

---

842 Für das PrHG: Batache, Rn. 408, m.w.H.; SHK PrHG-Hess, Art. 3 N 34; in Bezug auf die PLD 1985 und das deutsche ProdHaftG Oster, in: Foerste/Westphalen, § 57 Rn. 44; in Bezug auf die neue PLD 2024 Joggerst/Wendt, S. 14 f.

843 Gl.M., aber ohne Begründung Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG 9; ohne Meinung, aber feststellend, dass sich diese Ansicht durchgesetzt habe, SHK PrSG-Hess, Art. 2 N 12, wobei er zwischen «Standardsoftware» und «auf Träger gespeicherte Individualsoftware» unterscheidet. Ob die Software für viele oder einzelne entwickelt wurde, hat jedoch nichts mit der Art der Weitergabe zu tun.; Hess vertritt in einer neueren Publikation, dass Standard- und Individualsoftware unabhängig davon, wie sie überlassen wurden, als Produkt gelten, Hess, Produktehaftung – Produktesicherheit, S. 20; Mit Bezug auf das PrHG: Koch/Pichonnaz, S. 638; Straub, Jusletter 18.03.2002, Rn. 7.

844 Für das PrHG ebenso Damian, in: Praxishandbuch Produktregulierung, § 19 Rn. 2348; so auch die Beispiele in Wagner, Produkthaftung, S. 716; ähnlich Borges, Begriff, Rn. 31.

845 Interpellation 24.4178 vom 27.09.2024, Chappuis/Nationalrat, Zulassung von KI-Systemen für den allgemeinen Gebrauch auf dem Schweizer Markt.

IV. Zwischenfazit für die Schweiz

Smart Home Devices sind Produkte i.S.d. PrSG, wobei sie gesamthaft unter die NEV oder FAV fallen und das PrSG nur subsidiär anwendbar ist. Software ist ebenfalls ein Produkt i.S.v. Art. 2 Abs. 1 PrSG, unabhängig davon, ob es sich um Standard- oder Individualsoftware, Embedded oder Stand-alone-Software handelt. Da es sich bei KI-Systemen ebenfalls um Software handelt, sind diese auch als Produkte vom PrSG erfasst. Ergeben sich aus einem Smart Home Device Gefahren, die direkt auf Software zurückzuführen sind, kann die Software als eigenständiges gefährliches Produkt beurteilt werden, ohne Beschränkung auf ein bestimmtes Smart Home Device. Die Nachmarktpflichten des PrSG gelten somit auch für Software. Da die Nachmarktpflichten des PrSG nur auf Konsumentenprodukte anwendbar sind, gelten sie auch nur für Software und damit KI, wenn sie von Privaten verwendet wird oder vorhersehbar verwendet werden kann. 216

Dienstleistungen sind keine Produkte, können jedoch je nach Form dieselben gefährlichen Auswirkungen wie Produkte haben. Die Abgrenzung zwischen Produkten und Dienstleistungen ist im Einzelfall schwierig und bedarf klarerer Kriterien zur Unterscheidung. 217

V. Hardware als Produkt in der EU

Art. 3 Ziff. 1 GPSR definiert das Produkt als 218

> «jeden *Gegenstand*, der für sich allein oder in Verbindung mit anderen Gegenständen entgeltlich oder unentgeltlich – auch im Rahmen der Erbringung einer Dienstleistung – geliefert oder bereitgestellt wird und für Verbraucher bestimmt ist oder unter vernünftigerweise vorhersehbaren Bedingungen wahrscheinlich von Verbrauchern benutzt wird, selbst wenn er nicht für diese bestimmt ist».

Es handelt sich bei Produkten also um Gegenstände. Was genau ein Gegenstand ist, ist jedoch nicht definiert.[846] Da körperliche Gegenstände unbestritten Produkte sind,[847] handelt es sich bei Hardware um ein Produkt nach Art. 3 Ziff. 1 GPSR. Da gem. Art. 3 Ziff. 1 GPSR Produkte Gegenstände sein können, die «für sich allein oder in Verbindung mit anderen Gegenständen» bereitgestellt werden, können Produkte «aus einem oder mehreren Einzelteilen bestehen»[848].

846 Siehe auch NHK GPSR-Wilrich, Art. 3 N 8.
847 NHK GPSR-Wilrich, Art. 3 N 8 f.
848 NHK GPSR-Wilrich, Art. 3 N 14.

Auch die GPSR gilt nur für Produkte, die verwendungsbereit sind.[849] Sie werden «Endprodukte» genannt.[850] Produkte, die zur Weiterverarbeitung bestimmt sind, sind dabei nicht mitgemeint.[851] Dies schliesst jedoch nicht aus, dass Teile eines Endproduktes, also bspw. die Ladestation einer Staubsaugerrobotereinheit oder die Kamera in einem Staubsaugerroboter, als eigenständige Produkte erfasst sind. Auch das zusammengesetzte Endprodukt muss in Kombination aller seiner Teile sicher sein.[852] Hardware ist von der GPSR als Produkt erfasst, da es sich um einen Gegenstand handelt, sofern sie ein Verbraucherprodukt darstellt. Die GPSR gilt jedoch nur subsidiär bei Smart Home Devices, da es sich dabei um Funkanlagen i.S.v. Art. 2 Abs. 1 Ziff. 1 RED handelt.[853]

VI. Software und KI als Produkte in der EU

219 In diesem Kapitel wird dargelegt, inwiefern Software und KI-Systeme nach der europäischen GPSR und der KI-VO als Produkte erfasst sind.

220 Es ist unklar, ob die Produktsicherheitsrichtlinie auf neue Technologieprodukte wie vernetzte Geräte oder KI-gestützte Produkte anwendbar war.[854] Der Vorschlag der Europäischen Kommission aus dem Jahr 2021 für die Verordnung über die allgemeine Produktsicherheit zielte darauf ab, klarzustellen, dass das Produktsicherheitsrecht auch für Software gilt.[855] In der Produktdefinition von Art. 3 Abs. 1 Ziff. 1 des GPSR-Vorschlags wurde jedoch weiterhin auf den Begriff «Gegenstand» abgestellt und Software nicht erwähnt.[856] 2022 wurde im Gesetzgebungsverfahren[857] vorgeschlagen, Software explizit als Produkt zu definieren. So enthielt die Stellungnahme des Rechtsausschusses für den Ausschuss für Binnenmarkt und Verbraucherschutz zu dem Verordnungsvorschlag eine neue Erwägung 23a. Darin sollten «materielle und immaterielle

849 Art. 3 Ziff. 6 GPSR.

850 Europäische Kommission, Blue Guide, S. 16 f., wobei sich der Blue Guide noch auf die Produktsicherheitsrichtlinie bezieht; NHK GPSR-Wilrich, Art. 3 N 105, mit Verweis auf die deutsche Lehre.

851 NHK GPSR-Wilrich, Art. 3 N 105.

852 Europäische Kommission, Blue Guide, S. 17.

853 Siehe auch: NHK GPSR-Wiebe, Art. 6 N 35; Piovano/Schucht/Wiebe, S. 9.

854 Europäische Kommission, Impact Assessment GPSR, S. 12.

855 Europäische Kommission, Vorschlag GPSR, S. 14, 16; Reusch, KI und Software, Rn. 20; Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 163, m.w.H.

856 Siehe auch Ackermann/Golling, S. 67, welche hervorheben, dass auch der Entwurf unklar blieb.

857 Verfahren 2021/0170/COD, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/HIS/?qid=1700667068845&uri=CELEX:32023R0988>, zuletzt besucht am 31.05.2025.

Produkte, entweder in Form von eingebetteter Software [vorinstalliert oder nachträglich installiert] oder von eigenständiger Software» explizit in den Anwendungsbereich der Produktsicherheitsverordnung fallen.[858] Statt nur den Begriff «Gegenstand» enthielt der Änderungsantrag 44 für Art. 3 Abs. 1 Ziff. 1 des Entwurfs eine erweiterte Definition für Produkte. Als «Produkt» sollte jeder materielle oder immaterielle «Gegenstand, wie Software oder ein Produkt mit eingebetteter Software» definiert werden.[859]

Wie in Rn. 218 beschrieben, definiert die finale GPSR Produkte in Art. 3 Ziff. 1 GPSR als «Gegenstände». Software erwähnt sie nicht.[860] ErwG 24, 25 und 35 enthalten zumindest Hinweise darauf, dass es sich nicht zwingend um körperliche Gegenstände handeln muss. ErwG 24 spricht bspw. von «nicht eingebettete[n] Gegenstände[n], die beeinflussen, wie ein anderer Gegenstand funktioniert». ErwG 25 hält fest, dass neue Technologien neue Risiken mit sich bringen können, «beispielsweise im Falle eines externen Eingriffs, mit dem ein Produkt gehackt wird oder dessen Eigenschaften verändert werden». Weiter beschreibt ErwG 25, dass «durch neue Technologien [...] das ursprüngliche Produkt erheblich verändert werden [könnte], etwa durch Software-Updates». ErwG 35 spricht von der «digitale[n] Änderung eines Produkts». Gegenstände müssen gem. GPSR also nicht zwingend körperlich sein.[861] 221

In Art. 15 GPSR wird explizit auf in Produkte eingebettete Software eingegangen. Diese Embedded Software wird in aufzählender Weise im Zusammenhang mit in Produkten eingebetteten Teilen und Komponenten von der Verordnung erfasst.[862] Mindestens Embedded Software gilt also für sich selbst als (Teil-)Produkt im allgemeinen Produktsicherheitsrecht.[863] Embedded Software wird bereits in der MRL[864] und in der RED[865] als Risiko anerkannt.[866] 222

858 Europäisches Parlament, Stellungnahme GPSR, Änderungsantrag 13; übernommen in Europäisches Parlament, Bericht Vorschlag GPSR, Änderungsantrag 13, S.134 f., die Klammern stammen aus dem zitierten Text.

859 Europäisches Parlament, Stellungnahme GPSR, Änderungsantrag 44; übernommen in Europäisches Parlament, Bericht Vorschlag GPSR, Änderungsantrag 44, S. 154.

860 Siehe auch NHK GPSR-Wilrich, Art. 3 N 10, m.w.H.

861 Art. 3 Ziff. 1 GPSR; a.A. Wilrich, welcher zum Schluss kommt, dass nur körperliche Gegenstände erfasst sind, NHK GPSR-Wilrich, Art. 3 N 8 f.

862 Art. 15 Abs. 3 lit. a und Abs. 5 GPSR.

863 Ebenso NHK GPSR-Wilrich, Art. 3 N 9; NP GPSR-Schucht/Wiebe, § 3 N 12; ähnlich Beck KI-VO-Wendehorst, Art. 3 Rn. 8 Fn. 9, m.w.H. zur alten Produktsicherheitsrichtlinie.

864 Anhang I, Kapitel 1.2.1. MRL; siehe auch Europäische Kommission, Blue Guide, S. 18 Fn. 42.

865 Art. 3 Abs. 3 lit. i RED; siehe auch Europäische Kommission, Blue Guide, S. 18 Fn. 42.

866 Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 163; siehe auch Europäische Kommission, Blue Guide, S. 18.

223 Die Produktsicherheitsverordnung lässt offen, ob sie auf Stand-alone-Software anwendbar ist.[867] Ein Teil der Lehre geht davon aus, dass Stand-alone-Software nicht als Produkt von der GPSR erfasst ist.[868] Nach hier vertretener Meinung kann Stand-alone-Software jedoch durchaus als von der GPSR erfasst angesehen werden.[869] Die Anerkennung von Stand-alone-Software in der GPSR würde sich auch mit der Produktdefinition der neuen PLD 2024 decken.[870] Auch das europäische Sektorrecht erfasst Software, unabhängig davon, ob sie «embedded» oder «stand-alone» zur Verfügung gestellt wird, immer öfter als Produkt. Dies gilt für Software als Medizinprodukt[871] und als Sicherheitsbauteil in der MVO[872].

224 Unabhängig davon, ob Stand-alone-Software als Produkt anerkannt wird, sind auch gem. GPSR (mindestens «embedded») Standard- und Individualsoftware (Teil-)Produkte. Auch in der GPSR spielt es keine Rolle, ob ein Produkt in Serie oder als Einzelprodukt hergestellt wurde.[873] Damit gelten die gleichen Voraussetzungen wie gem. PrSG und es kann auf die obigen Ausführungen in Rn. 214 verwiesen werden.

1. KI in der GPSR

225 Bei der Erarbeitung der neuen Produktsicherheitsverordnung wurde der Vorschlag zur KI-VO bereits berücksichtigt. Ziel war es, «ein Sicherheitsnetz für Produkte und Risiken für die Gesundheit und Sicherheit der Verbraucher» zu schaffen, «die nicht in den Anwendungsbereich des KI-Vorschlags fallen».[874] Die GPSR kommt bei KI-Systemen im Sinne eines «Sicherheitsnetzes»[875] dort zur Anwendung, wo die KI-VO keine spezifischen Bestimmungen über die Si-

867 Beck KI-VO-Wendehorst, Art. 3 Rn. 8 Fn. 9; Feiler/Forgó, Einführung, S. 12; Rohrssen, S. 113.

868 NHK GPSR-Wilrich, Art. 3 N 11, welcher «Software und andere digitale Produkte» nicht als von der GPSR erfasst sieht. Mit Verweis auf NP GPSR-Schucht/Wiebe, § 3 N 12, welche auch den NHK GPSR-Kommentar herausgegeben haben; Voigt/Hullen, S. 32.

869 Gl.M. Morin, in: Canapa/Richa S. 127; ebenso Rohrssen, S. 113, mit Verweis auf Reusch, KI und Software, Rn. 20, welcher sich jedoch noch auf den Entwurf der GSPR bezieht; ebenfalls Software als Produkt anerkennend die (rechtlich nicht bindende) Europäische Kommission, GPSR FAQ, S. 2.

870 S. u., Rn. 234.

871 S. o., Rn. 179.

872 S. o., Rn. 178.

873 NHK GPSR-Wilrich, Art. 3 N 98, 128.

874 Europäische Kommission, Vorschlag GPSR, S. 6.

875 ErwG 166 KI-VO; siehe auch Voigt/Hullen, S. 217.

cherheit mit dem gleichen Ziel enthält.[876] Gem. Art. 6 Abs. 1 lit. h GPSR müssen Eigenschaften von KI bei der Sicherheitsbewertung von Produkten berücksichtigt werden. Die GPSR ist also auch auf KI-Systeme anwendbar,[877] wenn diese Verbraucherprodukte sind. Da die KI-VO lex specialis zur GSPR ist,[878] ist die GPSR nur dort anwendbar, wo die KI-VO keine Regelung mit dem gleichen Ziel enthält.[879] Dies gilt vor allem für KI-Systeme, die nicht als Hochrisikosysteme gelten.[880] Anzumerken ist hier, dass die von SCHUCHT/WIEBE herausgegebenen GPSR-Kommentare nur Embedded Software als Produkt anerkennen[881] und deshalb vermutlich auch nur Embedded KI. Ihrer Meinung nach ist die GPSR wohl nicht auf Stand-alone-KI-Systeme anwendbar.

2. KI in der KI-VO

Ein KI-System kann gem. Art. 6 Abs. 1 lit. a KI-VO ein eigenständiges Produkt[882] oder Teil eines anderen Produktes[883] sein. Wie bereits ausgeführt, sind KI-Systeme reine Software. Es handelt sich bei Embedded und Stand-alone-KI um das gleiche Konzept wie bei Embedded und Stand-alone-Software.[884] Genau wie Stand-alone-Software kann auch ein KI-System «stand-alone» sein und z.B. via Cloud (bspw. ChatGPT oder Download neuer KI-Funktionen für sich bereits auf dem Markt befindende Produkte) vertrieben werden. Ein Embedded-KI-System kann zwar genau wie Embedded Software in ein Gerät integriert werden, d.h. aber nicht, dass das Gerät selbst zum KI-System respektive zur Software wird.[885] Gemeint ist mit «KI-System» nicht einmal die ganze Software in einem Gerät.[886] Dies zeigt sich bspw. darin, dass KI-Systeme Sicherheitsbauteile in einem Produkt sein können. Das Produkt wird aber vermutlich zusätzliche, weitere Softwarekomponenten haben, die nicht der Sicherheit dienen und auch nicht zu diesem KI-System gehören. Zur Abgrenzung kann darauf abgestellt werden, ob die Komponenten eine Einheit 226

876 Art. 2 Abs. 1 GPSR.
877 Siehe auch NHK GPSR-WIEBE, Art. 6 N 39.
878 ErwG 166 KI-VO.
879 Art. 2 Abs. 1 GPSR; siehe auch NHK GPSR-WIEBE, Art. 6 N 39.
880 NHK GPSR-WIEBE, Art. 6 N 39.
881 NHK GPSR-WIEBE, Art. 6 N 36; NHK GPSR-WILRICH, Art. 3 N 9 ff.; NP GPSR-SCHUCHT/WIEBE, § 3 N 12.
882 Art. 6 Abs. 1 lit. a KI-VO, «das KI-System ist selbst ein solches Produkt».
883 Art. 6 Abs. 1 lit. a KI-VO, «das KI-System soll als Sicherheitsbauteil eines [...] Produkts verwendet werden».
884 S. o., Rn. 81.
885 S. o., Rn. 124.
886 Ebenso, aber mit anderer Schlussfolgerung Beck KI-VO-WENDEHORST, Art. 3 N 24.

bilden.[887] Beeinflussen sich verschiedene Softwarekomponenten *gegenseitig*, müssen sie als Gesamtheit als KI-System beurteilt werden.[888] Enthält ein Produkt jedoch bspw. redundante Sicherheitsbauteile und basiert nur eines auf KI, kann nicht die gesamte Software als KI-System klassifiziert werden. Redundante Sicherheitsbauteile sind nicht miteinander verbunden, damit sie unabhängig voneinander die Sicherheit gewährleisten können. Bspw. könnte die Erkennung einer Treppenkante mittels zwei verschiedener Sicherheitsbauteile erfolgen: ein KI-basiertes Bilderkennungssystem einerseits und ein nicht-KI-gestützter LiDar-Sensor andererseits. Beide könnten eine Treppe unabhängig voneinander erkennen und jeweils einzeln die Funktion auslösen, nicht zu nahe an die Treppenkante heranzufahren.[889]

227 Da die Nachmarktpflichten der KI-VO nur Hochrisiko-KI-Systeme betreffen, ist vorliegend zu prüfen, welche KI-Systeme als Hochrisiko-KI-Systeme gelten. Verbotene KI-Systeme nach Art. 5 KI-VO werden nicht betrachtet, da durch das generelle Verbot auch keine Nachmarktpflichten bestehen. Auch für KI-Systeme mit beschränktem Risiko nach Art. 50 KI-VO und mit geringem Risiko nach Art. 95 KI-VO ergeben sich keine Nachmarktpflichten aus der KI-VO.[890]

228 Gem. Art. 6 Abs. 1 KI-VO gelten KI-Systeme dann als Hochrisiko-KI-Systeme, wenn sie selbst ein Produkt darstellen oder als Sicherheitsbauteil in einem Produkt integriert sind, dieses Produkt oder Sicherheitsbauteil unter die Harmonisierungsvorschriften in Anhang I KI-VO fällt, und kumulativ einer Konformitätsbewertung durch Dritte unterzogen werden muss.[891] Hochrisiko-KI-Systeme im Zusammenhang mit Produkten werden in der KI-VO in zwei Kategorien eingeteilt. Die einen fallen unter die Harmonisierungsvorschriften nach Anhang I Abschnitt A, die anderen unter Abschnitt B KI-VO. Für jene KI-Systeme, die unter die Harmonisierungsvorschriften nach Anhang I Abschnitt B fallen, gelten nur wenige Artikel der KI-VO.[892] Die Nachmarktpflichten gehören nicht dazu. Während die Harmonisierungsvorschriften nach Anhang I Abschnitt A zum NLF gehören, gehören jene nach Abschnitt B fast alle zum «alten

887 Borges, Begriff, Rn. 53.

888 Etwas zurückhaltender Borges, Begriff, Rn. 54.

889 S. u. für ein Beispiel in Rn. 335.

890 Zur Risikoeinteilung siehe Chibanguza/Steege, Rn. 16.

891 Art. 6 Abs. 1 lit. a KI-VO; Beck KI-VO-Ruschemeier, Art. 6 N 28.

892 Gem. Art. 2 Abs. 2 KI-VO handelt es sich um die Art. 6 Abs. 1, Art. 102–109, Art. 112 und u.U. Art. 57 KI-VO; siehe auch Beck KI-VO-Ruschemeier, Art. 6 N 19, welche festhält, dass die Bestimmungen des Abschnitts III nicht für die Vorschriften nach Abschnitt B gelten; ebenso Beck KI-VO-Braun Binder/Egli, Art. 8 N 22.

Rechtsrahmen» und verweisen für detaillierte Regelungen auf die jeweiligen Rechtsakte.[893] Art. 6 Abs. 1 KI-VO und die entsprechenden Pflichten für die darunterfallenden KI-Systeme gelten ab dem 02. August 2027.[894]

Es wird in Art. 6 Abs. 1 KI-VO also ausdrücklich festgehalten, dass KI-Systeme eigenständige Produkte sein können, unabhängig davon, ob sie «embedded» oder «stand-alone» sind.[895] Es sind jedoch nur KI-Systeme als selbstständige Produkte erfasst, wenn auch Software von der jeweiligen (sektoralen) Produktsicherheitsrichtlinie oder -verordnung als Produkt erfasst ist.[896] In Bezug auf Smart Home Devices muss die RED genauer angeschaut werden: Sie ist in Anhang I Abschnitt A Ziff. 6 KI-VO als eine von 20 Richtlinien und Verordnungen aufgeführt. Software ist zwar in der RED erfasst, stellt aber für sich selbst keine Funkanlage dar und kann somit in der RED nicht als eigenständiges Produkt gelten.[897] KI-Systeme können jedoch als Sicherheitsbauteile in Funkanlagen eingesetzt werden.[898] Dies führt dazu, dass diese sektoralen Richtlinien und Verordnungen nur die «alten» Gefahren[899] abdecken und auch nur zu deren Eindämmung anwendbar sind. Diese alten Gefahren betreffen bei Funkanlagen gem. Art. 3 Abs. 1 lit. a RED die Gesundheit und Sicherheit von Menschen und Haus- und Nutztieren sowie den Schutz von Gütern einschliesslich der in der LVD enthaltenen Sicherheitsziele (ohne Anwendung der Spannungsgrenze) sowie nach lit. b die elektromagnetische Verträglichkeit. Nicht beinhaltet sind aber z.B. Gefahren aufgrund extensiver Datenerfassungen.[900] Neue KI-Risiken werden nicht abgedeckt, weil KI-Systeme ohne die spezifische Erfassung von Software in den Harmonisierungserlassen nicht als Produkte gelten.[901] Der Sicherheitsbegriff orientiert sich an den Sektorerlassen, welche andere Ziele als die KI-VO verfolgen.[902] Das bedeutet, dass die meisten sektoralen Richtlinien und Verordnungen angepasst werden müssten, damit sie für Software als eigenständige Produkte gelten könnten. 229

893 Beck KI-VO-Wendehorst, Art. 2 N 33 f., m.w.H.; siehe auch Krimphove, S. 154, mit einer beispielhaften Auflistung.
894 Art. 113 lit. c KI-VO.
895 Siehe auch ErwG 12 KI-VO.
896 Beck KI-VO-Ruschemeier, Art. 6 N 39.
897 S. o., Rn. 177.
898 S. u., Rn. 230.
899 Beck KI-VO-Ruschemeier, Art. 6 N 59, mit Bezug auf die Spielzeugrichtlinie, welche jedoch Software ebenfalls nicht als eigenständiges Produkt erfasst. Siehe dazu N 58.
900 Beck KI-VO-Ruschemeier, Art. 6 N 59.
901 Beck KI-VO-Ruschemeier, Art. 6 N 60.
902 Beck KI-VO-Ruschemeier, Art. 6 N 60.

230 Während früher zur Gefahrenabwehr mechanische Schutzmassnahmen eingesetzt wurden, übernehmen heute auch elektronische Systeme diese Funktion.[903] Ein «intelligenter» Sensor eines Küchengerätes, der das Schneiden stoppt, wenn ein Körperteil im Weg ist, hat bspw. eine Sicherheitsfunktion. KI-Systeme können insbesondere als Sicherheitsbauteile negative Auswirkungen auf die Gesundheit und Sicherheit von Personen haben.[904] Sie zählen deshalb auch als Hochrisiko-KI-Systeme, wenn sie einer Konformitätsprüfung durch Dritte unterliegen und Teil einer der Harmonisierungsvorschriften nach Anhang I KI-VO sind.[905] Art. 3 Ziff. 14 KI-VO definiert das «Sicherheitsbauteil» als «einen Bestandteil eines Produkts oder KI-Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet».[906] Ein KI-System gilt als Sicherheitsbauteil, wenn es entweder mit dem System oder Produkt «funktional verbunden» oder darin eingebettet ist[907], «ohne dass Software selbst als Produkt im Sekundärrecht adressiert sein muss»[908]. KI-Systeme können deshalb auch als Sicherheitsbauteile i.S.v. Art. 3 Ziff. 14 KI-VO in Funkanlagen gelten, obwohl die RED als Harmonisierungsvorschrift nach Anhang I Software nicht direkt als Produkt erfasst. So könnte bspw. eine Bilderkennungssoftware ein Sicherheitsbauteil sein,[909] die einem Staubsaugerroboter Informationen dazu liefert, ob er ein Objekt umfahren muss oder nicht.[910] Will man bei der alten Einteilung bleiben, ist ein KI-System, das die Sicherheitskomponente eines Produktes darstellt, ein «Embedded-KI-System».[911]

231 Wenn KI-Systeme als Produkte oder als Sicherheitsbauteile also aufgrund ihrer zugehörigen Harmonisierungsvorschriften nach Anhang I KI-VO einer Konformitätsbewertung durch Dritte bedürfen, dann gelten sie als Hochrisiko-KI-Systeme. Es kommt somit auf die Zweckbestimmung des konkreten

903 Freytag, S. 29.
904 ErwG 47 KI-VO.
905 Art. 6 Abs. 1 KI-VO.
906 Siehe auch den Hinweis bei Ruschemeier, dass «die erfassten Rechtsgüter sehr weit» seien, wobei aber die Grundrechte nicht als geschützte Rechtsgüter genannt sind, Beck KI-VO-Ruschemeier, Art. 6 N 42 Fn. 38, m.w.H. S. u., Rn. 266.
907 Beck KI-VO-Wendehorst, Art. 3 N 151.
908 Beck KI-VO-Ruschemeier, Art. 6 N 42.
909 Für ein ähnliches Beispiel in Bezug auf Drohnen siehe Krumm/Meyer, S. 21.
910 Wobei die Abgrenzung zwischen «Sicherheitsfunktion und allgemeiner Produktfunktion» nicht ganz klar ist, siehe dazu Beck KI-VO-Wendehorst, Art. 3 N 153 f. Für ein Beispiel s. u., Rn. 335.
911 Beck KI-VO-Braun Binder/Egli, Art. 8 N 19; Borges, Begriff, Rn. 46.

Produktes an, ob ein KI-System ein Hochrisiko-KI-System ist oder nicht,[912] und welche Pflichten damit verbunden sind.[913] Dasselbe KI-System kann also bei verschiedenen Verwendungen einmal als Hochrisiko-KI-System und einmal als Nicht-Hochrisiko-KI-System gelten.[914]

232 Zusätzlich gelten gem. Art. 6 Abs. 2 KI-VO auch die KI-Systeme aus Anhang III der KI-VO als Hochrisikosysteme. Ausnahmsweise gilt ein KI-System gem. Art. 6 Abs. 3 KI-VO aber nicht als Hochrisiko-KI-System, wenn es «kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst». Es handelt sich bei der Aufzählung in Anhang III um Umschreibungen von Anwendungsbeispielen (engl. «Use Cases»).[915] Es ist jedoch keiner dieser Use Cases für Smart Home Devices relevant.[916] Diese Liste kann von der EU-Kommission gem. Art. 7 KI-VO indes noch angepasst werden.

233 Wird ein KI-System als Hochrisiko-KI-System klassifiziert, heisst das nicht automatisch, dass das Produkt nach den Harmonisierungsvorschriften mit einem hohen Risiko verbunden ist.[917] Die Risikoeinstufung der KI-VO wirkt nicht auf das Produktsicherheitsrecht zurück.[918] Das Verhältnis der KI-VO zu den Harmonisierungsvorschriften in Anhang I KI-VO wird gem. Art. 96 Abs. 1 lit. e KI-VO noch via Leitlinie spezifiziert.

VII. Exkurs: Software in der PLD 2024 und im CRA

234 Nachdem der Entwurf der neuen PLD 2024 Software bereits vorbehaltlos als Produkt erfasste,[919] wurde dies in der 2024 in Kraft getretenen finalen Version bestätigt.[920] Die PLD 2024 hält fest, dass Produkte «körperlicher oder nichtkörperlicher Art sein» können und Software «eine immer wichtigere Rolle für

912 Buchalik/Gehrmann, Rn. 45.
913 Braun Binder/Egli, Umgang, S. 628.
914 Buchalik/Gehrmann, Rn. 45.
915 Buchalik/Gehrmann, Rn. 33.
916 Denkbar wäre zukünftig ein Smart Home Device mit einem KI-System, welches gem. Anhang III, Ziff. 1 lit. c KI-VO zur bestimmungsgemässen Emotionserkennung verwendet werden soll.
917 ErwG 51 KI-VO.
918 Beck KI-VO-Ruschemeier, Art. 6 N 19.
919 Europäische Kommission, Vorschlag PLD 2024, Art. 4 Abs. 1; ausführlich dazu: Spindler, Vorschläge, Rn. 4 ff.; Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 163.
920 Art. 4 Abs. 1, ErwG 13 PLD 2024.

die Produktsicherheit» spiele, da «durch ihre Ausführung Schäden» verursacht werden können.[921] Als Beispiele für Software werden «Betriebssysteme, Firmware, Computerprogramme, Anwendungen oder KI-Systeme» aufgezählt.[922] Zudem wird klargestellt, dass es keine Rolle spielt, wie Software bereitgestellt oder genutzt wird, und somit auch SaaS erfasst ist.[923] So sind Embedded und Stand-alone-Software (und damit auch KI-Systeme) also als Produkte von der PLD 2024 erfasst. Der «Rechtsstreit zur alten Rechtslage» wird damit auch in Bezug auf das Produktsicherheitsrecht als «erledigt» bezeichnet.[924] Reiner Quellcode wird in der PLD 2024 nicht als Produkt erfasst, da es sich gem. der EU-Kommission nur um Information handelt und, wie von SPINDLER hervorgehoben, nicht um «maschinenausführbare Codierung».[925] Reine Informationen wie der «Inhalt digitaler Dateien wie Mediendateien oder E-Books»[926] und Dienstleistungen[927] sind somit ebenfalls weiterhin nicht als Produkte im europäischen Produkthaftungsrecht erfasst. Dafür werden in Art. 4 Ziff. 3 PLD 2024 neu «verbundene Dienste» als digitale Dienste, die funktionsrelevant in Produkte integriert oder damit verbunden sind, und in Art. 4 Ziff. 4 PLD 2024 «Komponenten» auch als nichtkörperliche Gegenstände oder verbundene Dienste definiert.[928] Somit ist nun auch Zusatzsoftware wie bspw. eine mobile App in der PLD 2024 geregelt.[929]

235 Neben der Definition von Software[930] enthält der CRA in Art. 3 Ziff. 1 auch eine Definition zum Produkt mit digitalen Elementen. Es handelt sich dabei um «ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschliesslich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden». Es kann sich dabei auch um KI-Systeme handeln.[931] Die «Datenfernverarbeitung» wird in Art. 3 Ziff. 2 CRA als «entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte» bezeichnet. Beispiele für Produkte mit digitalen Elementen sind «Pro-

921 ErwG 13 PLD 2024.
922 ErwG 13 PLD 2024.
923 ErwG 13 PLD 2024.
924 DENGA, Rn. 24 Fn. 50, m.w.H.
925 SPINDLER, Vorschläge, Rn. 5; ErwG 13 PLD 2024.
926 ErwG 13 PLD 2024.
927 ErwG 17 PLD 2024.
928 S. o., Rn. 213.
929 Beck KI-VO-WENDEHORST, Art. 1 N 99.
930 S. o., Rn. 110.
931 Art. 12 Abs. 1 CRA, siehe auch ErwG 51 CRA.

dukte wie intelligente Haushaltsgeräte mit Sicherheitsfunktionen, einschliesslich intelligenter Türschlösser, Babyphone-Systemen und Alarmanlagen, vernetztes Spielzeug und am Körper tragbare medizinische Geräte (Wearables)».[932] Smart Home Devices und ihre Softwarekomponenten sind ebenfalls als Produkte mit digitalen Elementen erfasst.[933] Auch Produkte mit digitalen Elementen sind reine Softwareprodukte (also Stand-alone-Software wie mobile Apps[934]).

VIII. Zwischenfazit für die EU

Smart Home Devices sind Produkte i.S.d. GPSR, wobei sie gesamthaft unter die RED fallen und die GPSR nur subsidiär anwendbar ist. Im allgemeinen Produktsicherheitsrecht der EU sind Hardware, Embedded sowie Stand-alone- und Individual- sowie Standardsoftware nach vorliegend vertretener Meinung als Produkte erfasst. KI-Systeme sind deshalb ebenfalls als Produkte in der GPSR erfasst. Ergeben sich aus einem Smart Home Device Gefahren, die direkt auf Software zurückzuführen sind, kann die Software als eigenständiges gefährliches Produkt beurteilt werden, ohne Beschränkung auf ein bestimmtes Smart Home Device. Die Nachmarktpflichten der GPSR gelten somit auch für Software. Da die GPSR nur auf Konsumentenprodukte anwendbar ist, gelten ihre Nachmarktpflichten auch nur für Software und damit KI, wenn sie von Privaten verwendet wird oder vorhersehbar verwendet werden kann. Wo die KI-VO Regelungen mit dem gleichen Ziel enthält, geht diese als lex specialis der GPSR vor. 236

Die Nachmarktpflichten aus der KI-VO gelten nur für solche Hochrisiko-KI-Systeme, die entweder selbst Produkte sind oder als Sicherheitsbauteil in einem Produkt integriert sind, die unter die Harmonisierungsvorschriften nach Anhang I Abschnitt A KI-VO fallen und kumulativ eine Konformitätsbewertung durch Dritte nötig ist. Zudem gelten die Nachmarktpflichten für Hochrisiko-KI-Systeme, wenn sie von Anhang III KI-VO erfasst sind (unter Beachtung der Ausnahme nach Art. 6 Abs. 3 KI-VO). In Bezug auf Smart Home Devices sind jedoch vor allem Hochrisiko-KI-Systeme als Sicherheitsbauteile von in Anhang I Abschnitt A KI-VO harmonisierten Produkten relevant. Da die Nachmarktpflichten der KI-VO nicht für KI-Systeme als eigenständige Produkte gelten, wenn sie nicht explizit von den Harmonisierungsrechtsakten erfasst 237

932 ErwG 10 CRA.
933 Reusch, Produkt, S. 97.
934 Reusch, Produkt, S. 97.

sind, können auf solche KI-Systeme nur die Regeln der GPSR angewendet werden. Auch im Fall von Sicherheitsbauteilen, die Nicht-Hochrisiko-KI-Systeme sind, weil sie bspw. nicht einer Konformitätsbewertung durch Dritte unterliegen, regelt die KI-VO keine Nachmarktpflichten und es sind deshalb die Nachmarktpflichten der GPSR anwendbar.

238 Dienstleistungen sind auch im Produktsicherheitsrecht der EU keine Produkte, wobei aber digitale Dienste unter die neue PLD 2024 fallen können. Die nun klare Erfassung von Software als Produkt in der PLD 2024 und im CRA ist sinnvoll und sollte auch in einer überarbeiteten Fassung der GPSR ergänzt werden.

IX. Fazit

239 Hardware und Embedded Software sind in der Schweiz und der EU im allgemeinen Produktsicherheitsrecht – also dem PrSG und der GPSR – unbestritten als Produkte anerkannt. Nach vorliegend vertretener Meinung kann auch Stand-alone-Software als Produkt im allgemeinen Produktsicherheitsrecht anerkannt werden. Weiter darf es keinen Unterschied machen, ob Individual- oder Standardsoftware vorliegt. Da es sich bei KI um Software handelt, darf für KI nichts anderes gelten. Für Dienstleistungen gelten keine Nachmarktpflichten, da sie im Produktsicherheitsrecht nicht als Produkte gelten.

240 Während die GPSR sich ganzheitlich nur auf Verbraucherprodukte bezieht, schränkt das PrSG den Anwendungsbereich diesbezüglich nur bei den Nachmarktpflichten ein. Die KI-VO reguliert KI-Systeme, ohne zwischen B2B- und B2C-Produkten zu unterscheiden.

241 Smart Home Devices sind Konsumentenprodukte und fallen als Endprodukt in der Schweiz unter die NEV und die FAV. In der EU unterliegen sie der RED. Je nachdem können sie auch weiterem Sektorrecht unterstehen, welches hier aber nicht genauer betrachtet wird. Für Smart Home Devices sicherheitsrelevante Software kann in der Schweiz unter das PrSG und in der EU unter die GPSR respektive als Hochrisiko-KI-System unter die KI-VO fallen. Es sind somit in der Schweiz und der EU Nachmarktpflichten verschiedener Gesetze für Smart Home Devices zu beachten. Dies soll in der nachfolgenden Tabelle 2 und in Tabelle 3 veranschaulicht werden. Da die vorliegende Arbeit vor allem Software und KI-Systeme als Produkte untersucht, beschränken sich die weiteren Kapitel auf sicherheitsrelevante Software (inklusive KI) als Produkt. Damit werden die Nachmarktpflichten, die für Software Geltung erlangen, nach dem PrSG, der GPSR und der KI-VO genauer untersucht und verglichen. Lediglich

ergänzend werden die NEV und die FAV behandelt, da Software weder als Niederspannungserzeugnis noch als Funkanlage von diesen Erlassen erfasst wird.

Tabelle 2: Anwendungsbereich der Nachmarktpflichten 242

Gelten die Nachmarktpflichten nach			
CH	**EU**		
PrSG (nur Konsumentenprodukte)	**GPSR (nur Konsumentenprodukte)**	**KI-VO (alle KI-Systeme)**	
			für folgende Produkte oder Dienstleistungen?
Ja	Ja	Nein	Herkömmliche/ Physische Produkte
Ja	Ja	Ja, aber nur wenn Hochrisiko-KI-System	Embedded Software
Ja (h.L.)	Ja (vorliegend vertreten)	Ja, aber nur wenn Hochrisiko-KI-System	Stand-alone-Software
Ja (vorliegend vertreten)	Ja (vorliegend vertreten)	Nein	KI-System
Keine Anwendung in der Schweiz	Nein, da lex generalis zu KI-VO	Ja	Hochrisiko-KI-System nach KI-VO
Nein	Nein	Nein	Klassische Dienstleistungen
Nur Software inkl. KI. Für physische Teile und das gesamte Gerät sind Pflichten aus der NEV und der FAV anwendbar.	Nur Software inkl. Nicht-Hochrisiko-KI. Für physische Teile und das gesamte Gerät sind bspw. Pflichten aus der RED anwendbar.	Nur Sicherheitsbauteil als Hochrisiko-KI-System.	Smart Home Devices

B. Schutzumfang der produktsicherheitsrechtlichen Nachmarktpflichten in der Schweiz und der EU

243 In diesem Kapitel wird erläutert, welche Rechtssubjekte, Schutzobjekte und Rechtsgüter durch das schweizerische und durch das europäische Produktsicherheitsrecht geschützt werden.

I. Geschützte Rechtssubjekte und Schutzobjekte

244 Werden die Pflichten des Produktsicherheitsrechts nicht beachtet, handelt es sich um Sorgfaltspflichtverletzungen.[935] Daraus können sich Personen-, Sach- oder Vermögensschäden ergeben.[936] Siehe dazu die Beispiele in Kapitel Teil 1:D.I «Beispiele unsicherer Software- und KI-Produkte und ihr Gefahrenpotenzial».

1. Natürliche Personen

245 Obwohl Art. 8 PrSG die Nachmarktpflichten auf Konsumentenprodukte einschränkt, sind nicht nur Konsumenten durch die Vorschrift geschützt. Nach Art. 3 Abs. 1 PrSG dürfen nur Produkte in Verkehr gebracht werden, wenn sie bei normaler oder bei vernünftigerweise vorhersehbarer Verwendung die Sicherheit und Gesundheit von Verwendern und Dritten nicht oder nur geringfügig gefährden. Die produktsicherheitsrechtlichen Nachmarktpflichten sollen sicherstellen, dass auch nur sichere Produkte in Verkehr bleiben.[937] Die geschützten Rechtssubjekte des PrSG und der Nachmarktpflichten nach Art. 8 PrSG sind also Verwender und Dritte. Art. 7 Abs. 1 lit. a FAV hält fest, dass der Schutz der Gesundheit und der Sicherheit von Menschen gewährleistet sein muss. Zudem schreibt die FAV Nachmarktpflichten zum Schutz der Gesundheit und Sicherheit von Endnutzern vor.[938] Gem. Art. 3 NEV dürfen Niederspannungserzeugnisse die Sicherheit von Personen nicht gefährden. Die

935 S. u., Rn. 305.
936 Gerster, Rn. 423 f., mit Beispielen.
937 S. u., Rn. 305 ff.
938 Art. 23 Abs. 1 FAV.

Produktsicherheitsrichtlinie schützte die Gesundheit und Sicherheit von Personen.[939] Die GPSR zielt auf den Schutz der Gesundheit und Sicherheit von Verbrauchern ab.[940] Ein KI-System als Sicherheitsbauteil darf gem. Art. 3 Ziff. 14 KI-VO bei einem Ausfall oder einer Störung die Gesundheit und Sicherheit von Personen nicht beeinträchtigen.[941] Grundsätzlich sollen KI-Systeme «auf den Menschen ausgerichtet»[942] sein und «zum Wohle der Menschen eingesetzt werden»[943].

Die Vorschriften des PrSG dienen der Vermeidung der menschlichen Gefährdung von Sicherheit und Gesundheit.[944] Verwender ist, wer mit einem Produkt direkt interagiert. Der Begriff des Verwenders beinhaltet den Konsumenten.[945] Mit den Dritten sind sog. «innocent bystanders» oder auch «unbeteiligte Drittpersonen» gemeint, welche ohne irgendwelche Mitwirkung in den Gefahrenbereich des Produktes geraten.[946] Als Verbraucher nach der GPSR werden alle natürlichen Personen verstanden, «die zu Zwecken handel[n], die ausserhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit liegen».[947] Im Produktsicherheitsrecht decken sich die Inhalte des Begriffs «Konsument» der Schweiz mit denen des Begriffs «Verbraucher» des europäischen Rechts.[948] Wie in der Schweiz sind in der GPSR auch Verwender und Dritte vom persönlichen Schutzbereich erfasst.[949] 246

Einen erhöhten Schutz geniessen vulnerable Personengruppen. Produkte für «besonders gefährdete Personengruppen»[950] müssen in der Schweiz so konzipiert sein, dass auch dieser Gruppe zugehörige Personen vor Gefahren ge- 247

939 Art. 2 lit. b Produktsicherheitsrichtlinie; ausführlich dazu Bühler, Bestandteil, S. 44.

940 Art. 3 Abs. 2, ErwG 4 GPSR.

941 Der Schutz der Gesundheit und Sicherheit wird in der KI-VO oft hervorgehoben, siehe auch Beck KI-VO-Wendehorst, Art. 1 N 32.

942 Art. 1 Abs. 1 KI-VO.

943 Beck KI-VO-Wendehorst, Art. 1 N 44.

944 Botschaft PrSG, S. 7431; siehe auch Wey, in: Fellmann/Furrer, Schonzeit, S. 36.

945 Brunner, in: Fellmann/Furrer, Schonzeit, S. 75 ff.; Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 37.

946 Botschaft PrSG, S. 7431; Brunner, in: Fellmann/Furrer, Schonzeit, S. 75; Bühler/Tobler, S. 367, 371; Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 26; Fellmann, Jusletter 25.10.2010, Rn. 23, m.w.H.; SHK PrSG-Hess, Art. 3 N 4, m.w.H.

947 Art. 3 Ziff. 17 GPSR.

948 Fellmann, Jusletter 25.10.2010, Rn. 16; die Begriffe ebenfalls synonym verwendend: Bühler/Tobler, S. 394; SHK PrSG-Hess, Art. 8 N 8; Holliger-Hagmann, Fallstricke, S. 130.

949 NP GPSR-Schucht/Wiebe, § 4 N 15.

950 Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 31.

schützt sind.[951] In der GPSR sind besonders schutzbedürftige Verbraucher ebenfalls besonders geschützt, indem sie bei der Sicherheitsbewertung eines Produktes speziell berücksichtigt werden müssen, wenn sie zu den Verwendern des fraglichen Produktes gehören.[952] In der Schweiz[953] sowie in der EU[954] werden Kinder, ältere Menschen oder Menschen mit einer Behinderung zu den schutzbedürftigen Verbrauchern gezählt. Ausserdem müssen in der EU «die Auswirkungen geschlechtsspezifischer Unterschiede auf Gesundheit und Sicherheit» berücksichtigt werden.[955] Insbesondere Kinder werden dort stark geschützt.[956]

248 Auch im Bereich digitaler Produkte ist es essenziell, dass diese vulnerable Personengruppen nicht gefährden.[957] Schutzbedürftige Personen können aufgrund ihrer jeweiligen Vulnerabilität besonderen Gefahren durch unsichere Produkte ausgesetzt sein, da sie über eingeschränkte Ressourcen, geringere digitale Kompetenzen (engl. «digital literacy»)[958] oder fehlende technische Fähigkeiten verfügen können, um potenzielle Risiken zu identifizieren, angemessen darauf zu reagieren oder sich davor zu schützen. Ist bspw. nicht transparent, wie ein digitales Produkt auf bestimmte Eingaben reagiert, kann die Risikoeinschätzung erschwert werden.[959] Ebenso können Gefahren bestehen bleiben, wenn Updates zwar sicherheitsrelevante Probleme beheben, betroffene Personen jedoch ihre Notwendigkeit nicht erkennen und sie daher nicht installieren. Menschen mit Beeinträchtigungen können zudem vor besonderen Herausforderungen stehen, wenn sie bspw. Warnhinweise nicht oder nur eingeschränkt wahrnehmen oder komplexe Nutzungsbedingungen nur eingeschränkt verstehen können. Besonders im Kontext von KI-Systemen ist eine kritische Reflexion der generierten Ergebnisse erforderlich. Fehlt jedoch das notwendige Wissen zur Beurteilung dieser Systeme, ist eine fundierte Hinter-

951 Art. 3 Abs. 3 lit. d PrSG; Botschaft PrSG, S. 7437 f.; Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 31; siehe auch Bühler, Bestandteil, S. 52.

952 Art. 6 Abs. 1 lit. e, ErwG 23 GPSR.

953 Beispielhaft aufgezählt und nicht abschliessend in Art. 3 Abs. 3 lit. d PrSG; siehe auch Botschaft PrSG, S. 7437 f.

954 Art. 6 Abs. 1 lit. e, ErwG 5, 23 GPSR.

955 Art. 6 Abs. 1 lit. e, ErwG 5, 23 GPSR.

956 Art. 6 Abs. 1 lit. d und f, ErwG 23 GPSR.

957 ErwG 23 GPSR.

958 Siehe bspw. die Statistik zu digitalen Kompetenzen, welche grosse Unterschiede zwischen den Altersgruppen zeigt: Website des Bundesamts für Statistik, abrufbar unter <https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/gesamtindikatoren/haushalte-bevoelkerung/digitale kompetenzen.html>, zuletzt besucht am 31.05.2025.

959 S. o., Rn. 60 ff.

fragung nicht möglich, was die Gefahr von Fehlinterpretationen[960] oder unreflektierter Nutzung erhöht.[961]

2. Tiere, Sachen und Vermögen

Neben natürlichen Personen können auch Tiere, Sachen und Vermögen durch unsichere Produkte beeinträchtigt werden. Das PrSG verpflichtet den Hersteller nicht zum Schutz vor Sach- und Vermögensschäden. So sind bspw. Tiere[962] und «eine datenschutzrechtliche, umweltbezogene oder finanzielle Sicherheit» nicht durch das PrSG geschützt.[963] Somit gilt ein Produkt nicht als unsicher im Sinne des PrSG, wenn es Schäden an Sachen oder am Vermögen verursachen kann.[964] Dasselbe galt für die Produktsicherheitsrichtlinie.[965] Im Gegensatz dazu schützt die NEV zusätzlich die Sicherheit von Haustieren und Sachen, jedoch nicht die Gesundheit.[966] Die FAV schützt zusätzlich noch Nutztiere.[967] Im allgemeinen Produktsicherheitsrecht der EU wird der sachliche Schutzbereich in Art. 5 i.V.m. Art. 3 Ziff. 2 GPSR definiert.[968] Sachen und andere Vermögenswerte sowie Daten sind nicht geschützt.[969] Diese können jedoch – wie z.B. Tiere – von spezifischem Sektorrecht geschützt sein.[970] Nach Art. 3 Ziff. 14 KI-VO darf ein KI-System als Sicherheitsbauteil bei einem Ausfall oder einer Störung auch Eigentum nicht gefährden.[971] 249

Wie soeben dargelegt, sind Sachen als Vermögenswerte nicht vom allgemeinen Produktsicherheitsrecht geschützt. Holliger-Hagmann hält fest, dass der Schutz von Sicherheit und Gesundheit «auch den Schutz von Sachen implizieren» könne.[972] Nach ihr bezweckt das PrSG die Vermeidung von Sachschäden, die zu einer Beeinträchtigung der körperlichen Unversehrtheit von Menschen führen können. So müsse ein Rauchmelder funktionieren, damit er eine Person 250

960 Siehe auch Beck KI-VO-Braun Binder/Egli, Art. 10 N 52.

961 Diese Gefahr besteht selbstverständlich nicht nur für vulnerable Personengruppen.

962 Einige sektorielle Erlasse nennen jedoch bspw. Haus- oder Nutztiere als Schutzobjekte. Siehe dazu eine Auflistung von Beispielen in SHK PrSG-Hess, Art. 3 N 6.

963 SHK PrSG-Hess, Art. 3 N 5.

964 Bühler, Bestandteil, S. 44; SHK PrSG-Hess, Art. 3 N 1.

965 Art. 2 lit. b Produktsicherheitsrichtlinie; SHK PrSG-Hess, Art. 3 N 1.

966 Art. 3 NEV.

967 Art. 7 Abs. 1 lit. a FAV. Die Tiere in den Beispielen des Staubsaugerroboters und des Katzenklos in Rn. 25 und 26 wären also von der NEV und FAV als Schutzobjekte erfasst.

968 Siehe auch NHK GPSR-Wiebe, Art. 5 N 13.

969 NHK GPSR-Wiebe, Art. 5 N 19; siehe auch NP GPSR-Schucht/Wiebe, § 4 N 14.

970 NHK GPSR-Wiebe, Art. 5 N 18 f. mit Verweis auf die LVD.

971 Feiler/Forgó, Art. 3 N 76; siehe auch Beck KI-VO-Wendehorst, Art. 1 N 47.

972 Holliger-Hagmann, Fallstricke, S. 120 f.

vor einem Brand schützen könne.[973] Das BGer hielt 2013 fest, wenn der Gebrauchswert eines Produktes in der Abwehr von Schäden bestehe, lägen auch die Gebrauchstauglichkeit und die Sicherheit eng zusammen.[974] Daraufhin hat es entschieden, dass ein Funktionsmangel bei einem Feuerlöscher ein Sicherheitsmangel im Sinne des STEG war.[975] Dasselbe gilt für das PrSG.[976] Geschützt ist bei Produkten, die der Sicherheit dienen, also die Funktionsfähigkeit des Produktes, weil der Ausfall ihrer Funktion ein besonderes Gefährdungspotenzial mit sich bringt. Dadurch ist aber nicht der Vermögenswert des Produktes geschützt, sondern die Gesundheit und Sicherheit der Personen, die durch das Nichtfunktionieren des Produktes Gefahr laufen, beeinträchtigt werden zu können. Auch gem. der GPSR dürfen Produkte mit «Sicherheits- bzw. Schutzfunktion» keine sicherheitsrelevanten Funktionsmängel aufweisen.[977] Ebenfalls darf gem. Art. 3 Ziff. 14 KI-VO der Ausfall oder die Störung von Produktbestandteilen, die der Sicherheit eines Produktes dienen, keine Gefahr für die Gesundheit und Sicherheit von Personen oder von Eigentum darstellen.[978]

II. Geschützte Rechtsgüter

251 Die wichtigsten geschützten Rechtsgüter des PrSG, der NEV,[979] der FAV, der GPSR und der KI-VO sind die Sicherheit und Gesundheit von natürlichen Personen.[980] In diesem Kapitel wird zudem dargelegt, was genau unter «Gesundheit» verstanden wird und was diese umfasst. «Sicherheit» und «Gefahr» sind «Komplementärbegriffe».[981] Macht man die Definition von «Sicherheit» ab-

973 Holliger-Hagmann, Fallstricke, S. 120 f.; ebenso in Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 27; bereits ähnlich Röthlisberger, S. 45; a.A. Bühler/Tobler, S. 122.

974 BGE 139 II 534, 540 E. 4.4, mit Verweis auf BGE 64 II 254 (bekannt als «Steiggurtfall»); siehe auch Klett/Müller, S. 440.

975 BGE 139 II 534, 541 E. 4.6.

976 Klett/Müller, S. 440.

977 NHK GPSR-Wiebe, Art. 5 N 31; NP GPSR-Schucht/Wiebe, § 4 N 21.

978 Zum Sicherheitsbauteil s. o., Rn. 230.

979 Art. 3 NEV nennt nur die Sicherheit von Personen, Haustieren und Sachen, nicht aber die Gesundheit. Die Erwähnung des Schutzes der Gesundheit wurde 2022 gestrichen, da das EleG keine genügende gesetzliche Grundlage dafür bot, siehe Fn. 16 NEV.; UVEK, Erläuternder Bericht Revision NEV, S. 2. Trotzdem müssen gem. Art. 24 NEV weiterhin Risiken für die Gesundheit beobachtet werden.

980 SHK PrSG-Hess, Art. 3 N 5, mit Ausführungen zur eigentlichen Ununterscheidbarkeit von «Sicherheit und Gesundheit», welche gemäss ihm ein «etabliertes Begriffspaar» darstellen. Er verwendet den Begriff «Schutzgüter»; Bühler/Tobler, S. 371, verweisen auf Hess, gebrauchen jedoch den Begriff «Schutzobjekt».

981 Seiler, S. 46, 155; siehe auch: Bühler, Bestandteil, S. 53; Bühler/Tobler, S. 124, 127.

hängig von der Definition der «Gefahr», muss geklärt werden, wie «Gefahr» definiert ist.

1. Gesundheit

Der Begriff «Gesundheit» ist weder im PrSG noch in der FAV definiert. 252
Bühler[982] verweist für eine Definition auf die Präambel der WHO-Verfassung[983], welche auch vom EuGH[984] beigezogen wird. Danach wird «Gesundheit» als «Zustand des vollständigen körperlichen, geistigen und sozialen Wohlbefindens und nicht nur als Freisein von Krankheit und Gebrechen» verstanden.[985] Zur Auslegung des Begriffs «Gesundheit» kann auch Art. 118 BV zu Hilfe gezogen werden, da sich das PrSG mindestens teilweise darauf stützt.[986] In der Schweiz ist die Gesundheit «als Gegenbegriff zu Krankheit (bzw. Körperverletzung oder Behinderung) zu verstehen».[987] Das BGer hat für die Definition von «Gesundheit» – soweit ersichtlich – erst in einem Entscheid auf die WHO verwiesen und es hat den Gesundheitsbegriff somit weiter ausgelegt als bis anhin.[988] Auch wenn der Gesundheitsbegriff in der Schweiz enger als jener der WHO zu sein scheint,[989] schützt auch die BV die physische und die psychische Gesundheit.[990]

---

982 Bühler, Bestandteil, S. 132, mit Verweis auf Faeh, S. 53 Fn. 439. Bühler zitiert zwar den Wortlaut von FAEH, welche statt des Wortes «sozialen» den englischen Begriff «social well-being» im Original als «psychisch-seelischen» übersetzt. In allen auf der Website des Bundes verfügbaren und auf Deutsch übersetzten Versionen (seit 2005) heisst es in der Verfassung der WHO jedoch «sozialen».

983 Verfassung der Weltgesundheitsorganisation für die Schweiz in Kraft getreten am 7. April 1948, SR 0.810.1 (zit. WHO-Verfassung).

984 EuGH vom 19.09.2013, C-579/12 RX-II, Réexamen Commission / Strack, ECLI:EU:C:2013:570, Rn. 44; EuGH vom 09.09.2003, C-151/02, Jaeger, ECLI:EU:C:2003:437, Rn. 93; EuGH vom 12.11.1996, C-84/94, Vereinigtes Königreich / Rat, ECLI:EU:C:1996:431, Rn. 15.

985 Präambel, Satz 2 WHO-Verfassung.

986 Siehe Rn. 149.

987 SGK BV-Tomas/Bernhard, Art. 118 N 9; ähnlich BSK BV-Gächter/Renold-Burch, Art. 118 N 6.

988 Konkret bezogen auf die Definition von «Gesundheit» bzw. «santé», da es sich um einen französischen Entscheid handelt, in BGer 2C-136/2024 vom 13.09.2024, E. 4.8; ansonsten bspw. auf den «Zustand vollkommenen Wohlbefindens» eingehend BGer 9C_482/2014 vom 20.03.2015, E. 3.2; mit Verweis auf verschiedene Krankheiten nach ICD-10: BGE 143 V 418, 422 f. E. 4.1.2; BGE 142 V 342, 346 E. 5.1.

989 Im Gegensatz zur WHO beinhaltet der Schutz der Gesundheit nach Art. 118 Abs. 1 BV keine Förderung der Lebensqualität und des Wohlbefindens ohne einen Bezug zur Krankheitsverhütung und ist eher ein «Schutz vor Gesundheitsgefährdung», SGK BV-Tomas/Bernhard, Art. 118 N 10; im Ergebnis gleich, aber ohne Bezug zur WHO: BSK BV-Gächter/Renold-Burch, Art. 118 N 4, 6; a.A. BGer 2C-136/2024 vom 13.09.2024, E. 4.8.

990 SGK BV-Tomas/Bernhard, Art. 118 N 9, m.w.H.

253 Die Lehre zum Produktsicherheitsrecht in der Schweiz ist sich einig, dass mit den Schutzgütern «Sicherheit und Gesundheit der Verwender und Dritter» die körperliche Unversehrtheit bzw. Integrität dieser Personen gemeint ist.[991] Es handelt sich bei den Regeln des PrSG deshalb um Schutznormen.[992] Offensichtlich ist, dass das PrSG die physische Sicherheit und Gesundheit von Menschen schützt. Beispielhaft werden in der Literatur u.a. Verletzungen durch Schnitte, Stromschläge, Hitze, Chemikalien und Lärm genannt.[993] Auffallend ist, dass sich alle genannten Beispiele auf physische Einwirkungen beziehen.[994]

254 Unabhängig davon, ob auf den Schutz der körperlichen Integrität nach Zivil- oder Strafrecht abgestützt wird, ist auch die seelische Integrität[995] bzw. die geistige Gesundheit[996] von diesem Schutz erfasst. In der Schweiz wird zudem mehrheitlich davon ausgegangen, dass eine Genugtuung für immaterielle Unbill gestützt auf das PrHG geltend gemacht werden kann.[997] Wird davon ausgegangen, dass das PrHG dasselbe Sicherheitsniveau hat, bestätigen zum PrSG analoge Überlegungen zum Produkthaftpflichtrecht ebenfalls den Schutz der psychischen Unversehrtheit.[998]

255 Auch die GPSR schützt gem. Art. 5 i.V.m. Art. 3 Ziff. 2 GPSR die Gesundheit von Verbrauchern. Im Gegensatz zum PrSG und zur alten Produktsicherheitsrichtlinie definiert die GPSR den Begriff «Gesundheit» in ErwG 19 mit explizitem Hinweis auf die Definition der WHO.[999] Gem. ErwG 19 GPSR handelt es sich bei der «Gesundheit» um «einen Zustand des vollständigen körperlichen, geistigen und sozialen Wohlbefindens und nicht nur als das Nichtvorliegen von Krankheit oder Gebrechen». In der EU sind also ebenfalls die physische, psychische[1000] und so-

991 Wildhaber/Rey, Rn. 1496; Gerster, Rn. 22; Holliger-Hagmann, Fallstricke, S. 120; SHK PrSG-Hess, Art. 3 N 5; Bühler/Tobler, S. 371; Bühler, Bestandteil, S. 46, 172 f.

992 Wildhaber/Rey, Rn. 1496.

993 Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 26, mit einer ausführlichen Aufzählung weiterer Beispiele; siehe für zusätzliche Beispiele: Bühler/Tobler, S. 182; SHK PrSG-Hess, Art. 3 N 9.

994 S. u., Rn. 261.

995 Als einer der Schutzbereiche der Persönlichkeit nach Art. 28 ZGB, BSK ZGB I-Meili, Art. 28 N 17.

996 Bspw. im Rahmen von Art. 123 StGB, BSK StGB I-Andreas/Anne, Art. 123 N 4 f., mit Verweis auf BGE 134 IV 189, 192 E. 1.4.

997 Wildhaber/Rey, Rn. 1417; Damian, in: Praxishandbuch Produktregulierung, § 19 Rn. 2340; SHK PrHG-Hess, Art. 1 N 65.

998 S. o., Rn. 148.

999 Mit Kritik zu diesem Verweis siehe Mattheis, S. 106 f.

1000 Explizit ErwG 23 GPSR.

ziale Gesundheit geschützt.[1001] Als Beispiele für psychische Krankheiten werden Depressionen, niedriges Selbstwertgefühl und Schlaflosigkeit genannt.[1002] Die soziale Gesundheit umfasst «das Wohlsein in Gemeinschaftsgefügen».[1003]

WIEBE und SCHUCHT vertreten die Meinung, dass die Ausweitung des Schutzbereichs der GPSR auf die psychische und soziale Gesundheit zurückhaltend umgesetzt werden müsse.[1004] Entscheidend sei die «Produktunmittelbarkeit»: Nur Gefahren, die «unmittelbar vom Produkt als solchem» herrühren und welchen «mit konstruktiven oder instruktiven Mitteln begegnet werden» könne, sollen ihrer Meinung nach erfasst sein.[1005] Sie stellen fest, dass die Gefahrenquelle bei smarten Geräten nicht das Produkt selbst, sondern die zugehörige Software sei und dass eine Ausdehnung des Schutzbereichs auf die psychische und soziale Gesundheit den Zielen der GPSR und des traditionellen «Produktsicherheitsrechtskonzepts» entgegenstehe.[1006] Der Umfang des Risikos hänge vom individuellen Nutzer und von dessen Verhalten sowie seiner Veranlagung ab.[1007] Da der Hersteller keinen Einfluss auf die Verhaltensweise der Nutzer habe, könne ihm dafür keine Verantwortung für Risiken auferlegt werden, die sich nicht direkt auf das Produkt bezögen.[1008] Ausserdem seien Risiken für die psychische und soziale Gesundheit «kaum objektiv messbar oder bewertbar».[1009] Weiter fügen sie an, dass die Durchführung einer Risikoanalyse nach Art. 9 Abs. 2 GPSR für die genannten Risiken schwer vorstellbar sei[1010] und zudem die psychische Gesundheit nicht «in den verfügenden Teil der GPSR» aufgenommen worden sei.[1011] 256

Wie bereits oben beschrieben,[1012] ist es tatsächlich schwierig, den Kausalzusammenhang zwischen einem vermuteten gefährlichen Produkt und einer Gefahr für die psychische Gesundheit festzustellen, u.a. weil die Auswirkungen 257

1001 NHK GPSR-WIEBE, Art. 5 N 14 ff.; NP GPSR-SCHUCHT/WIEBE, § 4 N 14; dies war anscheinend noch unklar unter der Produktsicherheitsrichtlinie. Siehe dazu Europäische Kommission, Impact Assessment GPSR, S. 15.

1002 NHK GPSR-WIEBE, Art. 5 N 14.

1003 NHK GPSR-WIEBE, Art. 5 N 14.

1004 NHK GPSR-WIEBE, Art. 5 N 15; NP GPSR-SCHUCHT/WIEBE, § 4 N 14.

1005 NHK GPSR-WIEBE, Art. 5 N 16; NP GPSR-SCHUCHT/WIEBE, § 4 N 14.

1006 NHK GPSR-WIEBE, Art. 5 N 15; NP GPSR-SCHUCHT/WIEBE, § 4 N 14.

1007 Beide Male mit Verweis auf MATTHEIS, S. 105: NHK GPSR-WIEBE, Art. 5 N 15; NP GPSR-SCHUCHT/WIEBE, § 4 N 14.

1008 NHK GPSR-WIEBE, Art. 5 N 15; NP GPSR-SCHUCHT/WIEBE, § 4 N 14; MATTHEIS, S. 108.

1009 NHK GPSR-WIEBE, Art. 5 N 15.

1010 NHK GPSR-WIEBE, Art. 5 N 15; NP GPSR-SCHUCHT/WIEBE, § 4 N 14.

1011 NHK GPSR-WIEBE, Art. 5 N 15; NP GPSR-SCHUCHT/WIEBE, § 4 N 14.

1012 S. o. die Beispiele in Rn. 30 ff. und Diskussion in Rn. 32.

von der persönlichen Veranlagung der betroffenen Personen abhängen. Die Ursache der Gefahr ist bei Risiken für die psychische Gesundheit auch nach vorliegend vertretener Meinung wohl meistens Software. Software ist jedoch (entgegen WIEBES und SCHUCHTS Ansicht) ebenfalls als Produkt anzusehen. Zudem hält ErwG 23 GPSR explizit fest, dass das «Gesundheitsrisiko, das von digital vernetzten Produkten ausgeht, berücksichtigt werden [sollte], einschliesslich des Risikos für die psychische Gesundheit». Weiter kann in WIEBES und SCHUCHTS Argumentation nicht nachvollzogen werden, weshalb die Ausdehnung des Schutzbereichs den Zielen der GPSR und dem traditionellen Produktsicherheitsrecht entgegenstehen sollte. Das Ziel des hohen Verbraucherschutzniveaus wird mit der Erfassung der psychischen und sozialen Gesundheit sogar besser erfüllt. Die Funktionsweise des Binnenmarktes steht dem Schutz der psychischen und sozialen Gesundheit nicht stärker entgegen als dem Schutz der physischen Gesundheit. Es war bereits im traditionellen Produktsicherheitsrecht nach der Produktsicherheitsrichtlinie diskutabel, ob die psychische Gesundheit geschützt ist.[1013] Ebenfalls ist nicht ersichtlich, weshalb keine Risikoanalyse für Risiken der psychischen Gesundheit durchführbar sein sollten. Diese werden bspw. auch im Datenschutzrecht[1014] oder für Hochrisiko-KI-Systeme[1015] durchgeführt. Es stimmt zwar, dass die psychische und soziale Gesundheit nur in den ErwG der GPSR erwähnt wird, dasselbe gilt jedoch auch für die physische Gesundheit. Eine unterschiedliche Behandlung lässt sich aufgrund der Nichtaufnahme in den verfügenden Teil der GPSR deshalb ebenfalls nicht rechtfertigen.

258 Daraus folgt, dass zumindest die psychische Gesundheit gleich wie die physische Gesundheit zu behandeln ist. Richtig ist, dass die Gefahr immer dem Produkt inhärent sein muss[1016] und sich nicht aus der persönlichen Disposition der betroffenen Person ergeben darf. Ob der Hersteller den Risiken «mit konstruktiven oder instruktiven Mitteln» entgegenwirken kann, kann jedoch keine Rolle spielen. Hat der Hersteller ein Produkt mit einer Software unter seinem Namen auf den Markt gebracht und kann er die Software selbst nicht beein-

1013 Europäische Kommission, Impact Assessment GPSR, S. 14.

1014 Die sog. Datenschutzfolgeabschätzung nach dem Bundesgesetz über den Datenschutz (Datenschutzgesetz) vom 25. September 2020, SR 235.1 (zit. DSG), Art. 22; respektive in der EU nach Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 (zit. DSGVO), Art. 35.

1015 Art. 9 Abs. 2 lit. a KI-VO.

1016 Dies entspricht der «Produktunmittelbarkeit», NHK GPSR-WIEBE, Art. 5 N 16; NP GPSR-SCHUCHT/WIEBE, § 4 N 14.

flussen, weil er sie von einem anderen eingekauft hat, trägt er dennoch die Verantwortung als Quasihersteller für das in Verkehr gebrachte Produkt inklusive Software.[1017] Dies ändert indes nichts daran, dass es weiterhin schwierig sein wird, einen Kausalzusammenhang zwischen der Gefahr und der Beeinträchtigung der psychischen Gesundheit festzustellen und zu beweisen. Aus diesem Grund wird der Schutzbereich der GPSR auch nicht zu stark ausgeweitet, auch wenn die psychische Gesundheit in gleichem Masse wie die physische Gesundheit von der GPSR erfasst wird. Die Anerkennung der psychischen Gesundheit als Schutzgut im Produktsicherheitsrecht steht auch im Einklang mit der PLD 2024.[1018]

Trotz der Erwähnung von Umweltrisiken in ErwG 23, die ein Risiko für die Gesundheit und Sicherheit von Verbrauchern darstellen, dient die GPSR nicht dem Umweltschutz.[1019] Stattdessen sind nur «unmittelbar sicherheits- und gesundheitsrelevante produktbezogene Umweltrisiken» von der GPSR erfasst.[1020] Dasselbe gilt für den in ErwG 23 erwähnten Schutz der Privatsphäre von Kindern, der ebenfalls nur als geschütztes Rechtsgut nach Art. 5 GPSR erfasst ist, wenn ein Produkt unmittelbar die Gesundheit und Sicherheit eines Kindes gefährdet.[1021] 259

Art. 1 Abs. 1 KI-VO hält ebenfalls fest, dass die Gesundheit geschützt ist. Gemeint ist die «körperliche und psychische Unversehrtheit von Menschen» in Übereinstimmung mit der Auslegung des Gesundheitsbegriffs in Art. 114 Abs. 3 AEUV.[1022] Das bedeutet, dass auch KI-Systeme weder eine Gefahr für die physische noch für die psychische Gesundheit darstellen dürfen.[1023] 260

2. Sicherheit

Das allgemeine Sicherheitsgebot wird in Art. 3 Abs. 1 PrSG und Art. 5 GPSR festgehalten.[1024] Es besagt, dass nur sichere Produkte in Verkehr ge- 261

1017 Vorausgesetzt, er hat die Software nicht als vom anderen hergestellt ausgewiesen und ist als einziger Hersteller des Produktes ersichtlich. S. u., Rn. 279.

1018 Art. 6 Abs. 1 lit. a PLD 2024; siehe auch Beck KI-VO-Wendehorst, Art. 1 N 106.

1019 Siehe dazu ausführlich NHK GPSR-Wiebe, Art. 5 N 18.

1020 NHK GPSR-Wiebe, Art. 5 N 18.

1021 NHK GPSR-Wiebe, Art. 5 N 19.

1022 Beck KI-VO-Wendehorst, Art. 1 N 46; Beck KI-VO-Eisenberger, Art. 20 N 3, m.w.H.

1023 Siehe auch Europäische Kommission, Weissbuch KI, S. 18, welche bereits «explizite Verpflichtungen für Hersteller [...] in Bezug auf psychische Sicherheitsrisiken für Anwender in Erwägung [zog] z.B. bei Zusammenarbeit mit humanoiden Robotern».

1024 Siehe auch ErwG 47 KI-VO; für Niederspannungserzeugnisse siehe Art. 3 NEV.

bracht werden dürfen.[1025] Gem. Art. 3 Abs. 2 PrSG müssen Produkte den grundlegenden Sicherheits- und Gesundheitsanforderungen nach Art. 4 PrSG oder, wenn keine solchen Anforderungen festgelegt worden sind, dem Stand des Wissens[1026] und der Technik entsprechen.[1027] Die Anforderungen nach Art. 4 PrSG werden durch technische Normen konkretisiert.[1028] In der EU muss im Allgemeinen der Stand der Technik bei der Bewertung der Sicherheit berücksichtigt werden.[1029] Was im PrSG unter «Sicherheit» verstanden wird, wird weder im Gesetz noch in der Botschaft definiert.[1030] ERRASS sieht in der Sicherheit die «Abwesenheit von einem Schaden oder [...] vom Risiko, dass ein Schaden eintritt».[1031] BÜHLER zieht zur Definition von «Sicherheit» die Definition des «sicheren Produkts» der Produktsicherheitsrichtlinie bei.[1032] Dort wurde ein Produkt als «sicher» betrachtet, wenn die damit einhergehenden Gefahren «vertretbar» sind.[1033] In der GPSR wird Sicherheit zwar ebenfalls nicht definiert, dafür wird das sichere Produkt beschrieben. Ein sicheres Produkt ist gem. Art. 3 Ziff. 2 GPSR «jedes Produkt, das bei normaler oder vernünftigerweise vorhersehbarer Verwendung, was auch die tatsächliche Gebrauchsdauer einschliesst, keine oder nur geringe mit seiner Verwendung zu vereinbarende, als annehmbar erachtete und mit einem hohen Schutzniveau für die Gesundheit und Sicherheit der Verbraucher vereinbare Risiken birgt». Sind diese Voraussetzungen nicht erfüllt, gilt ein Produkt wiederum als «gefährlich».[1034] Die KI-VO definiert «Sicherheit» nicht. Gemeint ist jedoch ebenfalls im Einklang mit Art. 114 Abs. 3 AEUV «die technische Sicherheit im Zusammenhang mit Produkten».[1035] In der RAPEX-Leitlinie der EU wurden als klassische produktsicherheitsrechtliche Gefahren folgende aufgezählt: mechanische Gefahr, Erstickungsgefahr, Stromschlaggefahr, thermische Gefahr, chemische Gefahr, mikrobiologische Gefahr, Lärmgefahr, Gefahren durch Explosion, Implosion, Ultraschalldruck, Flüssigkeitsdruck oder Laserstrahlung.[1036] Daraus ergeben sich die Sicherheitsziele des allgemeinen

1025 Zum Risikoniveau s. u., Rn. 310.

1026 Zur Unterscheidung von «Wissen» und «Wissenschaft» und Technik siehe GERSTER, Rn. 192 ff.

1027 Siehe auch Botschaft PrSG, S. 7436, 7440; ausführlich BÜHLER, Bestandteil, S. 71 ff.

1028 Art. 6 Abs. 1 PrSG.

1029 NHK GPSR-WILRICH, Art. 3 N 43 ff.; NP GPSR-SCHUCHT/WIEBE, § 4 N 19; siehe auch zu Massnahmen nach der KI-VO ARIOLI, Jusletter IT 04.07.2024, Rn. 16.

1030 Siehe auch BÜHLER, Bestandteil, S. 43.

1031 ERRASS, S. 68, m.w.H.

1032 BÜHLER, Bestandteil, S. 44.

1033 Art. 2 lit. b Produktsicherheitsrichtlinie.

1034 Art. 3 Ziff. 3 GPSR; siehe auch NHK GPSR-WILRICH, Art. 3 N 36, 83.

1035 Beck KI-VO-EISENBERGER, Art. 20 N 3, m.w.H.

1036 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 55, S. 72 ff. mit Tabelle 2.

Produktsicherheitsrechts. In der Lehre werden verschiedene Ausprägungen aufgezählt. Es handelt sich dabei u.a. um «die funktionale Sicherheit, Standsicherheit, mechanische, physikalische, chemische und elektrische Sicherheit, Bruchsicherheit, Verschleissfestigkeit sowie Explosions- und Brandsicherheit».[1037] Art. 6 GPSR hält Aspekte für die Sicherheitsbewertung von Produkten fest. Aus Art. 6 Abs. 1 lit. b GPSR ergibt sich bspw., dass die Konnektivitätssicherheit, also Gefahren, die sich durch den Verlust der Verbindung von digital vernetzten Produkten ergeben, von der GPSR ebenfalls erfasst ist.[1038] Auch das Gefahrenpotenzial von anderen Produkten (wie z.B. von Software)[1039] auf das zu bewertende Produkt muss gem. Art. 6 Abs. 1 lit. c GPSR berücksichtigt werden. Des Weiteren sind Gefahren durch KI von der GPSR erfasst.[1040] Zudem erfasst die GPSR «sicherheitsrelevante Aspekte von Cyberrisiken».[1041]

Der Begriff «Gefahr»[1042] wird im PrSG ebenfalls nicht definiert, obwohl u.a. im Zusammenhang mit den Nachmarktpflichten mehrfach darauf abgestellt wird.[1043] Gem. Art. 3 Ziff. 3 GPSR ist ein gefährliches Produkt jedes Produkt, das kein sicheres Produkt ist. «Gefahr» wird jedoch in der GPSR ebenfalls nicht definiert. Die am 26. März 2025 ausser Kraft getretenen RAPEX-Leitlinien definierten die Produktgefahr folgendermassen: «Eine Gefahr ist das dem Produkt innewohnende Potenzial, eine Verletzung des Verbrauchers, der das Produkt verwendet, zu verursachen».[1044] Die Definition war ungünstig gewählt, da nicht nur der Verbraucher, der das Produkt verwendet, sondern auch unbeteiligte Dritte (und je nach Sektorrecht weitere Schutzobjekte) durch das Produktsicherheitsrecht geschützt werden.[1045] Auch das «Risiko» wird im PrSG nicht definiert. In der EU wird unter Risiko gem. Art. 3 Ziff. 4 GPSR «das Ver- 262

1037 NHK GPSR-Wiebe, Art. 5 N 31; NP GPSR-Schucht/Wiebe, § 4 N 21; zum PrSG siehe auch Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 26, welche die Beispiele der RAPEX-Leitlinie übernommen hat.

1038 ErwG 23 f. GPSR; Europäische Kommission, Blue Guide, S. 18.

1039 Siehe auch NHK GPSR-Wiebe, Art. 6 N 20, mit Ausführungen zu smarten Produkten.

1040 Art. 6 Abs. 1 lit. h GPSR; NP GPSR-Schucht/Wiebe, § 9 N 19.

1041 Europäische Kommission, Blue Guide, S. 18; Art. 6 Abs. 1 lit. g GPSR; NP GPSR-Schucht/Wiebe, § 9 N 19.

1042 Für eine normative Bedeutung siehe Seiler, S. 153: «Der Gefahrenbegriff [...] umschreibt einen unzulässigen, abzuwehrenden Zustand, im Gegensatz zu einem Normalzustand, welcher als zulässig gilt, auch wenn er nicht im technischen Sinne gefahrlos ist», m.w.H.

1043 U.a. in Art. 8 Abs. 2 lit. a und Art. 8 Abs. 5 PrSG.

1044 Europäische Kommission, RAPEX-Leitlinie, S. 164; ebenso Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 55; ebenfalls die RAPEX-Leitlinie zitierend Bühler, Bestandteil, S. 53.

1045 Dies galt bereits für die Produktsicherheitsrichtlinie und gilt weiterhin für die GPSR und das PrSG, s. o., Rn. 246.

hältnis zwischen der Eintrittswahrscheinlichkeit einer Gefahr, die einen Schaden verursacht, und der Schwere des Schadens» verstanden. Es handelt sich beim Risiko also um das Resultat einer Sicherheits- oder Risikobewertung.[1046] Fällt diese Bewertung so hoch aus, dass es sich um ein «nicht mehr erlaubtes Risiko» handelt, wird auch von «Gefahr» gesprochen.[1047] Eine geringfügige Gefährdung von Sicherheit und Gesundheit im Rahmen eines vertretbaren Restrisikos[1048] ist in der Schweiz und der EU erlaubt, da absolute Sicherheit unmöglich[1049] und auch nicht gefordert ist.[1050]

2.1. Problem der vernünftigen Vorhersehbarkeit

263 Das PrSG sowie die GPSR halten fest, dass Produkte bei einer normalen oder vernünftigerweise vorhersehbaren Verwendung ungefährlich bzw. sicher sein müssen.[1051] Gemeint sind damit zum einen Verwendungen, die teils vom Hersteller beeinflusst werden können, indem er den Zweck des Produktes bestimmt (engl. «intended use»).[1052] Damit ist die Produktwidmung gemeint, die der Hersteller bspw. durch die Funktion, Eigenschaft, Bauart und Bauweise des Produktes sowie die zugehörigen Unterlagen und Kommunikation (z.B. in Form von Werbung) ausdrückt.[1053] Zum anderen sind aber auch Verwendungen gemeint, die nicht vom Hersteller beeinflussbar sind, wenn diese «üblich» sind.[1054] Es handelt sich um den Gebrauch durch Konsumenten, mit dem «nach vernünftigem Ermessen gerechnet werden muss».[1055] Auch das Verhalten und allfällige Beeinträchtigungen von vulnerablen Personengruppen müssen einkalkuliert werden.[1056] Wird das Produkt «fehlerhaft» verwendet, wobei der Hersteller diese Fehlerhaftigkeit hätte voraussehen müssen (engl. «misuse»),

1046 S. u., Rn. 311 ff.

1047 Bühler/Tobler, S. 125, mit Verweis auf Seiler, S. 38 ff., 153 ff.

1048 Auch «erlaubtes Risiko» Seiler, S. 44 f.

1049 NHK GPSR-Wiebe, Art. 5 N 29; Wagner, Paukenschlag, S. 5; Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 27; Bühler/Tobler, S. 123.

1050 Bezogen auf das PrSG: BGE 143 II 518, 532 E. 5.7; BGer 2C_905/2010 vom 22.03.2011, E. 3.2.1, zwar ohne PrSG-Bezug, aber zur technischen Sicherheit; Botschaft PrSG, S. 7436; statt vieler Bühler, Bestandteil, S. 47; bezogen auf die GPSR: ErwG 22 GPSR; NHK GPSR-Wilrich, Art. 3 N 40; NHK GPSR-Wiebe, Art. 5 N 29; bezogen auf die KI-VO Beck KI-VO-Braun Binder/Egli, Art. 9 N 33.

1051 Art. 3 Abs. 1 und Art. 8 Abs. 2 lit. a PrSG; Art. 3 Ziff. 2 GPSR.

1052 NHK GPSR-Wiebe, Art. 5 N 21; NHK GPSR-Wilrich, Art. 3 N 58.

1053 NHK GPSR-Wiebe, Art. 5 N 22, m.w.H.

1054 NHK GPSR-Wilrich, Art. 3 N 58.

1055 NHK GPSR-Wiebe, Art. 5 N 23; ausführlich NHK GPSR-Wilrich, Art. 3 N 66 ff., m.w.H.

1056 Botschaft PrSG, S. 7436, mit Beispielen; Art. 6 Abs. 1 lit. e GPSR.

ist er deshalb für die Sicherheit des Produktes verantwortlich.[1057] Wird das Produkt jedoch «missbraucht» (engl. «abuse»)[1058], ist der Hersteller nicht für die Sicherheit des Produktes im Rahmen der missbräuchlichen Anwendung verantwortlich.[1059] Bei der Abgrenzung zwischen einer fehlerhaften und einer missbräuchlichen Verwendung wird also auf eine «vernünftige Vorhersehbarkeit» abgestellt. Diese Abgrenzung ist wichtig, da der Hersteller nach dem PrSG und der GPSR bzw. der Anbieter nach der KI-VO nur bei einer normalen oder vernünftigerweise vorhersehbaren Verwendung für die Sicherheit seiner Produkte verantwortlich ist.[1060] Hersteller haben im Rahmen des PrSG, der GPSR und der KI-VO deshalb auch nur Nachmarktpflichten im Rahmen einer fehlerhaften und nicht einer missbräuchlichen Anwendung wahrzunehmen.[1061] Dasselbe muss für Smart Home Devices gelten, wenn sie unter die NEV und die FAV fallen.

Die «vernünftige Vorhersehbarkeit» stellt in Bezug auf die Nachmarktpflichten für Hersteller mehrere Probleme dar. Die «vernünftige Vorhersehbarkeit» ist ein unbestimmter Rechtsbegriff[1062] und die Bestimmung der Grenze liegt damit im richterlichen Ermessen.[1063] Das Abstellen auf die «vernünftige Vorhersehbarkeit» kann problematisch sein, da sie einem «hindsight bias» unterliegen kann. Durch diese kognitive Verzerrung wirkt das Eintreten eines Geschehens im Nachhinein wahrscheinlicher, als vorab angenommen wurde.[1064] Gerster führt aus, dass bei schon eingetretenen Schäden die Wahrscheinlichkeit eines Schadenseintritts oft höher eingeschätzt wird, als sie tatsächlich ist.[1065] Aufgrund des «hindsight bias» 264

1057 BGE 143 II 518, 542 f. E. 8.3.1. Der vorhersehbare Fehlgebrauch wird gleich ausgelegt wie der «Gebrauch, mit dem vernünftigerweise gerechnet werden kann» gem. Art. 4 Abs. 1 lit. b PrHG. Statt vieler Gerster, Rn. 146, m.w.H. insbesondere BGE 133 III 81, 85 E. 3.1; BVGer C-4660/2013 vom 28.05.2015, E. 3.6; für die GPSR NHK GPSR-Wiebe, Art. 5 N 23.

1058 Zu den Begriffen «intended use», «misuse» und «abuse» siehe auch Piovano/Schucht/Wiebe, S. 125.

1059 BGE 133 III 81, 85 E. 3.1; Botschaft PrSG, S. 7436, welche die Grenze bei der groben Fahrlässigkeit der Benutzer und beim nicht vorhersehbaren, völlig abwegigen Produktgebrauch zieht; statt vieler siehe auch Gerster, Rn. 146, m.w.H.; zur GPSR NHK GPSR-Wiebe, Art. 5 N 24, welcher den Produktmissbrauch als «absichtliche Zweckentfremdung» definiert. Dazu gehört z.B. auch «die Nutzung entgegen den Warnhinweisen», m.w.H.; zur KI-VO: Beck KI-VO-Braun Binder/Egli, Art. 9 N 26; Arioli, Jusletter IT 04.07.2024, Rn. 24.

1060 Im Gegensatz zum STEG, gem. welchem der Schutz nur für die bestimmungsgemässe und sorgfältige Verwendung galt, Botschaft PrSG, S. 7428.

1061 S. u., Rn. 308.

1062 NHK GPSR-Wiebe, Art. 5 N 23; siehe auch Bühler/Tobler, S. 121.

1063 SHK PrSG-Hess, Art. 3 N 20; siehe auch Gerster, Rn. 150.

1064 Gerster, Rn. 150 f., mit ausführlicher Besprechung der Problematik des «hindsight bias» bzw. «Rückschaufehlers» in Bezug zum Fehlgebrauch und zum Missbrauch, m.w.H.

1065 Gerster, Rn. 150.

kann ein eigentlich nicht vorhersehbares Schädigungspotenzial im Nachhinein als «selbstverständlich» beurteilt werden. Dies erschwert dem Hersteller die Einschätzung seiner Produkte, insbesondere bei Software und relativ neuen Technologien wie KI, wo noch nicht klar ist, wie sie künftig eingesetzt werden. So ist bspw. die Verwendung mit einem anderen Produkt und die damit verbundene Einwirkung auf dieses Produkt[1066] bei Software und KI schwierig vorherzusehen.[1067] Da Smart Home Devices durch kabellose Verbindungen miteinander oder mit externen Plattformen verbunden sind, kann es bspw. auch zu Einwirkungen untereinander kommen, wenn die Produkte sich nicht physisch berühren.[1068] Die Gebrauchsdauer – mindestens wenn sie nicht angegeben wurde – muss ebenfalls «vernünftigerweise vorhersehbar» sein.[1069] Diese ist bei KI besonders schwer vorauszusehen, da Trainingsdaten jeweils nur einen momentanen Zustand abbilden und abgeschätzt werden muss, wie lange ein trainiertes System eingesetzt werden kann. In der Softwareentwicklung werden besonders schnell und häufig Fortschritte gemacht, so dass ältere Systeme rasch nicht mehr «State of the Art» sind und bspw. wiederum unvorhersehbar auf andere Systeme oder auf die beherbergenden Produkte einwirken und zu Gefahren führen können. Weiter wird auch bei der Gefahrenerkennung auf die normale oder vernünftigerweise vorhersehbare Verwendung abgestellt.[1070] In diesem Zusammenhang ist zu beachten, dass die alleinige Tatsache, dass ein höheres Sicherheitsniveau erreichbar wäre oder alternative Produkte mit geringeren Risiken verfügbar sind, weder in der Schweiz[1071] noch in der EU[1072] die Einstufung eines Produktes als «gefährlich» rechtfertigt. Da der Hersteller nur bei Konsumentenprodukten zu Nachmarktpflichten nach dem PrSG und der GPSR verpflichtet ist, muss dieser zudem die Benutzung durch Konsumenten «voraussehen» können. Er muss bedenken, dass ein ursprünglich gewerblich genutztes Produkt bspw. «schleichend» zu einem Dual-Use- und damit via Produktmigration auch zu einem Konsumentenprodukt werden kann.

1066 Die gem. Art. 3 Abs. 3 lit. b PrSG zu berücksichtigen ist und gem. ErwG 24 GPSR die Sicherheit nicht beeinträchtigen darf; zur Wechselwirkung siehe auch SHK PrSG-Hess, Art. 3 N 37.

1067 S. o., Rn. 47 f.

1068 S. o., Rn. 80.

1069 S. u., Rn. 396.

1070 S. u., Rn. 325.

1071 Art. 3 Abs. 5 PrSG.

1072 Art. 6 Abs. 2 GPSR.

2.2. Exkurs: Security als Bestandteil der Produktsicherheit

Der in der Produktsicherheit verwendete Begriff der Sicherheit entspricht dem englischen Begriff «safety».[1073] «Product safety» hat das Ziel, natürliche Personen und – je nach Sektorrecht – zusätzliche Schutzobjekte zu schützen.[1074] Im Gegensatz dazu wird unter dem englischen Begriff «security» die Erschwerung oder Verunmöglichung einer schädlichen oder manipulativen Einwirkung durch Dritte verstanden.[1075] Der Begriff «security» wird deshalb zumeist als Sicherheitsbegriff in der Informatik genutzt.[1076] Ein Produkt muss im Sinne von «safety» sicher sein und darf die Sicherheit der geschützten Rechtsgüter nicht beeinträchtigen.[1077] Demgegenüber kann die «security» eines Produktes kompromittiert sein, weil bspw. ein Unberechtigter die Kontrolle über das System übernommen hat.[1078] Durch die Kompromittierung der «security» kann das Produkt in seiner «safety» beeinträchtigt werden[1079] und bspw. Personen schädigen.[1080] Konsumenten haben i.d.R. nur eingeschränkte Möglichkeiten, Einfluss auf die «security» zu nehmen.[1081] IT-Sicherheit («security») ist deshalb ein Bestandteil der Produktsicherheit («safety»).[1082] Dem wird in Art. 6 Abs. 1 lit. g GPSR Rechnung getragen, indem die Cybersicherheit als Aspekt für die Bewertung der Sicherheit von Produkten aufgelistet wird. Die

265

1073 So bspw. die General Product *Safety* Regulation: GPSR und das General Product *Safety* Directive: Produktsicherheitsrichtlinie. Für das PrSG und die PrSV gibt es keine offizielle englische Übersetzung; siehe auch: NHK GPSR-Wiebe, Art. 5 N 32; Feiler/Forgó, Art. 3 N 74.

1074 NHK GPSR-Wiebe, Art. 5 N 32.

1075 Piovano/Schucht/Wiebe, S. 89; Errass, S. 69; ähnlich auch McGuire, in: Foerste/Westphalen, § 58 Rn. 39.

1076 Siehe zur Unterscheidung von «safety» und «security» Wittig, S. 31 und zur Abgrenzung der IT-Sicherheit von der Produktsicherheit S. 34; siehe auch Wiebe, Pflichten, S. 66; ebenfalls «Sicherheit» mit «security» übersetzend die CRA; für die Schweiz siehe auch die englische Übersetzung von Art. 3 lit. a CyRV, Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung) vom 27. Mai 2020, ausser Kraft, SR 120.73 (zit. CyRV). Dort wurde «Cybersicherheit» mit «cyber security» übersetzt; anders bspw. BGer 2C_488/2012 vom 01.04.2013, E. 7.5, wo es bei «security» um die Flughafensicherheit geht.

1077 Ähnlich NHK GPSR-Wiebe, Art. 5 N 32, welcher jedoch nur den Schutz von Personen nennt.

1078 S. o., Rn. 41.

1079 NP GPSR-Schucht/Wiebe, § 4 N 22; dies muss auch gem. ErwG 26 GPSR beachtet werden.

1080 Piovano/Schucht/Wiebe, S. 90; Reusch, Mobile Updates, S. 904 f.; siehe auch den Hinweis in EKK, Empfehlung, S. 2.

1081 Piovano/Schucht/Wiebe, S. 90; Reusch, Mobile Updates, S. 905.

1082 Siehe dazu ausführlich Wiebe, Pflichten, S. 67; ebenso Piovano/Schucht/Wiebe, S. 89; a.A. Hartmann/Klindt, S. 73 f., m.w.H.

GPSR bezweckt somit sowohl «product safety» als auch «product security».[1083] Im PrSG sind keine Hinweise auf «security», «IT-Sicherheit» oder «Cybersicherheit» zu finden. Dennoch muss auch im PrSG die IT-Sicherheit als Bestandteil der Produktsicherheit angesehen werden.

3. Nur KI-VO: Grundrechte

266 Art. 1 Abs. 1 KI-VO hält fest, dass «ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte, einschliesslich Demokratie, Rechtsstaatlichkeit und Umweltschutz» gewährleistet werden soll.[1084] Neben den klassischen Rechtsgütern des Produktsicherheitsrechts (also der Sicherheit und der Gesundheit von Personen, die auch in der GPSR geschützt werden), bezweckt die KI-VO explizit den Grundrechtsschutz.[1085] Dies ist für einen dem NLF zugehörigen Rechtsakt ungewöhnlich.[1086] Aus dem zusätzlichen Schutz folgt, dass sich «die Sicherheitsverständnisse zwischen KI-VO und Produktsicherheitsrecht je nach Kontext» unterscheiden können.[1087] Der Schutzzweck der KI-VO ist weiter als jener des allgemeinen Produktsicherheitsrechts.[1088] So umfassen bspw. die Nachmarktpflichten in Art. 20 Abs. 2 i.V.m. Art. 79 Abs. 1[1089] und Art. 9 Abs. 2 lit. a[1090] KI-VO als Schutzgüter zusätzlich zur Gesundheit und Sicherheit auch die Grundrechte. Zu beachten ist, dass der Schutz von Grundrechten in Bezug auf Sicherheitsbauteile entfällt.[1091]

III. Fazit

267 Geschütztes Rechtsgut im allgemeinen Produktsicherheitsrecht in der Schweiz und der EU sind die Sicherheit und die Gesundheit von natürlichen Personen. Es sollen Individuen und nicht «nur» die Allgemeinheit geschützt

1083 Ausführlich NHK GPSR-Wiebe, Art. 5 N 32, m.w.H.; NP GPSR-Schucht/Wiebe, § 4 N 22; wobei die «product security» nun primär in der CRA geregelt ist. Siehe Art. 1, ErwG 1 CRA.

1084 Siehe auch ErwG 2 KI-VO.

1085 Art. 1 Abs. 1 KI-VO; Beck KI-VO-Ruschemeier, Art. 6 N 35; zum Grundrechtsschutz der KI-VO ausführlich Feiler/Forgó, Art. 1 N 7 ff.; siehe dazu ebenfalls BJ, Rechtliche Basisanalyse KI, S. 90.

1086 Voigt/Hullen, S. 2.

1087 Beck KI-VO-Ruschemeier, Art. 6 N 35.

1088 Beck KI-VO-Ruschemeier, Art. 6 N 19.

1089 Beck KI-VO-Eisenberger, Art. 20 N 3.

1090 Beck KI-VO-Braun Binder/Egli, Art. 9 N 16.

1091 Art. 3 Ziff. 14 KI-VO; siehe auch Beck KI-VO-Ruschemeier, Art. 6 N 42 Fn. 38.

werden.[1092] Produkte müssen somit für jeden Einzelnen sicher sein, auch für vulnerable Personen, wenn diese zur Zielgruppe des Produktes gehören. Das Produktsicherheitsrecht soll vor Personenschäden schützen bzw. diese präventiv verhindern.[1093] Tiere, Sachen, Vermögen und Grundrechte sind vom allgemeinen Produktsicherheitsrecht weder in der Schweiz noch in der EU erfasst, deren Gesundheit oder Sicherheit können jedoch durch einzelne sektorielle Erlasse wie z.B. die NEV, die FAV oder die KI-VO geschützt sein.

Die vom allgemeinen Produktsicherheitsrecht geschützten Rechtsgüter sind in der Schweiz und in der EU die Gesundheit und Sicherheit von Menschen. Konkret sollen Personenschäden durch unsichere Produkte (inklusive Software und damit auch KI-Systeme) verhindert werden. Unter «Gesundheit» werden die physische und die psychische Gesundheit verstanden. In Europa geht der Gesundheitsbegriff jedoch weiter als in der Schweiz. Es könnte deshalb zu unterschiedlichen Massstäben kommen, wenn es um die Analyse von Beeinträchtigungen der Gesundheit kommt. Im allgemeinen Produktsicherheitsrecht sind viele Ausprägungen von «Sicherheit» erfasst. Neben etablierten Sicherheitszielen wie der elektrischen oder mechanischen Sicherheit ist auch die Sicherheit mit Bezug auf die Konnektivität von Produkten und auf KI vom Begriff «Sicherheit» abgedeckt. Produkte sind unsicher, wenn sie in einem nicht mehr tolerierbaren Rahmen gefährlich sind. Diese Beurteilung ist Teil einer Risikobewertung. Absolute Sicherheit ist weder möglich noch gefordert. Der Hersteller ist nicht für die Sicherheit seines Produktes verantwortlich, wenn dieses missbräuchlich verwendet wird. Massgeblich für die Abgrenzung zwischen fehlerhafter und missbräuchlicher Verwendung eines Produktes ist, ob die Verwendung vernünftigerweise vorhersehbar war. Die vernünftige Vorhersehbarkeit kann einem «hindsight bias» unterliegen, was vor allem für neue Technologien wie Smart Home Devices mit Software und insbesondere KI zu strikten Einschätzungen der Vorhersehbarkeit führen könnte. Insbesondere in Bezug auf Nachmarktpflichten ist die vernünftige Vorhersehbarkeit in verschiedenen Bereichen problematisch. Betroffen sind die Wechselwirkung mit anderen Produkten, die Gebrauchsdauer insbesondere bei mit Trainingsdaten «angelernten» KI-Systemen, die Gefahrenerkennung und die Produktmigration. Als «Ausreisser» im Produktsicherheitsrecht schützt die KI-VO auch Grundrechte. 268

1092 SHK PrSG-Hess, Art. 3 N 77.
1093 Gerster, Rn. 423.

C. Hersteller und Anbieter als in der Pflicht stehende Subjekte

269 Art. 8 PrSG nimmt explizit Hersteller, Importeure, Händler und «andere Inverkehrbringer» in die Pflicht. Somit sind jene Parteien in der Verantwortung, die Gewinne aus ihren Tätigkeiten schöpfen können.[1094] Da Hersteller den grössten Einfluss auf Produkte haben,[1095] wird vorliegend auf ihre Pflichten eingegangen. Der Hersteller ist auch der «zentrale Adressat»[1096] der GPSR.[1097] In der KI-VO ist der Hersteller nicht definiert.[1098] Der wichtigste Akteur in der KI-VO – und der dem Hersteller in anderen produktsicherheitsrechtlichen Erlassen gleichzusetzende[1099] Verpflichtete – ist der Anbieter (vor allem in der Praxis wird auch der engl. Begriff «provider» genutzt). Grundsätzlich folgen das europäische und das schweizerische Produktsicherheitsrecht dem Konzept der Selbstverantwortung.[1100] Somit setzen auch die Hersteller ihre Nachmarktpflichten in erster Linie selbstverantwortlich um. Der Staat schreitet erst ein, wenn er eine Gefahr vermutet.[1101]

270 Zu klären, wer alles als Hersteller im Sinne des Produktsicherheitsrechts gilt, ist essenziell, weil dieser in erster Linie verpflichtet ist, die Produktsicherheit zu gewährleisten[1102] und damit auch Nachmarktpflichten wahrzunehmen. Der Hersteller ist i.d.R. der Einzige, der das Gefahrenpotenzial seines Produktes richtig einschätzen kann.[1103] Sind sich die Wirtschaftsteilnehmer nicht im Klaren, wer als Hersteller die entsprechenden Verantwortungen trägt, führt dies zu einer ungenügenden Erfüllung der verlangten Pflichten[1104] und damit zu einem steigenden Risiko von gefährlichen Produkten auf dem Markt.

1094 Wey, in: Fellmann/Furrer, Schonzeit, S. 33.

1095 Bezüglich KI-Systeme siehe bspw. Piovano, Hersteller, S. 1; Fellmann, in: Fellmann S. 124; Wildhaber, Einführung, S. 37 f., zusätzlich mit Ausführungen über die «Zuordnung in die Risikosphäre des KI-Betreibers».

1096 NHK GPSR-Wilrich, Art. 3 N 133.

1097 Art. 3 Ziff. 8 GPSR.

1098 Siehe bspw. auch Voigt/Hullen, S. 16.

1099 S. u., Rn. 273.

1100 S. o., Rn. 65.

1101 Gerster, Rn. 129.

1102 NHK GPSR-Wiebe, Art. 5 N 37.

1103 Botschaft PrSG, S. 7442; je nachdem kann auch der Importeur das Gefahrenpotenzial gut einschätzen bzw. sollte er dies können. Er hat jedoch weniger weitgehende Pflichten, siehe dazu Gerster, Rn. 274, m.w.H.

1104 Piovano, Rechtsfragen, S. 6, m.w.H.

I. Keine Pflichten für KI selbst

In Zusammenhang mit komplexer KI, die «eigene» Entscheidungen mit Auswirkungen auf ihre Umwelt trifft[1105] oder «menschliche Züge»[1106] hat, wird seit einiger Zeit die Frage gestellt, ob diesen Systemen selbst Rechtspersönlichkeit zukommen sollte. Da ein KI-System weder eine natürliche noch eine juristische Person ist, könnte eine «E-Personhood» eine eigene Rechtspersönlichkeit mit Rechten und Pflichten inklusive Haftungssubstrat für solche Systeme schaffen.[1107] In der Schweiz wurde die in einem Postulat geforderte Prüfung zur Schaffung von Rechtspersönlichkeit für «Roboter mit künstlicher Intelligenz» 2018 vom Nationalrat abgelehnt.[1108] Ein KI-System ist nach heutigem Recht kein Subjekt, welchem Pflichten auferlegt werden können, da ihm keine Rechtspersönlichkeit zukommt.[1109] 271

II. Keine Pflichten bei nichtgewerblicher Tätigkeit

Privatpersonen, die Produkte nichtgewerblich[1110] in Verkehr bringen, sind keine Adressaten des PrSG und deshalb auch nicht zur Erfüllung von Nachmarktpflichten gem. Art. 8 PrSG verpflichtet. Die Botschaft schliesst Private explizit aus und betont, dass es nicht sinnvoll sei, ihnen produktsicherheitsrechtliche Vorschriften aufzuerlegen, und dass Kontrollen in der Praxis gar nicht umsetzbar wären.[1111] So muss sich auch der Teilsatz in Art. 8 Abs. 2 PrSG «im Rahmen seiner Geschäftstätigkeit» darauf beziehen, dass der Hersteller gewerblich handelt.[1112] Ebenso gilt die GPSR nur, wenn die Bereitstellung von Produkten auf dem Markt «im Rahmen einer Geschäftstätigkeit» erfolgt.[1113] 272

1105 Beck, S. 188.

1106 Systeme haben zum heutigen Stand kein Bewusstsein, Hildt, S. 2; siehe auch: Batache, Rn. 30; Spindler, Roboter, S. 767 Fn. 16.

1107 Wagner, Paukenschlag, S. 2; Braun Binder et al., Jusletter 28.06.2021, Rn. 50, m.w.H.; Lohmann, Roboter, S. 162; Beck, S. 189 f.; für eine Übersicht siehe auch Borio, S. 225 Fn. 26.

1108 Postulat 17.3040 vom 01.03.2017, Reynard/Nationalrat, Die Schaffung einer Rechtspersönlichkeit für Roboter prüfen, hier in Bezug auf Roboter; Der Bundesrat verweist in seiner Antwort u.a. auf die Interpellation 15.3446 vom 06.05.2015, Markwalder/Nationalrat, Neue Technologien und autonome Apparate. Rechtliche Rahmenbedingungen für die Haftung.

1109 Ebenso in der EU Wagner, Verantwortlichkeit, S. 739.

1110 Zur gewerblichen Inverkehrbringung s. u., Rn. 300 f.

1111 Botschaft PrSG, S. 7432; so auch Bühler, Bestandteil, S. 63.

1112 SHK PrSG-Hess, Art. 8 N 12; a.A.: Gerster, Rn. 275, insbesondere Fn. 438; Holliger-Hagmann, Fallstricke, S. 159.

1113 Art. 3 Ziff. 6 GPSR; NHK GPSR-Wilrich, Art. 3 N 124; siehe auch NHK GPSR-Wilrich, Art. 2 N 10 ff., m.w.H.

Dasselbe gilt für den Anbieter nach Art. 3 Ziff. 3 KI-VO.[1114] Das heisst, dass auch unter der GPSR und der KI-VO keine Pflicht zur Erfüllung von Nachmarktpflichten für Privatpersonen besteht.

III. Hersteller und Anbieter als primäre Verpflichtete

273 Der Begriff des Herstellers ist durch die Regulierung zur Produktsicherheit und zur Produkthaftung und bspw. auch durch die VO (EU) 2019/1020 über Marktüberwachung und Konformität von Produkten längst etabliert.[1115] Trotzdem verwendet die KI-VO den Begriff «Anbieter» (engl. «provider») statt jenen des «Herstellers» (engl. «manufacturer»).[1116] Weshalb, ist unklar.[1117] Es handelt sich jedoch beim Anbieter und beim Hersteller ebenfalls um jene Personen, die grundsätzlich am meisten Einfluss auf ihre KI-Systeme haben.[1118] Wird vorliegend vom Hersteller gesprochen, ist der Anbieter grundsätzlich mitgemeint, da die Begriffe in Bezug auf KI-Systeme und im Zusammenhang mit der KI-VO synonym verwendet werden. Auch die PLD hält fest, dass Anbieter von KI-Systemen (zumindest i.S.d. PLD) als Hersteller betrachtet werden.[1119] In Bezug auf Produkte, die keine KI-Systeme nach der KI-VO sind, sollte jedoch ausschliesslich der Begriff des «Herstellers» verwendet werden.[1120] Hersteller und Anbieter können in der KI-VO u.U. auch dieselbe Person sein.[1121]

274 Der Begriff «Anbieter» wird in der GPSR ebenfalls genutzt, bezeichnet gem. Art. 3 Ziff. 14 GPSR jedoch immer den «Anbieter eines Online-Marktplatzes». Auch Anbieter eines Online-Marktplatzes können z.B. als Hersteller verpflichtet werden, wenn sie eigene Markenprodukte (oder White-Label-Produkte

1114 Beck KI-VO-Wendehorst, Art. 3 N 69.
1115 Beck KI-VO-Wendehorst, Art. 3 N 64.
1116 Beck KI-VO-Wendehorst, Art. 3 N 64, welche zudem in N 71 festhält, dass sich die Begriffe im Wesentlichen entsprechen, und für eine gegebenenfalls nötige Auslegung empfiehlt, «mit aller Vorsicht» auf den Herstellerbegriff zurückzugreifen; siehe auch Voigt/Hullen, S. 2.
1117 Siehe auch Wagner, Rauch, S. 127, mit Diskussion zu den Richtlinienentwürfen zur Produkthaftung und zur KI-Haftung.
1118 S. u. die Ausnahme, wenn ein Anbieter ein KI-System unter seinem Namen in Verkehr bringt oder in Betrieb nimmt, aber nicht der ist, der es entwickelt hat, Rn. 279.
1119 ErwG 13 PLD 2024; noch zum Vorschlag siehe auch Wagner, Paukenschlag, S. 3.
1120 Siehe auch Borges, Teil 1, Rn. 76.
1121 S. u., Rn. 285.

unter eigener Marke als Quasihersteller[1122]) verkaufen.[1123] Ein Anbieter eines Online-Marktplatzes ist ein Anbieter eines Vermittlungsdienstes, der eine Online-Schnittstelle bereitstellt, die es Verbrauchern ermöglicht, mit Unternehmern Fernabsatzverträge über den Verkauf von Produkten abzuschliessen.[1124] Der Anbieter in der GPSR hat also eine abweichende Bedeutung vom Anbieter in der KI-VO.

Vorliegend werden Hersteller – in Anlehnung an GERSTER und BÜHLER – in zwei Kategorien eingeteilt: Hersteller i.e.S., die tatsächlich neue Produkte erschaffen, und Hersteller i.w.S., die dies nicht tun.[1125] Im PrSG, in der GPSR und der KI-VO kann jede natürliche oder juristische Person Hersteller sein.[1126] 275

1. Hersteller i.e.S. bzw. tatsächlicher Hersteller

Das PrSG enthält selbst keine Definition des Begriffs des Herstellers. Gem. der Botschaft zum PrSG ist Hersteller, «wer die Verantwortung für die Konzeption und Herstellung inklusive der Ausstattung des Produkts trägt».[1127] Der Begriff des Herstellers im PrSG beruht auf den Definitionen von Art. 2 lit. e Produktsicherheitsrichtlinie und auf dem PrHG.[1128] Der Hersteller i.e.S. nach Art. 2 Abs. 4 PrSG entspricht dem Hersteller nach Art. 2 Abs. 1 lit. a PrHG.[1129] Er ist der tatsächliche Erschaffer neuer Produkte.[1130] Er ist verantwortlich für die Konzeption und die eigentliche Herstellung sowie die Ausstattung.[1131] Der Hersteller i.e.S. ist i.d.R. jene Person, die das Produkt am besten kennt und deshalb auch die Sicherheitseigenschaften am besten beurteilen kann.[1132] Als Hersteller gilt gem. Art. 3 Ziff. 8 GPSR, wer Produkte herstellt, entwirft, herstellen 276

1122 S. u., Rn. 279.

1123 ErwG 46 GPSR.

1124 Art. 3 Ziff. 14 GPSR für weitere Definitionen der «Online-Schnittstelle» und des «Fernabsatzvertrages» siehe Ziff. 15 und 16 m.w.H. sowie Art. 4 GPSR.

1125 GERSTER, Rn. 93 ff., 99 ff.; BÜHLER, Bestandteil, S. 64.

1126 Zum PrSG siehe Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 25; SHK PrSG-HESS, Art. 2 N 40; für die GPSR NHK GPSR-WILRICH, Art. 3 N 135; Art. 3 Ziff. 3 KI-VO, wobei bei KI-Systemen auch Behörden, Einrichtungen oder sonstige Stellen in Frage kommen.

1127 Botschaft PrSG, S. 7432; siehe auch Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 24.

1128 SHK PrSG-HESS, Art. 2 N 39; siehe auch FORNAGE, in: Chappuis/Winiger/Campi S. 212, welche sich für eine übereinstimmende Herstellerdefinition im PrSG und im PrHG ausspricht.

1129 GERSTER, Rn. 380; BÜHLER, Bestandteil, S. 64.

1130 GERSTER, Rn. 94 ff.

1131 Botschaft PrSG, S. 7432; ebenso SHK PrSG-HESS, Art. 2 N 39.

1132 GERSTER, Rn. 136.

lässt und im eigenen Namen oder unter der eigenen Handelsmarke vermarktet. Im Gegensatz zum PrSG knüpft die GPSR den Herstellerbegriff also nicht nur an die eigentliche Herstellung, sondern kumulativ an die Vermarktung[1133] im eigenen Namen an.[1134] Wer ein Produkt zwar herstellt, aber durch einen Dritten unter dessen Namen vermarkten lässt, gilt nicht als Hersteller nach der GPSR.[1135] In diesem Fall handelt es sich beim Dritten (dem, der das Produkt herstellen lässt), um den tatsächlichen Hersteller nach Art. 3 Ziff. 8 GPSR.[1136] Dasselbe gilt unter der KI-VO: Nur wer ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und dieses dann *auch noch* unter eigenem Namen in Verkehr bringt oder betreibt, kann gem. Art. 3 Ziff. 3 KI-VO als Anbieter gelten. Entwickelt eine Person ein KI-System, aber ein Dritter vermarktet dieses unter seinem Namen, gilt wiederum der Dritte als Anbieter gem. Art. 3 Ziff. 3 KI-VO.

277 Der Begriff des Herstellers ist im PrSG und in der GPSR weit auszulegen und inkludiert auch, wer Produkte verarbeitet sowie Teile zusammensetzt oder montiert, wie bspw. den Assembler.[1137] Auch Hersteller von Teilprodukten sind in der Schweiz für ihre Erzeugnisse verantwortlich.[1138] Ist das Endprodukt wie bspw. eine Küchenmaschine aufgrund eines Teilproduktes wie etwa einer Software, die erweiterte Funktionen ermöglicht, gefährlich, ist der Hersteller der Software für Gefahren verantwortlich, die sich direkt aus der Software ergeben. Ein Teilprodukt ist jedoch keine verwendungsbereite Sache, da es nicht direkt zur Nutzung durch Konsumenten bestimmt ist.[1139] Der Endhersteller bleibt deshalb weiterhin für sein Gesamtprodukt verantwortlich.[1140] Er ist am besten geeignet, die Sicherheit seines Produktes zu beurteilen.[1141] Im Produktsicherheitsrecht der EU gibt es immer nur einen Hersteller, und zwar den, der

1133 Zur Vermarktung siehe NHK GPSR-Piovano, Art. 9 N 62 ff., der sich mangels einer Definition in der GPSR auf einen EuGH-Entscheid zur Produkthaftung stützt: EuGH vom 09.02.2006, C-127/04, O'Byrne, ECLI:EU:C:2006:93, Rn. 27, welcher festhält, dass ein Produkt vermarktet wird, «in dem es in ge- oder verbrauchsfertigem Zustand öffentlich angeboten wird»; genauso mit Bezug auf die KI-VO Beck KI-VO-Wendehorst, Art. 3 N 122.

1134 Art. 3 Ziff. 8 GPSR; NHK GPSR-Wilrich, Art. 3 N 137, 140, m.w.H.

1135 NHK GPSR-Wilrich, Art. 3 N 138.

1136 Siehe auch NHK GPSR-Wilrich, Art. 3 N 144.

1137 Botschaft PrSG, S. 7432; Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 24; SHK PrSG-Hess, Art. 2 N 46; für die GPSR NHK GPSR-Wilrich, Art. 3 N 142.

1138 SHK PrSG-Hess, Art. 2 N 42; mit Bezug zum PrHG auch: BSK OR I-Fellmann, Art. 2 PrHG N 6 f.; BSK OR I-Fellmann, Art. 1 PrHG N 12.

1139 Siehe zum PrHG BSK OR I-Fellmann, Art. 2 PrHG N 6.

1140 Siehe zum PrHG BSK OR I-Fellmann, Art. 1 PrHG N 12.

1141 Bühler, Bestandteil, S. 65 f.

seinen Namen auf das Produkt setzt.[1142] Das heisst, dass der Hersteller von Smart Home Devices, der Software eines Dritten installiert, für das ganze Produkt zum Hersteller wird. Der Endhersteller ist deshalb für die Interaktion seines Produktes mit der Software von Dritten verantwortlich, wenn er entscheidet, diese zusammenzufügen. Ihn treffen also nicht nur Nachmarktpflichten in Bezug auf sein Endprodukt, sondern auch in Bezug auf die von ihm eingesetzten Komponenten, die damit interagieren, wie bspw. von ihm installierte oder ausdrücklich empfohlene Software. In der EU wird in Art. 25 Abs. 3 KI-VO explizit geregelt, dass der Hersteller des Gesamtproduktes zum Anbieter eines Hochrisiko-KI-Systems wird, wenn er dieses KI-System in Kombination mit seinem Produkt in Verkehr bringt oder in Betrieb nimmt und unter seinem Namen oder seiner Handelsmarke vermarktet.[1143]

2. Hersteller i.w.S. oder wer sonst noch als Hersteller oder Anbieter gilt

Im Gegensatz zum Hersteller i.e.S. *erschafft* der Hersteller i.w.S. keine neuen Produkte.[1144] Dennoch wird er im PrSG dem Hersteller i.e.S. gleichgestellt.[1145] Auch in der GPSR und in der KI-VO können Personen als Hersteller bzw. Anbieter gelten, wenn sie ihre Produkte nicht selbst erschaffen. 278

2.1. Quasi- oder Anscheinshersteller

Gem. Art. 2 Abs. 4 lit. a PrSG ist jede Person Hersteller, die «sich als Hersteller ausgibt, indem sie ihren Namen, ihr Warenzeichen oder ein anderes Erkennungszeichen auf dem Produkt anbringt». Weiter gilt auch als Hersteller, wer Produktionstätigkeiten auslagert, «um das Produkt unter seinem Namen oder seiner Marke in den Verkehr zu bringen».[1146] Diese werden auch Anscheins- oder Quasihersteller genannt.[1147] Die Definitionen des Quasiherstellers im PrSG und im PrHG sind deckungsgleich.[1148] Quasihersteller tauchen vor allem 279

1142 NHK GPSR-Wilrich, Art. 3 N 139; NHK GPSR-Schucht, Art. 13 N 4; NP GPSR-Schucht/Wiebe, § 3 N 21.

1143 S. u., Rn. 285.

1144 Gerster, Rn. 99 ff.

1145 Art. 2 Abs. 4 lit. a bis c PrSG; Botschaft PrSG, S. 7435 f.

1146 Botschaft PrSG, S. 7432.

1147 Botschaft PrSG, S. 7432.

1148 Botschaft PrSG, S. 7435; SHK PrSG-Hess, Art. 2 N 50; zu Bühlers Aussage siehe auch Gerster, Rn. 380; a.A. Bühler, Privatrecht, S. 47, welcher feststellt, dass die Botschaft die Herstellerdefinition im PrSG jener in Art. 2 Abs. 4 PrHG gleichsetze. Weiter stellt er fest,

im Bereich von «White-Label-Produkten»[1149] auf, da solche Produkte durch einen Dritten unter dessen Namen vermarktet werden und nicht unter jenem des eigentlichen «Erschaffers» des Produktes.[1150] Den Quasihersteller (auch «private label manufacturer» oder «own brand manufacturer»)[1151] gibt es auch in der GPSR.[1152] Um als Quasihersteller zu gelten, muss gem. Art. 13 Abs. 1 GPSR ein Produkt in Verkehr gebracht und kumulativ der Name oder die Handelsmarke (sog. «Labeling»)[1153] angebracht werden.[1154] Auch wer ein KI-System oder KI-Modell entwickeln *lässt* und es – ebenfalls kumulativ – unter seinem eigenen Namen oder seiner Handelsmarke in Verkehr bringt oder in Betrieb nimmt, gilt als Anbieter, obwohl er das KI-System oder KI-Modell nicht selbst entwickelt hat.[1155] Das Konstrukt des Quasiherstellers gibt es also auch als Pendant für den Anbieter. Quasihersteller müssen alle Herstellerpflichten und somit auch die Nachmarktpflichten erfüllen.[1156] Dasselbe gilt für die ebengenannten Quasi- oder Anscheinsanbieter, die dem Anbieter, der das KI-System selbst entwickelt hat, gleichgestellt sind.

2.2. Vertreter und Bevollmächtigter des Herstellers

280 Wer als Vertreter des Herstellers auftritt, wenn dieser seinen Sitz nicht im Inland (also der Schweiz) hat, gilt gem. Art. 2 Abs. 4 lit. b PrSG ebenfalls als Hersteller. Voraussetzung für die Qualifizierung als Hersteller ist, dass der Vertreter «objektiv für den ausländischen Hersteller auftritt» und «subjektiv auch diesen Hersteller im Inland vertreten will».[1157] Der Vertreter kann gleichzeitig Importeur sein, muss das aber nicht.[1158] Sinn dieser Bestimmung ist die Ver-

dass die Aussage in der Botschaft so nicht zutreffe, da das PrSG – zusätzlich zu den Herstellereigenschaften im PrHG – Personen als Hersteller erfasse, welche Produkte wiederaufbereiten oder die Sicherheitseigenschaft von Produkten in anderer Weise beeinflussen. Bühler verkennt jedoch, dass die Botschaft lediglich Art. 2 Abs. 4 lit. a PrSG der Quasiherstellerdefinition in Art. 2 Abs. 1 lit. b PrHG gleichsetzt und nicht der Herstellerdefinition grundsätzlich.

1149 Es handelt sich um ein markenneutrales Serienprodukt, das der «Erschaffer» i.d.R. an mehrere Abnehmer liefert. Als Quasihersteller bringen sie diese Produkte dann als ihr «eigenes» Markenprodukt in Verkehr.

1150 Siehe auch Kasper, Jusletter 23.09.2024, Rn. 24.

1151 NHK GPSR-Schucht, Art. 13 N 9.

1152 Art. 13 Abs. 1 GPSR; NHK GPSR-Wilrich, Art. 3 N 148 ff., m.w.H.

1153 NHK GPSR-Schucht, Art. 13 N 3, 4.

1154 NHK GPSR-Wilrich, Art. 3 N 149.

1155 Art. 3 Ziff. 3 KI-VO.

1156 Art. 2 Abs. 4 lit. a i.V.m. Art. 8 Abs. 2, 3 und 5 PrSG; NHK GPSR-Schucht, Art. 13 N 18.

1157 SHK PrSG-Hess, Art. 2 N 58.

1158 SHK PrSG-Hess, Art. 2 N 59, sowie zum Unterschied im Detail N 59 Fn. 125.

antwortungszuordnung für Importprodukte, weshalb er seinen Sitz in der Schweiz haben muss.[1159] Somit treffen den Vertreter als Hersteller dieselben Nachmarktpflichten wie den Hersteller i.e.S. Tritt jemand als Vertreter des Herstellers auf und werden parallel durch andere Importeure andere Produkte derselben Marke auf den Schweizer Markt gebracht, die der Vertreter nicht im Sortiment hat, ist der Vertreter nicht für diese zusätzlichen Produkte verantwortlich. Diese dritten Importeure (und nicht der Vertreter) sind in diesem Fall auch gem. Art. 8 Abs. 2 PrSG für die Nachmarktpflichten dieser zusätzlich eingeführten Produkte verantwortlich.[1160]

In der EU kommt der Bevollmächtigte dem Vertreter des PrSG am nächsten. 281
Bevollmächtigter ist gem. Art. 3 Ziff. 9 GPSR «jede innerhalb der Union niedergelassene natürliche oder juristische Person, die von einem Hersteller schriftlich beauftragt wurde, in dessen Namen bestimmte Aufgaben im Hinblick auf die Erfüllung der Pflichten des Herstellers» wahrzunehmen. Die Bestellung eines Bevollmächtigten in der EU ist dann sinnvoll (und teilweise verpflichtend), wenn der Sitz des Herstellers sich ausserhalb der EU befindet.[1161] So muss es für Smart Home Devices, die unter die RED fallen, nach Art. 4 Abs. 1 i.V.m. Art. 4 Abs. 5 MÜVO einen Wirtschaftsakteur in der EU geben, um bspw. nach Art. 4 Abs. 3 lit. c MÜVO die Marktüberwachungsbehörden über riskante Produkte zu unterrichten.[1162] Dieser Wirtschaftsakteur kann der Bevollmächtigte sein, der im Auftrag des Herstellers dessen Nachmarktpflichten übernimmt.[1163] Der Bevollmächtigte kann auch Einführer nach Art. 3 Ziff. 10 GPSR (also Importeur) sein.[1164] Auch die KI-VO kennt den Bevollmächtigten. Art. 3 Ziff. 5 KI-VO definiert ihn als «eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen». So muss bspw. ein Schweizer Anbieter, der ein Hochrisiko-KI-System in der EU auf den Markt bringen will, zuerst gem. Art. 22 Abs. 1 KI-VO schriftlich einen Bevollmächtigten in der EU ernennen. Somit kann der Bevollmächtigte die

1159 Botschaft PrSG, S. 7436.
1160 SHK PrSG-Hess, Art. 2 N 59.
1161 NHK GPSR-Wilrich, Art. 3 N 169.
1162 Siehe auch NHK GPSR-Wilrich, Art. 3 N 177; wurde ein Bevollmächtigter ernannt, muss dieser mindestens die Aufgaben gem. Art. 10 Abs. 2 GPSR übernehmen, wobei auch Meldepflichten dazugehören (lit. c).
1163 Siehe auch NHK GPSR-Wilrich, Art. 3 N 175, 179.
1164 Siehe auch NHK GPSR-Wilrich, Art. 3 N 170.

Nachmarktpflichten des Anbieters (genau wie für den Hersteller in der GPSR) übernehmen, wenn er dazu ermächtigt wurde.

282 Während der Vertreter im PrSG als Hersteller gilt, gilt der Bevollmächtigte nach der GPSR und der KI-VO nicht als Hersteller, kann aber dessen Pflichten übernehmen. Diese Pflichten müssen jedoch schriftlich übertragen werden. Der Vertreter muss nicht zwingend schriftlich beauftragt werden.

2.3. Wesentliche Beeinflusser von Sicherheitseigenschaften

283 Verändert eine Person die Sicherheitsaspekte eines Produktes wesentlich, gilt sie in der Schweiz nach Art. 2 Abs. 4 lit. c PRSG und in der EU nach Art. 13 Abs. 2 GPSR als Herstellerin (sofern sie gewerblich handelt[1165]). Der Grund dafür ist, dass aus produktsicherheitsrechtlicher Sicht ein neues Produkt geschaffen wird.[1166] Art. 13 Abs. 3 GPSR hält die wesentliche Veränderung detaillierter fest und verlangt, dass alle physischen oder digitalen[1167] Änderungen, die die Produktsicherheit beeinträchtigen und die nachfolgenden Kriterien kumulativ[1168] erfüllen, als wesentlich gelten. Das erste Kriterium gem. lit. a umfasst alle Änderungen, die nicht in der «ursprünglichen Risikobewertung des Produkts»[1169] berücksichtigt waren. Das zweite Kriterium nach lit. b umfasst Änderungen, aufgrund derer «sich die Art der Gefahr geändert, […] eine neue Gefahr entstanden [ist] oder […] sich das Risikoniveau erhöht» hat.[1170] Beim dritten Kriterium nach lit. c wird verlangt, dass «die Änderungen […] nicht von den Verbrauchern selbst oder in ihrem Auftrag für ihren eigenen Bedarf vorgenommen» wurden. Auch nach dem PrSG führen wesentliche Veränderungen durch Konsumenten nicht dazu, dass diese zu Herstellern werden, da es ihnen an der Gewerblichkeit fehlt.[1171] Ausschlaggebendes Kriterium für die wesentliche Veränderung ist in der Schweiz und der EU, dass eine Tätigkeit eine sicherheitsrelevante Auswirkung auf das Produkt hat.[1172] So ist auch Hersteller,

1165 S. u., Rn. 300.

1166 S. u., Rn. 302.

1167 Bereits im Blue Guide wurden wesentliche Veränderungen durch Software anerkannt, siehe Europäische Kommission, Blue Guide, S. 18.

1168 Siehe das «und» in Art. 13 Abs. 3 lit. b GPSR; ebenso NHK GPSR-Schucht, Art. 13 N 46.

1169 Zu welcher Hersteller vor der Inverkehrbringung verpflichtet sind gem. Art. 9 Abs. 2 GPSR.

1170 Wobei nur eine dieser drei Alternativen erfüllt sein muss, NHK GPSR-Schucht, Art. 13 N 52 f.

1171 S. u., Rn. 300.

1172 Botschaft PrSG, S. 7436; siehe auch Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 31, welche die Botschaft wortwörtlich zitiert; SHK PrSG-Hess, Art. 2 N 47 mit Beispielen; für die EU siehe: NHK GPSR-Schucht, Art. 13 N 27, 48.

wer das Produkt ergänzt oder Funktionen (wie bspw. durch Funkmodule[1173]) ändert, wenn diese Tätigkeiten die Sicherheit beeinflussen.[1174] Nimmt eine Person Veränderungen eines Produktes vor, die dessen Sicherheitseigenschaften verändern, ist diese Person nur bezogen auf das von der Veränderung betroffene Teil des Produktes als Hersteller zu qualifizieren,[1175] ausser die Veränderung wirkt sich auf das Produkt als Ganzes aus.[1176] Der Hersteller, der nur einen Teil eines Produktes einer wesentlichen Veränderung unterzogen hat, muss somit lediglich Herstellerpflichten (und damit Nachmarktpflichten) Pflichten in Bezug auf die von den Änderungen betroffenen Aspekte des Produktes wahrnehmen.[1177] Die wesentliche Veränderung muss nach dem Inverkehrbringen stattgefunden haben[1178] und das Produkt muss nach der Änderung vermarktet werden,[1179] damit eine Person als Hersteller nach Art. 13 Abs. 2 GPSR gilt.

Auch die KI-VO kennt die wesentliche Veränderung. Gem. Art. 25 Abs. 1 lit. b KI-VO gelten Personen als Anbieter eines Hochrisiko-KI-Systems, wenn sie an einem solchen System eine wesentliche Veränderung vornehmen und das KI-System ein Hochrisiko-KI-System i.S.v. Art. 6 KI-VO bleibt. Art. 3 Ziff. 23 KI-VO definiert die wesentliche Veränderung als «eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 beeinträchtigt wird *oder* die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde». Wer nach der Vornahme einer wesentlichen Veränderung als Anbieter gilt, hat auch die Pflichten gem. Art. 16 KI-VO zu erfüllen.[1180] Zur praktischen Durchführung der Bestimmungen über wesentliche Veränderungen werden gem. Art. 96 Abs. 1 lit. c KI-VO von der Europäischen Kommission noch Leitlinien erarbeitet. 284

1173 NHK GPSR-Schucht, Art. 13 N 44.
1174 Botschaft PrSG, S. 7432; ähnlich SHK PrSG-Hess, Art. 2 N 62; NHK GPSR-Schucht, Art. 13 N 44.
1175 Gerster, Rn. 137.
1176 Art. 13 Abs. 2, ErwG 35 GPSR.
1177 NHK GPSR-Schucht, Art. 13 N 30, m.w.H.
1178 NHK GPSR-Schucht, Art. 13 N 59.
1179 NHK GPSR-Schucht, Art. 13 N 62.
1180 Art. 25 Abs. 1 KI-VO.

2.4. Nur KI-VO: Wer nach Art. 25 KI-VO zum Anbieter eines Hochrisiko-KI-Systems wird

285 Art. 25 Abs. 1 KI-VO hält – zusätzlich zur wesentlichen Veränderung in lit. b – fest, dass auch zum Anbieter eines Hochrisiko-KI-Systems wird, wer gem. lit. a ein Hochrisiko-KI-System mit seinem Namen oder seiner Handelsmarke anschreibt und nach lit. c die Zweckbestimmung eines bereits in Verkehr gebrachten KI-Systems so verändert, dass dieses zu einem Hochrisiko-KI-System wird. Der ursprüngliche Anbieter verliert dann gem. Art. 25 Abs. 2 KI-VO seine Anbietereigenschaft. Zusätzlich wird gem. Art. 25 Abs. 3 KI-VO der Produkthersteller, der ein Hochrisiko-KI-System als Sicherheitsbauteil eines Produktes, das unter Anhang I Abschnitt A KI-VO fällt, zum Anbieter eines Hochrisiko-KI-Systems.[1181] Der Produkthersteller gilt jedoch nur als solcher Anbieter, wenn er das Hochrisiko-KI-System zusammen mit seinem Produkt unter seinem Namen oder seiner Handelsmarke in Verkehr bringt (lit. a) oder in Betrieb nimmt (lit. b). Produkthersteller und Anbieter (bzw. «Hersteller» eines Hochrisiko-KI-Systems) sind dann dieselbe Person. Verweist der Produkthersteller auf seinem Produkt also darauf, dass das Sicherheitsbauteil nicht von ihm stammt,[1182] gilt er nicht als Anbieter der KI-Komponente und kann sich entsprechend den zugehörigen Pflichten entziehen.[1183] Dies ist sinnvoll, da der Anbieter die Pflichten für KI-Systeme besser wahrnehmen kann als der Hersteller, der ein KI-System lediglich in sein Produkt integriert.[1184] Trotzdem ist der Produkthersteller weiterhin für die Gesamtsicherheit seines Produktes verantwortlich.[1185] Wer als Anbieter gem. Art. 25 Abs. 1 oder 3 KI-VO gilt, unterliegt den Anbieterpflichten nach Art. 16 KI-VO. Art. 16 KI-VO enthält keine eigenständigen Nachmarktpflichten, sondern verweist diesbezüglich lediglich auf andere Bestimmungen der KI-VO.[1186]

IV. Exkurs: Betreiber

286 Der Betreiber ist vom Anbieter abzugrenzen. Der Betreiber verwendet gem. Art. 3 Ziff. 4 KI-VO KI-Systeme in eigener Verantwortung. Verwendet eine Person ein KI-System privat und nicht gewerblich, handelt es sich bei dieser Per-

1181 Siehe auch Beck KI-VO-Wendehorst, Art. 3 N 78.

1182 Siehe dazu den Vorschlag von Borges, einen Hinweis in der Art von «Sicherheit made by X» anzubringen, Borges, Begriff, Rn. 50.

1183 Noch zum KI-VO Entwurf Borges, Begriff, Rn. 49 f.

1184 Siehe auch Borges, Teil 1, Rn. 77.

1185 Borges, Teil 1, Rn. 77.

1186 Art. 16 lit. d i.V.m. Art. 18 Abs. 1 KI-VO; Art. 16 lit. e i.V.m. Art. 19 Abs. 1 KI-VO; Art. 16 lit. j i.V.m. Art. 20 Abs. 1 KI-VO.

son um einen Verbraucher und nicht um einen Betreiber.[1187] Der Betreiber kann wie andere Wirtschaftsakteure wie z.B. der Importeur oder der Bevollmächtigte Nachmarktpflichten haben, auf welche vorliegend jedoch nicht weiter eingegangen wird.

V. Fazit

287 Als Hersteller gelten im allgemeinen Produktsicherheitsrecht der Schweiz und der EU Quasihersteller, u.U. Vertreter (Bevollmächtigte gelten nicht als Hersteller, können aber deren Pflichten haben) sowie wesentliche Beeinflusser von Sicherheitseigenschaften. Die Herstellerbegriffe in der Schweiz und in der EU decken sich grösstenteils. In der EU gilt der tatsächliche Erschaffer eines Produktes jedoch nicht als Hersteller, wenn er sein Produkt nicht auch unter seinem Namen oder seiner Handelsmarke vermarktet, in der Schweiz aber schon. In der KI-VO gelten Quasianbieter (für Bevollmächtigte gilt dasselbe wie in der GPSR) sowie wesentliche Beeinflusser von Sicherheitseigenschaften als Anbieter, wobei dies nur gilt, wenn sie ein KI-System unter eigenem Namen oder unter einer eigenen Handelsmarke in Verkehr bringen oder in Betrieb nehmen. Weiter gilt als Anbieter eines Hochrisiko-KI-Systems, wer sich als Anbieter eines Hochrisiko-KI-Systems ausgibt und wer die Zweckbestimmung eines in Verkehr gebrachten KI-Systems so verändert, dass es zu einem Hochrisiko-KI-System wird. Zudem sind Produkthersteller, die Hochrisiko-KI-Systeme als Sicherheitsbauteile verwenden, nach Art. 25 Abs. 3 KI-VO auch Anbieter von Hochrisiko-KI-Systemen. Wer als Hersteller bzw. als Anbieter gilt, muss auch die Hersteller- bzw. Anbieterpflichten und die damit einhergehenden Nachmarktpflichten erfüllen.

288 Da mit Einführung des PrSG eine Angleichung des Schutzniveaus an jenes der EU angestrebt wurde,[1188] würde es Sinn ergeben, den Herstellerbegriff gleich wie in der EU zu regulieren. Die zwei wichtigsten Unterschiede zwischen dem Hersteller im Produktsicherheitsrecht für KI-Produkte in der Schweiz und der EU sind, 1) dass die tatsächlichen Erschaffer von Produkten nur in der Schweiz als Hersteller zu klassifizieren sind, wenn sie ihre Produkte *nicht* unter ihrem Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen, und 2) dass die EU mit der KI-VO den Hersteller von KI-Systemen als «Anbieter» speziell geregelt hat und ihm vor allem in Bezug auf Hochrisiko-KI-Systeme besondere Pflichten auferlegt.

1187 Siehe mit Beispielen auch KASPER, Jusletter 23.09.2024, Rn. 24.

1188 S. o., Rn. 148.

289 Problematisch ist, dass Quasihersteller, Vertreter und wesentliche Beeinflusser von Sicherheitseigenschaften zwar als Hersteller gelten, aber das Produkt i.d.R. nicht so gut kennen wie der Hersteller, der das Produkt tatsächlich erschafft. Hersteller i.w.S. werden auch kaum sicherheitsrelevante Eigenschaften am Produkt ändern können, indem sie ein Update zur Verfügung stellen, da sie gar keine technische Verbindung zum Produkt haben.[1189] Bezüglich Nachmarktpflichten heisst das, dass Hersteller i.w.S. Produkte gar nicht so genau beobachten können, wie dies der Hersteller i.e.S. kann.[1190]

290 Hersteller und Anbieter handeln immer gewerblich. Wenn Konsumenten Produkte verändern, indem sie sie bspw. aktualisieren oder mit eigenen Daten trainieren, sind sie weder vom PrSG noch von der GPSR als Hersteller erfasst. Dies gilt selbst dann, wenn sie damit eine sicherheitsrelevante Funktion des Produktes verändern, da sie nicht gewerblich handeln. Der Hersteller ist auch in diesem Fall weiterhin für die Nachmarktpflichten verantwortlich, ausser wenn die Verwendung durch den Konsumenten missbräuchlich war und nicht im Rahmen einer vernünftigen Vorhersehbarkeit lag.

1189 Diese müsste vom Hersteller technisch so eingerichtet werden, dass auch der Hersteller i.w.S. Updates zur Verfügung stellen kann. S. o., Rn. 84. Für den wesentlichen Beeinflusser von Sicherheitseigenschaften gilt dies nur eingeschränkt, da er sich diese technische Verbindung u.U. selbst einrichten kann.

1190 Siehe auch Furrer, in: Fellmann/Furrer, Schonzeit, S. 93.

D. Beginn der Nachmarktpflichten

Die Nachmarktpflichten grenzen sich von den Vormarktpflichten ab. Wie der Name sagt, sind diese Pflichten zu erfüllen, nachdem das Produkt «auf den Markt gebracht» wurde. Was das genau heisst, soll in diesem Kapitel geklärt werden. Selbstverständlich benötigt die richtige Umsetzung von Nachmarktpflichten bereits vor dem Inverkehrbringen Vorkehrungen. Auf Pflichten vor der Inverkehrbringung (sog. Vormarktpflichten) wird vorliegend jedoch nicht eingegangen. 291

I. Gebrauchsdauer und erstmalige Bereitstellung

Die Dauer von Nachmarktpflichten hängt im Allgemeinen von der Gebrauchsdauer eines Produktes ab.[1191] In der Schweiz muss der Hersteller gem. Art. 8 Abs. 2 PrSG «während der angegebenen oder vernünftigerweise vorhersehbaren Gebrauchsdauer eines Produktes» Massnahmen nach dem Inverkehrbringen treffen. Da die Gebrauchsdauer nur in Art. 8 Abs. 2 PrSG genannt ist, geht Holliger-Hagmann davon aus, dass es sich hier um eine Gesetzeslücke handelt.[1192] Sie spricht sich zu Recht dafür aus, dass auch für die Festlegung des Zeitraums der weiteren Pflichten gem. Art. 8 Abs. 3 bis 5 PrSG auf die Gebrauchsdauer abgestellt werden kann.[1193] Da die Gebrauchsdauer mit der Inverkehrbringung beginnt, beginnen auch die Nachmarktpflichten mit der Inverkehrbringung des Produktes.[1194] In der EU beginnen die Nachmarktpflichten des Herstellers nach der GPSR mit der erstmaligen Bereitstellung eines Produktes.[1195] Mit dem erstmaligen Bereitstellen eines Produktes auf dem Markt der EU gilt das Produkt gem. Art. 3 Ziff. 7 GPSR als in Verkehr gebracht. Die Nachmarktpflichten für Anbieter von Hochrisiko-KI-Systemen beginnen ebenfalls mit dem Inverkehrbringen.[1196] Die Inverkehrbringung grenzt im PrSG[1197] sowie in der 292

1191 S. u., Rn. 395 ff.

1192 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 3.

1193 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 3; siehe auch Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 3, in Bezug auf die Meldepflicht; wohl auch Furrer, in: Fellmann/Furrer, Schonzeit, S. 92; eventuell auch Bühler, Bestandteil, S. 158.

1194 Art. 8 PrSG befindet sich als einziger Art. im 3. Abschnitt «Pflichten nach dem Inverkehrbringen».

1195 NHK GPSR-Wilrich, Art. 3 N 125.

1196 Zur Beobachtungspflicht nach Art. 72 Abs. 2 KI-VO siehe Beck KI-VO-Hartmann, Art. 72 N 10.

1197 Gerster, Rn. 125, m.w.H.

GPSR und der KI-VO die Vor- und Nachmarktpflichten zeitlich voneinander ab.

II. Inverkehrbringung und Inbetriebnahme

293 Da die Nachmarktpflichten erst ab der Inverkehrbringung eines Produktes gelten, muss zunächst geklärt werden, ab wann Software als «in Verkehr gebracht» gilt. Aufgrund der Veränderlichkeit von Softwareprodukten und der Überlassung von Software via Downloads wird die Feststellung des Zeitpunkts der Inverkehrbringung erschwert.[1198]

294 Die Inverkehrbringung wird in Art. 2 Abs. 3 PrSG definiert.[1199] Demnach gilt ein Produkt unabhängig davon, ob es neu, gebraucht, wiederaufbereitet oder wesentlich verändert worden ist, als in Verkehr gebracht. Dies im Unterschied zur GPSR und der KI-VO: Nur die *erstmalige* Bereitstellung auf dem EU-Markt gilt gem. Art. 3 Ziff. 7 GPSR[1200] bzw. Art. 3 Ziff. 9 KI-VO[1201] als Inverkehrbringen. Da ein erneutes Inverkehrbringen eine Beeinflussung einer sicherheitsrelevanten Eigenschaft voraussetzt,[1202] handelt es sich bei der Regelung des PrSG im Prinzip aber um die gleiche Regelung wie in der GPSR und der KI-VO.[1203] Die Bereitstellung auf dem Markt wird in Art. 3 Ziff. 6 GPSR und Art. 3 Ziff. 10 KI-VO beinahe deckungsgleich geregelt. Produkte bzw. KI-Systeme oder KI-Modelle mit allgemeinem Verwendungszweck gelten als bereitgestellt, wenn sie zum Vertrieb oder zur Verwendung[1204] auf dem Markt der EU abgegeben wurden. Auch wenn die Literatur zum PrSG nichts darüber aussagt, wird vorliegend davon ausgegangen, dass ein Produkt analog zum PrHG *willentlich* in

1198 Europäische Kommission, Impact Assessment GPSR, S. 14; Twigg-Flesner, S. 10 f.

1199 Art. 3 lit. d THG enthält die gleiche Definition.

1200 Siehe auch NHK GPSR-Wilrich, Art. 3 N 127.

1201 Siehe auch Beck KI-VO-Wendehorst, Art. 3 N 113.

1202 S. u., Rn. 302.

1203 Siehe auch das BVGer, welches die Bestimmung des PrSG als «im Wesentlichen dieselbe Regelung» bezeichnet wie die «erstmalige Bereitstellung» gem. Art. 2 Abs. 1 lit. b NEV, BVGer A-4413/2021 vom 20.09.2023, E. 4.3.3.

1204 Art. 3 Ziff. 6 GPSR nennt zusätzlich zum Vertrieb und zur Verwendung noch den Verbrauch.

Verkehr gebracht werden muss.[1205] Dasselbe gilt für die Bereitstellung nach der GPSR[1206] sowie der KI-VO[1207].

In der KI-VO wird teilweise statt nur auf die Inverkehrbringung auch auf die Inbetriebnahme abgestellt. Es handelt sich bei der Inbetriebnahme gem. Art. 3 Ziff. 11 KI-VO um die Bereitstellung eines KI-Systems in der EU zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung. Wird das KI-System vom Anbieter z.B. nicht in Verkehr gebracht, sondern nur «intern» zum Eigengebrauch verwendet, handelt es sich um eine Inbetriebnahme.[1208] Die Inbetriebnahme wird dem Inverkehrbringen in diesem Fall gleichgestellt.[1209] Der gewerbliche Eigengebrauch wird nach Art. 2 Abs. 3 lit. a PRSG ebenfalls als ein Inverkehrbringen gewertet. Nach der GPSR ist der Eigengebrauch durch den Hersteller kein Inverkehrbringen.[1210] Da das Inverkehrbringen und die Inbetriebnahme durch den Anbieter grundsätzlich gleichgestellt sind, ist die Unterscheidung nicht besonders relevant.[1211] Wichtig ist jedoch, dass die Inbetriebnahme in der KI-VO von der normalerweise im Produktsicherheitsrecht verwendeten Inbetriebnahme abweicht.[1212] In der Schweiz wird die Inbetriebnahme weder im PrSG noch im PrHG, sondern in Art. 3 lit. e THG definiert. Die Inbetriebnahme eines Produktes gilt dort als «die *erstmalige Verwendung* eines Produkts durch Endbenutzerinnen und Endbenutzer». Vorliegend wird in Anlehnung an Bühlers Meinung vertreten, dass ein Produkt keine solche Inbetriebnahme erfordert, um als in Verkehr gebracht zu gelten.[1213] Ein Produkt kann bereits vor der erstmaligen Verwendung gefährlich sein, wenn eine Batterie bspw. schon in der Verpackung überhitzt[1214] und das Gerät vom Endnutzer noch vor der «erstmaligen Verwendung» steht. 295

1205 BSK OR I-Fellmann, Art. 5 PrHG N 2 f., womit z.B. ein Diebstahl nicht als Inverkehrbringen gilt. Andererseits handelt es sich um ein Inverkehrbringen, wenn der Hersteller sein Produkt z.B. aufgrund eines Irrtums freigibt. Würde eine Software also aufgrund eines internen Kommunikationsfehlers zu früh auf den Markt kommen, handelt es sich um ein Inverkehrbringen; SHK PrHG-Hess, Art. 5 N 4, 6, m.w.H.

1206 NHK GPSR-Wilrich, Art. 3 N 107.

1207 Beck KI-VO-Wendehorst, Art. 2 N 15.

1208 Beck KI-VO-Wendehorst, Art. 2 N 18; Beck KI-VO-Wendehorst, Art. 3 N 135.

1209 Beck KI-VO-Wendehorst, Art. 3 N 135.

1210 Europäische Kommission, Blue Guide, S. 20; NHK GPSR-Schucht, Art. 13 N 62; NHK GPSR-Wilrich, Art. 3 N 118, 121, jedoch mit Verweisen auf das deutsche Recht.

1211 Beck KI-VO-Wendehorst, Art. 3 N 139.

1212 Beck KI-VO-Wendehorst, Art. 3 N 131; zur GPSR NHK GPSR-Wilrich, Art. 3 N 118.

1213 Bühler, Bestandteil, S. 61 f.

1214 Elektronische Geräte werden üblicherweise mit teilweise geladenen Batterien in Verkehr gebracht.

1. Verfügbarmachen reicht aus

296 Es war früher logisch, dass es sich nur um ein Inverkehrbringen eines Produktes handelt, wenn der Hersteller die Verfügungsgewalt oder Sachherrschaft über sein Produkt definitiv aufgibt.[1215] Das ändert sich mit Produkten, welche nach Inverkehrbringung verändert werden können, z.B. in Form von Softwareupdates.[1216] Bei Geräten mit einer bestehenden Verbindung zum Hersteller (im Sinne einer technischen Konnektivität)[1217] wird die Verfügungsgewalt über das Gerät nicht vollständig übertragen, weil der Hersteller auch nach einem Besitzwechsel immer noch auf das Gerät einwirken kann. Der Hersteller, der nach der Inverkehrbringung seiner Software bzw. seines KI-Systems weiterhin Einfluss auf sein Produkt hat, hat auch die Kontrolle darüber nicht abgegeben.[1218] Der Hersteller eines intelligenten Rasenmähers kann sich bspw. die Möglichkeit offenlassen, via Internet weiterhin Softwareupdates auf dem Rasenmäher zu installieren.

297 In der Literatur zum PrSG wird für die Überlassung in Bezug auf die Inverkehrbringung nach Art. 2 Abs. 3 PrSG auf die Übertragung der Verfügungsgewalt[1219] oder der Sachherrschaft[1220] abgestellt. Die GPSR stellt zwar auf die Abgabe ab,[1221] Abgabe und Überlassung sind jedoch austauschbar.[1222] Auch bezogen auf die GPSR werden «Besitz- und Verantwortungsübergang» als die zentralen Kriterien der Abgabe genannt.[1223] Das Produkt kann beim «Überlassen» im Sinne der Inverkehrbringung gleichzeitig immer noch im Herrschaftsbereich des Herstellers sowie bereits im Herrschaftsbereich eines Dritten sein. Das Vorliegen einer Gefahr, welche von einem Produkt ausgeht, ist nicht davon abhängig, ob sich ein Produkt *immer noch*, sondern ob es sich – mindestens teil-

1215 Alle diese Meinung vertretend: Bühler, Bestandteil, S. 144 f.; SHK PrSG-Hess, Art. 2 N 19 m.w.H.; bezogen auf die GPSR: NHK GPSR-Wilrich, Art. 3 N 110, m.w.H.; NP GPSR-Schucht/Wiebe, § 3 N 43.

1216 Koch/Pichonnaz, S. 630; siehe auch: Wagner, in: Lohsse/Schulze/Staudenmayer, Smart Products, S. 157; Wagner, Verantwortlichkeit, S. 728.

1217 Bspw. bei allen IoT-Geräten, s. o., Rn. 84.

1218 Wildhaber, Einführung, S. 48; Wagner, Verantwortlichkeit, S. 728, 734.

1219 Gerster, 46; Bühler, Bestandteil, S. 145.

1220 Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 11; Furrer, in: Fellmann/Furrer, Schonzeit, S. 90; SHK PrSG-Hess, Art. 2 N 19 m.w.H.; im Detail, jedoch bezogen auf das deutsche ProdSG: Beck ProdSG-Klindt/Schucht, § 2 Rn. 26 ff.

1221 Art. 3 Ziff. 6 GPSR.

1222 Siehe dazu mit Kritik NHK GPSR-Wilrich, Art. 3 N 108.

1223 NHK GPSR-Wilrich, Art. 3 N 109 ff., m.w.H.

weise – *nicht mehr* im Herrschaftsbereich[1224] des Herstellers befindet.[1225] So kann der Rasenmäher aus obigem Beispiel Auswirkungen auf Verbraucher und Dritte (z.B. «innocent bystanders») haben, auch wenn sich die Software immer noch im Herrschaftsbereich des Herstellers befindet. Der Hersteller könnte bspw. (aus Versehen) die Software dementsprechend aktualisieren, dass der Rasenmäher bei der Verwendung im Garten des Verbrauchers Hindernisse nicht mehr richtig erkennt und ein auf der Wiese sitzendes Kind verletzt. Bereits das «Verfügbarmachen» muss also reichen, da ab dann schon Gefahren bezüglich der Produktsicherheit bestehen können.[1226] Gerade bei digitalen Produkten kann der «Übergang der Verantwortlichkeit für den Zustand des Produktes»[1227] nicht das ausschlaggebende Kriterium sein. Konkret in Bezug auf Softwareprodukte müssen diese deshalb auch als in Verkehr gebracht gelten, wenn sie online, z.B. über eine Cloud, zur Verfügung gestellt werden.[1228]

Ein Produkt muss deshalb als in Verkehr gebracht gelten, sobald es im Rahmen des «Wirtschaftsverkehrs bestimmungsgemäss eingesetzt wird», der Produktionsprozess zumindest vorläufig beendet ist,[1229] und die potenzielle Gefahr, die vom unsicheren Produkt ausgeht, nicht länger auf innerbetriebliche Abläufe beschränkt bleibt sowie Dritte in ihren schutzwürdigen Interessen beeinträchtigt werden[1230]. Dies lässt sich mit den Formulierungen «Überlassen» im PrSG und «Abgabe» in der GPSR problemlos vereinbaren. Da auch das Anbieten eines Produktes nach Art. 2 Abs. 3 lit. d PrSG ein Inverkehrbringen ist, z.B. wenn online eine Bestellung aufgegeben werden kann,[1231] und nun neu dasselbe in der EU gem. Art. 4 GPSR gilt,[1232] erübrigt sich die Diskussion im 298

1224 Der EuGH hat festgehalten, dass es für das Inverkehrbringen nach der (alten) PLD 1985 nicht nötig sei, dass das Produkt die «Herrschaftsspähre» des Herstellers verlassen müsse: EuGH vom 10.05.2001, C-203/99, Veedfald, ECLI:EU:C:2001:258, Rn. 17; ausführlich mit Bezug auf den ebengenannten Entscheid: SHK PrHG-Hess, Art. 5 N 7; Wagner, Produkthaftung, S. 719.

1225 Für das PrHG: BSK OR I-Fellmann, Art. 5 PrHG N 5; siehe auch zum deutschen ProdSG Beck ProdSG-Klindt/Schucht, § 2 N 29, welche festhalten, dass es auf den Übergang «des produktspezifischen Gefahrenpotenzials auf einen neuen (Produkt-)Nutzer» ankomme; unklar NHK GPSR-Wilrich, Art. 3 N 109 f., m.w.H.

1226 Erstaunlicherweise NHK GPSR-Wilrich, Art. 3 N 110, obwohl er in N 109 a.M. zu sein scheint.

1227 So NHK GPSR-Wilrich, Art. 3 N 110.

1228 Beck KI-VO-Wendehorst, Art. 3 N 139; Wagner, Produkthaftung, S. 719.

1229 Mit Bezug auf das deutsche und europäische Produkthaftungsrecht Wagner, Produkthaftung, S. 719; passend dazu auch die Beispiele in BSK OR I-Fellmann, Art. 5 PrHG N 5.

1230 Mit Bezug auf das PrHG: BSK OR I-Fellmann, Art. 5 PrHG N 5, m.w.H.

1231 BVGer A-4413/2021 vom 20.09.2023, E. 4.3.3 f.; Botschaft PrSG, S. 7435; Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 21; SHK PrSG-Hess, Art. 2 N 33.

1232 Siehe auch NHK GPSR-Wilrich, Art. 3 N 113.

Prinzip. Die Inverkehrbringung nach Art. 3 Ziff. 9 KI-VO wird zwar ebenfalls über die Abgabe definiert, ist aber auch bereits erfüllt, wenn ein KI-System verfügbar gemacht wird.[1233]

299 Bietet der Hersteller eine Dienstleistung an, bei der er sein Produkt verwendet, dann gilt dies gem. Art. 2 Abs. 3 lit. b PrSG ebenfalls als Inverkehrbringung.[1234] Es ist nicht nötig, dass er das Produkt abgibt oder aushändigt. Dasselbe gilt nach Art. 3 Ziff. 1 GPSR. Anderer Meinung ist WILRICH. Er stellt fest, dass das Zurverfügungstellen in der GPSR im Rahmen einer Dienstleistung kein Bereitstellen sei, da nur kurzzeitig «zur Verfügung gestellt» statt dauerhaft «bereitgestellt» werde.[1235] Da das Zurverfügungstellen vorliegend als ausreichend angesehen wird (auch lediglich kurzzeitig), kann dieser Ansicht nicht gefolgt werden. Ebenfalls als Inverkehrbringen gilt das Bereithalten eines Produktes zur Benützung durch Dritte nach Art. 2 Abs. 3 lit. c PrSG.[1236] WILRICH verneint die Bereithaltung als Bereitstellung wiederum für die GPSR, da er auf eine «Aushändigung» des Produktes besteht.[1237]

2. Gewerbsmässigkeit nötig

300 Vom PrSG erfasst sind gem. Art. 1 Abs. 2 PrSG nur Produkte, die gewerblich oder beruflich in Verkehr gebracht werden.[1238] Gem. Art. 2 Abs. 3 PrSG spielt es dabei keine Rolle, ob etwas für das Produkt bezahlt werden muss oder dieses kostenlos zur Verfügung gestellt wird.[1239] Auch «wenn ein Produkt einem Kunden zum Ausprobieren überlassen wird», ist dies eine Inverkehrbringung.[1240] Auch Werbegeschenke sind Produkte i.S.d. PrSG.[1241] Dasselbe gilt gem. Art. 3 Ziff. 6 GPSR und nach Art. 3 Ziff. 10 KI-VO. Ob Produkte bzw. KI-Systeme entgeltlich oder unentgeltlich und z.B. als Werbegeschenke abgegeben werden, spielt keine Rolle, solange sie gewerblich in Verkehr gebracht werden.[1242]

1233 Beck KI-VO-WENDEHORST, Art. 2 N 15. Die in Beck KI-VO-WENDEHORST, Art. 3 N 125 aufgezählten Ausnahmen widersprechen dem oben Gesagten nicht.

1234 Siehe auch Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 17.

1235 NHK GPSR-WILRICH, Art. 3 N 117.

1236 Siehe auch Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 18.

1237 NHK GPSR-WILRICH, Art. 3 N 109.

1238 Zuletzt und statt vieler HESS, in: Häner/Waldmann S. 220.

1239 Botschaft PrSG, S. 7434; Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 13; SHK PrSG-HESS, Art. 1 N 4.

1240 Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 2 PrSG N 13; SHK PrSG-HESS, Art. 2 N 21, 31.

1241 HESS, in: Häner/Waldmann S. 221; HOLLIGER-HAGMANN, Produktsicherheit und Haftpflicht, S. 14.

1242 Art. 3 Ziff. 6 i.V.m. Ziff. 7 GPSR; Art. 3 Ziff. 9 i.V.m. Ziff. 10 KI-VO; zur GPSR siehe auch NHK GPSR-WILRICH, Art. 3 N 22; zur KI-VO siehe auch Beck KI-VO-WENDEHORST, Art. 3 N 128.

In Bezug auf Software ist dies u.a. relevant bei Demoversionen (engl. «Trial Versions») von Produkten. Oftmals ist es möglich, ein Programm bspw. 30 Tage lang kostenlos zu nutzen, bevor es nur noch kostenpflichtig genutzt werden kann. Auch für eine solche «Testzeit» gilt das Produkt als in Verkehr gebracht, da die Testversion den Nutzer anregen soll, das Produkt weiterhin zu verwenden und nach Ablauf der unentgeltlichen Zeitspanne dafür zu bezahlen. Es handelt sich um ein zeitlich begrenztes, digitales Werbegeschenk. Ebenfalls verbreitet ist Software mit eingeschränkten Funktionen, die erst durch Bezahlung vollständig genutzt werden können (sog. Freemium-Modell). Auch hier handelt es sich bei der kostenlosen Version im Prinzip um Werbung für die Vollversion und sie ist als gewerbliches Inverkehrbringen anzusehen.[1243] Ebenfalls als gewerbliche Inverkehrbringung zu verstehen ist kostenlos als Download zur Verfügung gestellte Software, die noch nicht ganz fertig entwickelt oder getestet ist, z.B. bei Alpha- oder Beta-Versionen.[1244] Wenn das Testen dem Konsumenten überlassen wird und das Produkt bspw. mittels automatischer Feedbacks verbessert werden soll, untersteht es ebenfalls den Nachmarktpflichten. 301

3. Erneute Inverkehrbringung durch wesentliche Änderung

Gem. Art. 2 Abs. 3 PrSG handelt es sich um eine Inverkehrbringung eines neuen Produktes, wenn ein zuvor bereits in Verkehr gebrachtes Produkt in wesentlich verändertem Zustand wieder auf den Markt gebracht wird.[1245] Gemeint ist die *sicherheitsrelevante*, wesentliche Veränderung.[1246] Auch nach Art. 13 Abs. 2 GPSR wird bei einer sicherheitsrelevanten, wesentlichen Veränderung eines Produktes ein neues Produkt geschaffen, wenn es nach der Änderung vermarktet wird.[1247] Die Vornahme einer sicherheitsrelevanten, wesentlichen Veränderung macht das Hochrisiko-KI-System – analog zum neuen Produkt in der GPSR und im PrSG – zu einem neuen (Hochrisiko-)KI-System.[1248] Die Kriterien zur wesentlichen Veränderung wurden bereits in 302

1243 Für weitere Beispiele siehe Beck KI-VO-Wendehorst, Art. 3 N 128.

1244 Siehe auch bezogen auf Prototypen: Botschaft PrSG, S. 7435; Gerster, Rn. 66, m.w.H.; zur GPSR siehe NP GPSR-Schucht/Wiebe, § 3 N 9, m.w.H.; zur KI-VO siehe Beck KI-VO-Wendehorst, Art. 3 N 123.

1245 Siehe auch Fornage, Sécurité, Rn. 38, mit Verweis auf BGE 143 II 518, 551 E. 10.

1246 Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 7; ähnlich SHK PrSG-Hess, Art. 2 N 11.

1247 ErwG 35 GPSR; siehe auch NHK GPSR-Schucht, Art. 13 N 26, 62.

1248 Art. 3 Ziff. 23, ErwG 84 und 128 KI-VO.

Rn. 283 ff. im Zusammenhang mit dem Beeinflusser von Sicherheitseigenschaften, der zum Hersteller wird, erläutert. In Bezug auf Geräte mit Software oder bei selbstständiger Software ist die wesentliche Veränderung besonders relevant, da ein Softwareupdate eine solche Veränderung mit sich bringen kann.[1249] Ein Update kann ein bestehendes Produkt so weit verändern, dass nach der Installation aus produktsicherheitsrechtlicher Perspektive ein neues Produkt vorliegt[1250] und – zumindest in der EU – eine erneute Risikobewertung erfordert.[1251] Bei der erneuten Risikobewertung handelt es sich nicht um eine Nachmarkt-, sondern um eine Vormarktpflicht.[1252] Nicht als wesentliche Veränderung gelten Änderungen, die durch das geplante «Dazulernen» von KI-Systemen geschehen.[1253]

III. Fazit

303 In Bezug auf den Beginn der Nachmarktpflichten im allgemeinen Produktsicherheitsrecht wird in der Schweiz auf die Gebrauchsdauer und in der EU auf die erstmalige Bereitstellung eines Produktes abgestellt. Die Gebrauchsdauer und die erstmalige Bereitstellung beginnen mit der Inverkehrbringung eines Produktes. Die Nachmarktpflichten für KI-Systeme beginnen gem. KI-VO ebenfalls mit der Inverkehrbringung. Ein Produkt bzw. ein KI-System ist in Verkehr gebracht, wenn dieses vom Hersteller willentlich als (zumindest vorläufig) fertiges Produkt gewerbsmässig verfügbar gemacht wurde. Auch eine Bereitstellung und ein Anbieten des Produktes über das Internet zum Download – egal ob kostenpflichtig oder nicht – sind ein Inverkehrbringen. Wird das Produkt nach der Inverkehrbringung wesentlich verändert (bspw. durch ein Softwareupdate) und danach vermarktet, handelt es sich um ein neues Produkt und somit um eine erneute Inverkehrbringung.

304 Der gewerbliche Eigengebrauch des Herstellers ist in der GPSR kein Inverkehrbringen und löst damit keine Nachmarktpflichten für Software aus. Im PrSG gilt der gewerbliche Eigengebrauch des Herstellers als Inverkehrbringen

1249 Europäische Kommission, Blue Guide, S. 18 f.; ErwG 35 GPSR, hält fest, dass digitale Änderungen die Sicherheit von Produkten gefährden können; siehe auch Europäisches Parlament, Stellungnahme GPSR, Änderungsantrag 11, Vorschlag für eine Verordnung Erwägung 20, Geänderter Text.

1250 Oster, in: Foerste/Westphalen, § 57 Rn. 26; Piovano/Schucht/Wiebe, S. 100.

1251 ErwG 25 GPSR; zur Risikobewertung siehe Art. 9 Abs. 2 GPSR.

1252 Vormarktpflichten müssen bereits bei der Bereitstellung auf dem Markt erfüllt sein. Nachmarktpflichten hingegen, werden erst danach «aktiviert», Schucht, Produktkrisen, S. 313, m.w.H.

1253 Art. 43 Abs. 4 Uabs. 2 und ErwG 128 KI-VO; NHK GPSR-Wiebe, Art. 6 N 38.

und in der KI-VO als Inbetriebnahme, weshalb er in der Schweiz in Bezug auf Software und in der KI-VO in Bezug auf Hochrisiko-KI-Systeme Nachmarktpflichten auslöst.

E. Inhalt der Nachmarktpflichten

305 Sobald der Hersteller ein Produkt in Verkehr gebracht hat, befindet es sich im Nachmarktstadium.[1254] Ab dann ist er verpflichtet, Nachmarktpflichten wahrzunehmen. Da der Begriff Nachmarktpflichten nicht definiert wird, werden vorliegend alle Pflichten dazugezählt, die von den Wirtschaftsakteuren selbstständig nach der Inverkehrbringung zu erfüllen sind.[1255] Vorbereitungshandlungen, die bereits vor der Inverkehrbringung zu erfüllen sind, und von Behörden verlangte Massnahmen gehören nicht dazu. Zu den Vorbereitungshandlungen gehören bspw. (je nach Regulierung und Art des Produktes) die Risikoanalyse und Beseitigung von bereits erkennbaren Gefahren, das Planen eines Risiko- und Krisenmanagements inklusive Notfallplan, die Sicherstellung der Rückverfolgbarkeit von Produkten[1256] sowie die Kennzeichnung von KI-Erzeugnissen, das Erstellen von Bedienungsanleitungen und Warn- und Sicherheitshinweisen sowie das Bereitstellen von Kanälen für Beschwerden. Behörden können vom Hersteller die Mitwirkung beim Vollzug von Massnahmen verlangen (z.B. Zugang gewähren und Informationen aushändigen). Dabei wird dem Hersteller bspw. vorgeschrieben, welche Massnahmen getroffen werden müssen, und er hat (fast) keinen Spielraum mehr, wie er dies erfüllen will. Es handelt sich also nicht mehr um selbstverantwortete Nachmarktpflichten. Konkret werden hier zu den Nachmarktpflichten gezählt: Gefahrenerkennungsmassnahmen bzw. die Beobachtung nach der Inverkehrbringung, Gefahrenabwendungsmassnahmen, Melde- und Aufbewahrungspflichten. Bei den produktsicherheitsrechtlichen Nachmarktpflichten handelt es sich um Sorgfaltspflichten.[1257] Dadurch, dass keine gefährlichen Produkte in Verkehr bleiben bzw. Konsumenten vor diesen gewarnt werden, werden die Sicherheit und die Gesundheit von Konsumenten und Dritten geschützt.[1258]

1254 Gerster, Rn. 130.

1255 Dazu a.A. Gerster, Rn. 311, der Art. 11 PrSG auch als Nachmarktpflicht kategorisiert, obwohl es sich bei Mitwirkungs- und Auskunftspflichten erst um Pflichten handelt, die auf konkrete Aufforderung der Behörden erfüllt werden müssen.

1256 Die Pflicht zur Sicherstellung der Rückverfolgung von Produkten befindet sich im allgemeinen Produktsicherheitsrecht der Schweiz zwar im 3. Abschnitt über die «Pflichten nach dem Inverkehrbringen», Art. 8 Abs. 2 lit. c PrSG. Trotzdem handelt es sich klar um eine Vorbereitungshandlung, die bereits vor Inverkehrbringung getätigt werden muss. Nur die sich aus Art. 8 Abs. 2 lit. c PrSG ergebende Aufbewahrungspflicht der Informationen zur Rückverfolgung ist eine Nachmarktpflicht, s. u., Rn. 383.

1257 Wildhaber/Rey, Rn. 1496; Gerster, Rn. 440, m.w.H. und konkret zu Art. 8 PrSG, Rn. 445.

1258 S. o., Rn. 267.

Wie oben ausgeführt, fallen Geräte mit integrierter Software (wie bspw. Smart Home Devices) unter verschiedene Spezialerlasse. Somit können auch die nachfolgenden Nachmarktpflichten nicht auf diese Produkte angewandt werden, ohne dass zuerst die Anwendbarkeit der leges speciales geprüft wird. Die Nachmarktpflichten aus dem PrSG und der GPSR gelten für Stand-alone-Software, da es sich dabei um ein selbstständiges Produkt handelt, welches – bis auf wenige Ausnahmen[1259] – nicht unter einen Spezialerlass fällt.[1260] Die einzige relevante Ausnahme in Bezug auf Smart Home Devices ist die KI-VO. Die KI-VO erfasst KI-Systeme und regelt deren Nachmarktpflichten. In der EU kann die GPSR deshalb nur auf KI-Systeme angewandt werden, wenn die KI-VO keine Regelung mit demselben Ziel enthält. Die Nachmarktpflichten der KI-VO haben also Vorrang gegenüber den Nachmarktpflichten der GPSR. Die GPSR wird jedoch ergänzend angewandt.[1261] Da es in der Schweiz keinen solchen Spezialerlass gibt, können die Nachmarktpflichten des PrSG auf alle Stand-alone-KI-Systeme (ausser im Medizinprodukterecht) angewandt werden. 306

Um die neue Regulierung der EU bezüglich Nachmarktpflichten für Hersteller von KI-Produkten mit den geltenden Schweizer Regelungen zu vergleichen, werden in diesem Kapitel die geltenden Nachmarktpflichten für Hersteller in der Schweiz und in der EU dargelegt. Verglichen werden konkret die europäischen Pflichten gem. GPSR sowie der KI-VO mit den schweizerischen Pflichten gem. PrSG. Diese werden vorliegend in folgende Kategorien eingeteilt: Gefahrenerkennungsmassnahmen bzw. Beobachtungspflichten, Gefahrenabwendungsmassnahmen, Melde- sowie Aufbewahrungs- und Aktualisierungspflichten. Nötig sind zuerst zwei Vorbemerkungen zur missbräuchlichen Verwendung von Produkten und zur Angemessenheit der Massnahmen, zu welchen Hersteller verpflichtet sind. 307

1259 In der Schweiz enthält das Medizinprodukterecht Regeln für Stand-alone-Software, s. o., Rn. 179. In der EU das Medizinprodukterecht (Rn. 179) und die neue Maschinenverordnung (Rn. 178), sowie die KI-VO, wenn es sich bei der Software um ein KI-System handelt.

1260 Verzichtet man auf eine Unterscheidung zwischen Embedded und Stand-alone-Software, können das PrSG und die GPSR auf jegliche Software angewandt werden, solange sie nicht durch Sektorrecht erfasst ist.

1261 S. o., Rn. 183.

I. Vorbemerkung 1: keine missbräuchliche Verwendung

308 Als Vorbemerkung sei festgehalten, dass der Hersteller keine Pflichten hat, wenn eine Gefahr durch eine missbräuchliche Verwendung (engl. «abuse») des Produktes droht. Er muss lediglich bei einer fehlerhaften Anwendung[1262] angemessene Massnahmen treffen. Bei einem Missbrauch ist er nicht verantwortlich und muss solche Gefahren weder erkennen[1263] noch sonst wie darauf reagieren. Obwohl die Voraussetzung der normalen oder vernünftigerweise vorhersehbaren Verwendung (engl. «intended use») für die Nachmarktpflichten im PrSG nur in Art. 8 Abs. 2 lit. a PrSG explizit festgehalten ist, muss für den Rest des Art. 8 PrSG dasselbe gelten. Art. 3 Abs. 1 PrSG hält den Grundsatz der vernünftigen vorhersehbaren Verwendung bereits für die Inverkehrbringung fest, weshalb auch für die Nachmarktpflichten nichts anderes gelten kann. Somit bezieht sich das Kriterium der Vorhersehbarkeit der Verwendung auch auf Art. 8 Abs. 2 lit. b PrSG (und lit. c, was aber keine Nachmarktpflicht ist) und auf Art. 8 Abs. 5 PrSG. Andernfalls müssten die Pflichten, für welche die «vernünftigerweise vorhersehbare Verwendung» nicht genannt ist, auch für die missbräuchliche Verwendung gelten. Es kann aber nicht davon ausgegangen werden, dass der Gesetzgeber wollte, dass die missbräuchliche Verwendung von Produkten in der Verantwortung des Herstellers liegt. Auch gem. der GPSR[1264] und der KI-VO verpflichtet die missbräuchliche Verwendung den Hersteller bzw. Anbieter nicht. Die KI-VO definiert die «vernünftigerweise vorhersehbare Fehlanwendung» in Art. 3 Ziff. 13 als «die Verwendung eines KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen, auch anderen KI-Systemen, ergeben kann». So müssen bspw. im Rahmen des Risikomanagementsystems nach Art. 9 Abs. 2 lit. b KI-VO lediglich Risiken beachtet werden, «wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird».[1265]

1262 S. o., Rn. 263.

1263 Siehe auch Botschaft PrSG, S. 7442, welche nur den «allfälligen Fehlgebrauch», jedoch nicht den Missbrauch nennt.

1264 NHK GPSR-Wiebe, Art. 5 N 24.

1265 S. u., Rn. 331.

II. Vorbemerkung 2: nur angemessene Massnahmen

Hersteller bzw. Anbieter sind zu angemessenen Massnahmen verpflichtet. 309
Konkret hält Art. 8 Abs. 2 PrSG fest, dass der Hersteller «im Rahmen seiner Geschäftstätigkeit[1266] angemessene Massnahmen treffen» muss.[1267] Gemeint ist damit, dass die zu treffenden Massnahmen verhältnismässig, also «geeignet und notwendig […], um die in Art. 1 PrSG anvisierte Produktsicherheit zu gewährleisten», sein müssen.[1268] Der Hersteller ist als privatwirtschaftlicher Akteur zwar nicht an den Verhältnismässigkeitsgrundsatz von Art. 5 Abs. 2 BV gebunden.[1269] Hält die zuständige Behörde die Massnahme aber für ungenügend, kann sie verhältnismässige[1270] Massnahmen verfügen.[1271] Auch im allgemeinen Produktsicherheitsrecht der EU müssen die vom Hersteller zu treffenden Massnahmen «in einem angemessenen Verhältnis zu der vom Produkt ausgehenden Gefahr stehen».[1272] Auch die KI-VO stellt an verschiedenen Orten auf die Angemessenheit von Massnahmen ab.[1273] So steht bspw. die Risikomanagementpflicht in einem angemessenen Verhältnis zum Risiko.[1274] Das heisst, dass Hersteller und Anbieter nicht zu jeder möglichen Massnahme verpflichtet sind, sondern «nur» zu angemessenen. Gleichzeitig dürfen sie aber auch nicht «irgendeine» Massnahme vornehmen, die nicht verhältnismässig zur Gefahr ist. Je grösser das Risiko ist, desto mehr oder intensivere Massnahmen sind angemessen.[1275] Für die Einschätzung der Gefahr wird bisweilen auch in der Schweizer Lehre auf die RAPEX-Leitlinie der EU verwiesen.[1276] Obwohl die Leitlinie an die Behörden der Mitgliedstaaten gerichtet war,[1277] kann sie auch

1266 S. o., Rn. 272.

1267 Ebenso wie für alle Nachmarktpflichten nach Art. 8 PrSG gilt, dass sie während der Gebrauchsdauer eines Produktes beachtet werden müssen, gilt auch für alle Nachmarktpflichten, dass diese angemessen sein müssen. S. o., Rn. 292. Siehe auch Holliger-Hagmann, Fallstricke, S. 160, in Bezug auf Art. 8 Abs. 3 PrSG.

1268 Fellmann, Jusletter 25.10.2010, Rn. 28; siehe auch SHK PrSG-Hess, Art. 8 N 13.

1269 SGK BV-Schindler, Art. 5 N 19; BSK BV-Epiney, Art. 5 N 33.

1270 BVGer C-3805/2020 vom 09.05.2022, E. 9.1; BVGer A-3085/2016 vom 26.06.2017, E. 3.3.7; BVGer C-914/2013 vom 06.10.2016, E. 5.2.1.1; BVGer A-727/2016 vom 13.07.2016, E. 8.1; BVGer C-6342/2013 vom 23.02.2015, E. 4.3; BGer 2C_905/2010 vom 22.03.2011, E. 3.3.1.

1271 Art. 10 Abs. 2 bis 4 PrSG.

1272 NHK GPSR-Piovano, Art. 9 N 99; siehe auch Piovano/Schucht/Wiebe, S. 96.

1273 Siehe bspw. Art. 9 Abs. 3, 4 und 5 lit. b sowie Art. 14 Abs. 3 KI-VO; siehe auch Beck KI-VO-Eisenberger, Art. 20 N 17.

1274 Beck KI-VO-Braun Binder/Egli, Art. 9 N 9.

1275 NHK GPSR-Wiebe, Art. 5 N 30, welcher dies die «Je-desto-Formel» nennt.

1276 Fellmann, Jusletter 25.10.2010, Rn. 44 ff.

1277 Europäische Kommission, RAPEX-Leitlinie, Anhang, Teil I, Ziff. 2.

dem Hersteller zur Risikobewertung dienen.[1278] Mit dem Wechsel von RAPEX zu Safety Gate wurde die RAPEX-Leitlinie ausser Kraft gesetzt.[1279] Gestützt auf die GPSR und ergänzend zur GPSR wurde eine «Delegierte Verordnung» (u.a.) mit Kriterien für die Bewertung des Risikoniveaus erlassen.[1280]

310 Für die Verhältnismässigkeitsprüfung einer zu treffenden Massnahme werden in der Schweizer Lehre die Grösse der Gefahr und der Erfolg der Massnahme gegen die Nachteile für den Hersteller bei Ergreifung der Massnahme abgewogen.[1281] Ob sich eine Gefahr noch im Rahmen des Zumutbaren befindet, hängt davon ab, ob Verwender und Dritte bei normaler oder bei vernünftigerweise vorhersehbarer Verwendung nicht oder nur gering gefährdet werden.[1282] Nicht mehr nur geringfügige Gefahren lösen eine Handlungspflicht[1283] des Herstellers aus.[1284] Tatsächlich als gefährlich (und damit als unsicher) gilt das Produkt erst, wenn die Gefahr nicht mehr toleriert wird.[1285] Was als eine noch tolerierte Gefahr akzeptiert wird, hängt von gesellschaftlichen Werten ab.[1286] Das von der Gesellschaft akzeptierte Risikoniveau gibt deshalb auch das Niveau der

1278 Siehe bspw. Fellmann, Jusletter 25.10.2010, Rn. 48, der die Meldepflicht der europäischen Hersteller von der Risikobewertung nach der Leitlinie abhängig macht; siehe auch Gerster, Rn. 208 Fn. 336.

1279 Europäische Kommission, Liste der förmlich aus dem Besitzstand zu streichenden Rechtsakte, ABl. C 2025/1229 vom 26.03.2025.

1280 Delegierte Verordnung (EU) 2024/3173 der Kommission vom 27. August 2024 zur Ergänzung der Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates um Vorschriften für den Zugang zum Schnellwarnsystem Safety Gate, den Betrieb des Systems, die in das System einzugebenden Informationen, die für Meldungen zu erfüllenden Anforderungen und die Kriterien für die Bewertung des Risikoniveaus, ABl. L 2024/3173 (zit. Delegierte VO (EU) 2024/3173), Anhang II, wobei gem. Ziff. 2.1. i.V.m. Art. 26 GPSR die Mitgliedstaaten und nicht die Hersteller Adressaten sind.

1281 SHK PrSG-Hess, Art. 8 N 13; ähnlich Fellmann, Jusletter 25.10.2010, Rn. 28; weniger detailliert Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 56; Bühler/Tobler, S. 175 f., mit Verweis auf Bodewig, S. 240, welcher sich auf das deutsche Recht bezieht. Siehe Abbildung 10.

1282 Art. 3 Abs. 1 PrSG; sog. «Bagatellgrenze» SHK PrSG-Hess, Art. 3 N 8 Fn. 11, m.w.H.; auch in Art. 3 Ziff. 2 GPSR ist eine Bagatellgrenze integriert, siehe dazu NHK GPSR-Wiebe, Art. 5 N 29.

1283 Im Gegensatz zum Haftpflichtrecht, wo es nötig ist, dass zuerst ein Schaden eintritt und die blosse Gefahr nicht ausreicht, Bühler, Bestandteil, S. 141; Haftpflichtkommentar-Holliger-Hagmann, Art. 3 PrSG N 1; für die EU siehe auch EuGH vom 21.10.2014, C-503/13, Boston Scientific Medizintechnik, ECLI:EU:C:2014:2306, Rn. 37, noch in Bezug auf die PLD 1985.

1284 Siehe bspw. die Meldepflicht nach Art. 8 Abs. 5 PrSG, Fellmann, Jusletter 25.10.2010, Rn. 39, 41.

1285 Für das PrSG SHK PrSG-Hess, Art. 3 N 7; für die GPSR NHK GPSR-Wiebe, Art. 5 N 29; ähnlich auch für die KI-VO Beck KI-VO-Braun Binder/Egli, Art. 9 N 34.

1286 Arioli, Jusletter IT 04.07.2024, Rn. 29; Beck KI-VO-Braun Binder/Egli, Art. 9 N 34.

Produktsicherheit vor,[1287] weshalb die zu treffenden Massnahmen des Herstellers von der «berechtigten Sicherheitserwartung»[1288] der Gefährdeten abhängig sind. In der Botschaft zum PrSG wird festgestellt, dass von mündigen Konsumenten ausgegangen werden kann, «die über das landesübliche Allgemeinwissen und Gefahrenbewusstsein verfügen».[1289] Auch in der EU wird von einem «durchschnittlich mündigen, informierten, aufmerksamen und verständigen» Verbraucher ausgegangen.[1290] Es stellt sich die Frage, inwieweit Konsumenten in der Nutzung von KI zur Selbstverantwortung befähigt und verpflichtet werden dürfen. Wenn Hersteller befugt sind, Produkte mit inhärentem Gefahrenpotenzial – wie etwa scharfe Messer – auf den Markt zu bringen, so sollte es grundsätzlich auch zulässig sein, persönliche digitale Assistenten oder vergleichbare Systeme auf den Markt zu bringen, selbst wenn diese ein gewisses Risiko mit sich bringen.[1291] Ob es sich um eine geringfügige Gefährdung handelt, ist schlussendlich abhängig vom Einzelfall[1292] und das Resultat einer Sicherheits- oder Risikobewertung.[1293]

1. Grösse der Gefahr und Erfolg der Massnahme

Um die potenzielle Schwere der Verletzung, also die Gefahr, welche von einem Produkt ausgeht, einzuschätzen, zählt bspw. HESS Art, Grad und Ursache der Gefahr auf. Zudem müsse evaluiert werden, wer gefährdet ist, wie hoch die Eintrittswahrscheinlichkeit der Gefahr ist und wie viele Produkte sich auf dem Markt befinden und verwendet werden.[1294] Die Grösse der Gefahr ergab sich bereits gem. RAPEX-Leitlinie aus dem Schweregrad und der Eintretenswahr- 311

1287 LOHSSE/SCHULZE/STAUDENMAYER, in: Lohsse/Schulze/Staudenmayer, Liability for AI, S. 10; SHK PrSG-HESS, Art. 3 N 9 im Kontext einer «wirtschaftlichen Betrachtungsweise», m.w.H. und Beispielen.

1288 Zum PrHG WILDHABER/REY, Rn. 1431.

1289 Botschaft PrSG, S. 7439; siehe auch BRUNNER, in: Fellmann/Furrer, Schonzeit, S. 77; mit Verweis auf die EU siehe auch BÜHLER/TOBLER, S. 394.

1290 NHK GPSR-WIEBE, Art. 6 N 23, mit Verweis auf EuGH vom 04.06.2015, C-195/14, Teekanne, ECLI:EU:C:2015:361, Rn. 36.

1291 Siehe auch FURRER, in: Fellmann/Furrer, Herausforderungen, S. 2.

1292 NHK GPSR-WIEBE, Art. 5 N 29; zu den «sehr schwierigen Wertungsfragen» bei der Feststellung des Sicherheitsniveaus siehe ausführlich NHK GPSR-WILRICH, Art. 3 N 41 f., m.w.H.; siehe auch Beck KI-VO-BRAUN BINDER/EGLI, Art. 9 N 34, m.w.H.

1293 Zur Je-desto-Formel s. o., Rn. 309 und zur Sicherheits- oder Risikobewertung sogleich, Rn. 311.

1294 SHK PrSG-HESS, Krisenmanagement N 44; siehe auch das Flowchart der RAPEX-Leitlinie: «describe the product unambigously, and its hazard(s)» und «identify consumer(s)» sowie «describe the Injury scenario», Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 67.

scheinlichkeit der erwarteten Rechtsgutverletzung.[1295] Die RAPEX-Leitlinie enthielt eine dreistufige Anleitung zur Risikobewertung:

312 Zunächst haben alle Produkte ein spezifisches Gefährdungspotenzial, auch inhärente Produktgefahr[1296] genannt.[1297] Es handelt sich dabei um die potenzielle Schwere der Verletzung, die durch das Produkt ausgelöst werden kann.[1298] Um festzustellen, wie gross das Gefährdungspotenzial ist, muss der Hersteller eine Risikoanalyse vornehmen.[1299] Als Orientierungshilfe zur Einschätzung des Schweregrads einer Verletzung kann die Tabelle 3 (siehe sogleich) in der RAPEX-Leitlinie dienen.[1300] Kriterien zur Quantifizierung der Gefahr sind neben dem Schweregrad der möglichen Verletzung z.B. die Handhabung des Produktes durch Verbraucher oder die Verbraucherkategorien.[1301] In einem zweiten Schritt muss die Eintretenswahrscheinlichkeit der drohenden Gefährdung berücksichtigt werden.[1302] Diese wird als Bruch oder in Prozent angegeben.[1303] Zuletzt wird in einem dritten Schritt «die Gefahr (als Schweregrad der Verletzung) mit der Wahrscheinlichkeit» kombiniert.[1304] SEILER bringt es auf den Punkt: «je gravierender die Rechtsgutverletzung (d.h.: je hochwertiger das beeinträchtige Rechtsgut und/oder je intensiver die Verletzung dieses Rechtsgutes), eine desto kleinere Wahrscheinlichkeit genügt bereits, um von einer Gefahr im Rechtssinne zu sprechen».[1305] Zur Ermittlung des Risikograds «als Resultat der Kombination aus Schweregrad der Verletzung und Wahrscheinlichkeit» wird in der Leitlinie ebenfalls eine Tabelle zur Verfügung gestellt.[1306]

1295 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 48.
1296 S. o. zu den verschiedenen Arten von Gefahren, Rn. 261.
1297 Die RAPEX-Leitlinie bezeichnet dies als die innewohnende oder inhärente Gefahr eines Produktes, Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 47 f.; SEILER, S. 154, welcher dies die «relative Gefährlichkeit» nennt; siehe auch Art. 3 Abs. 4 PrSG.
1298 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 55.
1299 SHK PrSG-HESS, Art. 3 N 44.
1300 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 81, Tabelle 3.
1301 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 48.
1302 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 48.
1303 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 48.
1304 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 48.
1305 SEILER, S. 154, m.w.H.
1306 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 82, Tabelle 4.

Tabelle 3: *Auszug aus Tabelle 3 der RAPEX-Leitlinie*[1307]

Art der Verletzung	Schweregrad der Verletzung			
	1	2	3	4
Riss-/Schnittverletzung	Oberflächlich	Äußerlich (tief) (> 10 cm lang, am Körper) (> 5 cm lang, im Gesicht), Nähen erforderlich Sehne oder in Gelenk Augapfel oder Hornhaut	Sehnerv Halsschlagader Luftröhre Innere Organe	Bronchien Speiseröhre Aorta Rückenmark (unterer Bereich) Tiefe Rissverletzung innerer Organe Durchtrennung des oberen Rückenmarks Gehirn (schwere Schädigung/Funktionsstörung)

Ebenfalls als Kriterium für die Grösse der Gefahr werden die Häufigkeit der Rechtsgutverletzungen[1308] und die Anzahl der in Verkehr gebrachten Produkte[1309] genannt. Je grösser die Anzahl in Verkehr gebrachter Produkte ist, desto grösser ist die Anzahl potenziell gefährdeter Personen. Da das PrSG nicht nur die Gesundheit und Sicherheit der Allgemeinheit schützt, sondern auch jene von Individuen,[1310] darf nach vorliegend vertretener Meinung die Anzahl in Verkehr gebrachter Produkte und somit die Anzahl gefährdeter Personen nicht pauschal als Kriterium verwendet werden, da bereits ein einziges unsicheres Produkt zum Tod einer oder mehrerer Personen führen kann.[1311] In Bezug auf die Gefahren*erkennungs*massnahmen kann es Sinn ergeben, die Anzahl der potenziell gefährdeten Personen in die Risikoanalyse einzubeziehen. Sind weniger Produkte in Verkehr gebracht worden, ist die Wahrscheinlichkeit kleiner, dass sich eine Gefahr überhaupt zeigt (niedrige Eintretenswahrscheinlichkeit), selbst wenn sie in einem Anteil der Produkte «schlummert». Selbst wenn also aktiv nach Nachrichten über gefährliche Produkte gesucht wird und diese auch existieren, kann es sein, dass sich niemand die Mühe gemacht hat, mit Informationen über diese Gefahren an die Öffentlichkeit zu treten. In Be- 313

1307 Europäische Kommission, Konsolidierte RAPEX-Leitlinie, S. 78, Tabelle 3.

1308 Bezogen auf Rückrufmassnahmen Bühler/Tobler, S. 175 f., mit Verweis auf Bodewig, S. 240, der sich auf das deutsche Recht bezieht.

1309 In Bezug auf die Gefahrenerkennung: Botschaft PrSG, S. 7441; SHK PrSG-Hess, Art. 8 N 18; für die EU Piovano/Schucht/Wiebe, S. 95.

1310 S. o., Rn. 267.

1311 Ebenfalls differenzierend Gerster, welcher in Rn. 277 bezüglich der Gefahrenerkennungsmassnahmen die Anzahl in Verkehr gebrachter Produkte als sinnvolles Kriterium erachtet, sich in Rn. 352 (zwar im Kontext von Art. 10 Abs. 3 lit. d PrSG, aber im Ergebnis gleich) indes dagegen ausspricht, die Anzahl gefährdeter Personen als Kriterium für eine «unmittelbare» und «ernste» Gefahr heranzuziehen.

zug auf die Gefahren*abwendungs*massnahmen sollte die Anzahl in Verkehr gebrachter Produkte bzw. gefährdeter Personen jedoch kein Kriterium dafür sein, *ob* eine Massnahme getroffen werden sollte. Bspw. ist bei sehr vielen, aber nur leicht gefährdeten Personen eine schwerwiegende Massnahme (wie z.B. der Rückruf eines Produktes) nicht sinnvoller als bei wenigen gefährdeten Personen.[1312] Umgekehrt kann bereits eine einzige besonders schwerwiegend gefährdete Person eine für den Hersteller stark einschneidende Massnahme rechtfertigen, wenn die Gefahr aufgrund weiterer Produkte noch immer besteht. Anzumerken ist deshalb Folgendes: *Ob* eine Gefahren*abwendungs*massnahme getroffen wird, sollte nicht von der Anzahl abhängen, aber *welche* Massnahme getroffen wird, kann durchaus davon abhängen.[1313] Für weitere Hinweise zur Bestimmung von Massnahmen verweisen die Botschaft sowie die Lehre auf die Normenreihe SN EN ISO 9000ff. zur Qualitätssicherung.[1314]

314 Art. 6 GPSR listet Aspekte für die Bewertung der Sicherheit von Produkten auf. Diese beinhalten die Eigenschaften des Produktes (lit. a), seine Einwirkung auf andere Produkte (lit. b), die mögliche Einwirkung anderer Produkte auf das zu bewertende Produkt (lit. c), die Aufmachung des Produktes (lit. d), die Verbraucherkategorien, die das Produkt verwenden (lit. e), das Erscheinungsbild des Produktes (lit. f), Cybersicherheitsmerkmale (lit. g) und KI-Funktionen (lit. h). Diese Aspekte dienen als Anhaltspunkte dafür, wann Nachmarktpflichten vorzunehmen sind.[1315] Unter anderem gestützt auf Art. 26 Abs. 10 GPSR hat die Europäische Kommission zudem einen delegierten Rechtsakt[1316] erlassen, der Kriterien für die Bewertung des Risikoniveaus liefert.[1317] Die Methodik richtet sich wie bei der alten RAPEX-Leitlinie an die Behörden der EU-Mitgliedstaaten,[1318] kann jedoch wieder als Anhaltspunkt für Hersteller und Anbieter dienen. Die Bewertung des Risikoniveaus berücksichtigt die Eintretenswahrscheinlichkeit und «wie bestimmte Gefahren zu potenziellen Schäden führen können».[1319] Für die Bewertung des Risikoniveaus muss zuerst ein Schadensszenario mit einer Beschreibung der Gefahr und des Schweregrads des (potenziell) verursachten Schadens erstellt werden.[1320] Danach müssen die

1312 Zu den Gefahrenabwendungsmassnahmen s. u., Rn. 349 ff.
1313 Siehe dazu auch den Praxishinweis zur Anzahl in Piovano/Schucht/Wiebe, S. 95.
1314 Botschaft PrSG, S. 7441; Gerster, Rn. 277, m.w.H.; SHK PrSG-Hess, Art. 8 N 18; Fellmann, Jusletter 25.10.2010, Rn. 24.
1315 NHK GPSR-Wiebe, Art. 6 N 7.
1316 Delegierte VO (EU) 2024/3173.
1317 Art. 2 Delegierte VO (EU) 2024/3173.
1318 Siehe auch ErwG 10 Delegierte VO (EU) 2024/3173.
1319 Anhang II, Ziff. 3 lit. a und b Delegierte VO (EU) 2024/3173.
1320 Anhang II, Ziff. 3.1.2 Delegierte VO (EU) 2024/3173.

Schritte des Schadensszenarios aufgezeigt werden, die zum Schaden führen.[1321] Für die Analyse des Schweregrads der Verletzung oder des Schadens für die Gesundheit und Sicherheit wird eine Reihe von Faktoren aufgezählt. Dazu gehören bspw. die Art und das Ausmass der Gefahr, der verletzte Körperteil und die Verbraucherkategorie.[1322] Der Schweregrad wird in vier Schadensniveaus eingeteilt, die von geringfügig (Stufe 1) bis lebensbedrohlich (Stufe 4) reichen.[1323] Der Schweregrad wird dann mit der Eintretenswahrscheinlichkeit kombiniert, um das Risikoniveau zu bestimmen.[1324] Für die «Wahrscheinlichkeit des Eintretens des Schadensszenarios während der vorhersehbaren Lebensdauer des Produktes» wird eine Tabelle zur Verfügung gestellt mit quantitativen (1/1'000'000 oder geringer bis 50 % oder höher) und qualitativen Angaben (äusserst selten bis sehr häufig).[1325] Das zu ermittelnde Risikoniveau wird in vier Stufen von niedrigem Risiko bis ernstem Risiko eingeteilt (siehe dazu Tabelle 4). Die Tabelle zur Bestimmung des Risikoniveaus ist fast deckungsgleich mit der Tabelle 3 der RAPEX-Leitlinie.

1321 Anhang II, Ziff. 3.2 Delegierte VO (EU) 2024/3173.
1322 Anhang II, Ziff. 3.3.1 Delegierte VO (EU) 2024/3173.
1323 Anhang II, Ziff. 3.3.3 Delegierte VO (EU) 2024/3173, mit Tabelle und weiterführenden Kriterien.
1324 Anhang II, Ziff. 3.6.1 Delegierte VO (EU) 2024/3173.
1325 Anhang II, Ziff. 3.4.4 und 3.5 Delegierte VO (EU) 2024/3173.

315 ***Tabelle 4:*** *Tabelle zur Bestimmung des Risikoniveaus*[1326]

Wahrscheinlichkeit einer Schädigung während der voraussichtlichen Lebensdauer des Produkts		Schweregrad der Verletzung			
		1	2	3	4
Hoch	>50 %	H	E	E	E
	> 1/10	M	E	E	E
	> 1/100	M	E	E	E
	> 1/1000	N	H	E	E
	> 1/10 000	N	M	H	E
	> 1/100 000	N	N	M	H
	> 1/1 000 000	N	N	N	M
Gering	< 1/1 000 000	N	N	N	N

E — Ernstes Risiko
H — Hohes Risiko
M — Mittleres Risiko
N — Niedriges Risiko

316 Als Nebenbemerkung sei festgehalten, dass zwischen der nicht geringfügigen und der ernsten Gefahr bzw. einem (qualifizierten) Risiko und einem ernsten Risiko unterschieden werden kann. Eine ernste und unmittelbare Gefahr legitimiert nach Art. 10 Abs. 3 lit. d PrSG die Vollzugsorgane zu besonderen Massnahmen. Dasselbe gilt für die europäischen Marktüberwachungsbehörden bei ernsten Risiken gem. Art. 3 Ziff. 4 GPSR und Art. 3 Ziff. 20 MÜVO. Der Hersteller ist jedoch nicht erst bei einer ernsten Gefahr verpflichtet, sondern bereits bei einer nicht mehr geringfügigen Gefahr.

317 Die Angemessenheit einer Massnahme richtet sich zudem nach ihrem voraussichtlichen Erfolg, also ihrer Eignung zur wirksamen Abwendung der Gefahr. Der Inverkehrbringer muss daher auch beachten, welche Massnahmen die Gefahren am effektivsten verhindern.[1327]

1326 Anhang II, Ziff. 3.6.2 inklusive Tabelle Delegierte VO (EU) 2024/3173.

1327 SHK PrSG-Hess, Art. 8 N 13; siehe auch Bühler/Tobler, S. 176, mit Verweis auf Bodewig, S. 240, zum deutschen Recht; für die EU siehe Piovano/Schucht/Wiebe, S. 96.

2. Nachteile des Herstellers

Der Hersteller darf bei der Verhältnismässigkeitsprüfung der Massnahme wirtschaftliche Elemente berücksichtigen.[1328] Hess nennt bspw. «den Kaufpreis und die Betriebskosten».[1329] Die Berücksichtigung der Nachteile des Herstellers ist sinnvoll, da eine geringfügige Gefährdung durch Produkte generell zulässig ist.[1330] Die Nachteile des Herstellers dürfen zwar berücksichtigt, aber im Verhältnis zu den anderen Kriterien nicht zu stark gewichtet werden, da sonst nicht sichergestellt werden könnte, dass nur sichere Produkte (einer der wichtigsten Zwecke des Produktsicherheitsrechts) auf dem Markt sind.[1331] 318

3. Zusammenfassung der Vorbemerkungen

Die produktsicherheitsrechtlichen Nachmarktpflichten setzen sich aus Gefahrenerkennungsmassnahmen bzw. der Beobachtung nach der Inverkehrbringung, Gefahrenabwendungsmassnahmen, Melde- sowie Aufbewahrungs- und Aktualisierungspflichten zusammen und sind nach der Inverkehrbringung eines Produktes zu erfüllen. 319

Nachmarktpflichten sind nur bei einer vernünftigerweise vorhersehbaren Verwendung des Produktes zu beachten, da den Hersteller bei einer missbräuchlichen Verwendung keine Verantwortung für sein Produkt trifft. 320

Hersteller müssen im Rahmen der Nachmarktpflichten angemessene Massnahmen treffen. Je höher das Risiko, desto weiterreichende Massnahmen sind angemessen. Ob eine Massnahme angemessen ist, ergibt sich aus der Grösse der Gefahr und dem erwarteten Erfolg der Massnahme, wobei auch die Nachteile für den Hersteller berücksichtigt werden dürfen. Eine Bagatellgrenze bewirkt, dass nur geringfügige Gefahren keine Pflicht zur Ergreifung von Massnahmen auslösen. Was als nicht mehr geringfügige und somit nicht mehr tolerierte Gefahr gilt, ist abhängig vom gesellschaftlich akzeptierten Risikoniveau und das Resultat einer einzelfallbezogenen Risikobewertung. Herstellern wird in der Schweizer Lehre auch hierzulande die Risikobewertung nach der RAPEX-Leitlinie der EU nahegelegt. Diese Leitlinie wurde 2024 zur Ergänzung 321

1328 SHK PrSG-Hess, Art. 3 N 9; Bühler/Tobler, S. 176, mit Verweis auf Bodewig, S. 240, zum deutschen Recht; für die EU: NHK GPSR-Wiebe, Art. 5 N 30; Piovano/Schucht/Wiebe, S. 96.

1329 SHK PrSG-Hess, Art. 3 N 9.

1330 Zur Bagatellgrenze s. o., Rn. 310.

1331 NHK GPSR-Wiebe, Art. 5 N 30; Schmid, Pflicht, Rn. 30; ähnlich jedoch noch vor Entstehung des PrSG Röthlisberger, S. 34.

der GPSR durch neue Kriterien für die Bewertung des Risikoniveaus abgelöst. Es wird damit gerechnet, dass sich zukünftig auch in der Schweiz an dieser neuen Risikoanalysemethode orientiert wird.

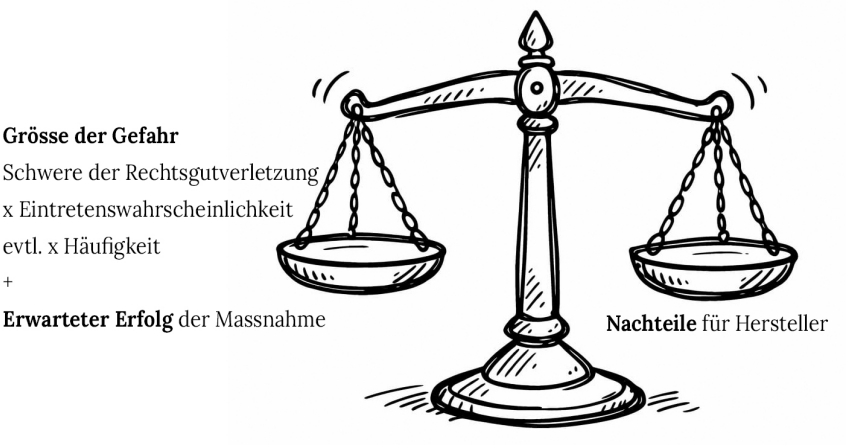

Abbildung 8: *Abwägung der Verhältnismässigkeit einer Massnahme*

III. Gefahrenerkennungsmassnahmen

322 Um Gefahren rechtzeitig zu erkennen, müssen Hersteller ihre Produkte nach der Inverkehrbringung beobachten. Massnahmen zur Produktbeobachtung dienen der Erkennung von Gefahren, die sich erst *nach* dem Inverkehrbringen zeigen.[1332] Alle Gefahren, welche schon *vor* dem Inverkehrbringen erkannt werden können, müssen auch in diesem Zeitraum bereits beseitigt werden. Unterschieden werden eine aktive und eine passive Produktbeobachtungspflicht.

323 Aufgrund der (technischen) Opazität[1333] von KI-Systemen kann es schwierig sein, Gefahren überhaupt zu erkennen, was deren Produktbeobachtung so wichtig macht.[1334] Die technische Opazität (KI-System als «Black Box») ist ein Hindernis bei der Gefahrenerkennung. Lässt ein Anbieter ein KI-System entwickeln und erhält vom Entwickler nicht alle Informationen darüber («strategische Opazität»), wird ihm auch die Gefahrenerkennung erschwert, selbst

1332 Botschaft PrSG, S. 7441; SHK PrSG-Hess, Art. 8 N 17; Fellmann, Jusletter 25.10.2010, Rn. 29.
1333 S. o., Rn. 47 f.
1334 Mit Bezug zur Produkthaftung McGuire, in: Foerste/Westphalen, § 58 Rn. 39, m.w.H.

wenn die Dokumentation zum System weitergegeben wird. Anbieter werden kein Problem mit dieser Art von Opazität haben, wenn sie das KI-System selbst entwickelt haben.

1. Aktive Beobachtungspflicht

Eine aktive Produktbeobachtungspflicht ist – im Gegensatz zur passiven Produktbeobachtungspflicht[1335] – die Pflicht, eigene Nachforschungen über seine und konkurrenzierende[1336] Produkte zu betreiben. Sie ist im PrSG in Art. 8 Abs. 2 lit. a PrSG und in der KI-VO in Art. 72 KI-VO und Art. 9 Abs. 2 KI-VO geregelt. Die Erkennung von Gefahren war in der Produktsicherheitsrichtlinie in Art. 5 Abs. 1 Uabs. 3 lit. a Produktsicherheitsrichtlinie ebenfalls vorgeschrieben. Im Gegensatz zur Produktsicherheitsrichtlinie verpflichtet die GPSR nicht mehr zu einer aktiven Produktbeobachtung.[1337] Auch die Pflicht zur Durchführung von Stichproben für in Verkehr gebrachte Produkte (sofern diese zweckmässig war) gem. Art. 5 Abs. 1 Uabs. 4 lit. b Produktsicherheitsrichtlinie ist in der GPSR entfallen.[1338] 324

1.1. Klassische aktive Produktbeobachtung

Nach Art. 8 Abs. 2 lit. a PrSG haben Hersteller, die ein Produkt in Verkehr gebracht haben, die Pflicht, angemessene Massnahmen zu treffen, um Gefahren zu erkennen, die von dem Produkt bei normaler oder bei vernünftigerweise vorhersehbarer Verwendung ausgehen können. Das PrSG verpflichtet den Hersteller somit zu Massnahmen, die die Erkennung von Gefahren im Rahmen einer aktiven Produktbeobachtung ermöglichen.[1339] Konkret reicht es somit nicht, Meldungen aus Reklamationen oder sonstigen Hinweisen nachzugehen (sog. passive Produktbeobachtungspflicht). Stattdessen müssen die Verpflichteten eigene Nachforschungen betreiben.[1340] Eine klassische aktive Produktbeobachtungspflicht besteht auch nach Art. 9 Abs. 2 lit. a KI-VO.[1341] 325

1335 S. u., Rn. 339 ff.

1336 Botschaft PrSG, S. 7442; siehe auch Schmid, Pflicht, Rn. 8, zum deutschen Recht.

1337 Piovano/Schucht/Wiebe, S. 152.

1338 Piovano/Schucht/Wiebe, S. 152; NHK GPSR-Piovano, Art. 9 N 148.

1339 Gerster, Rn. 278 Fn. 444, m.w.H.; Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 5; SHK PrSG-Hess, Art. 8 N 20; Fellmann, Jusletter 25.10.2010, Rn. 25.

1340 SHK PrSG-Hess, Art. 8 N 20; Hess zustimmend Fellmann, Jusletter 25.10.2010, Rn. 25.

1341 S. u., Rn. 331.

326 Das PrSG schreibt keine konkreten Massnahmen zur aktiven Gefahrenerkennung vor. Als mögliche Massnahmen zur Gefahrenerkennung werden u.a. das Durchsuchen von Medien nach Meldungen[1342] über das betreffende Produkt sowie die Registrierung dieser Meldungen,[1343] die Konsultation der RAPEX-Liste[1344] mit gefährlichen Produkten[1345] und das Lesen von «Fachlektüre»[1346] genannt. Im Bereich von Software könnte die Produktbeobachtung insbesondere die laufende Überprüfung technischer Informationen zu verwendeten Softwarekomponenten, wie etwa Änderungsprotokollen (Release Notes), bekannten Fehlermeldungen in Entwicklerforen und Supportdatenbanken oder Einträgen in sog. «Issue Trackern» (z.B. GitHub Issues) umfassen. Hersteller sollten beobachten, ob Updates, Systemänderungen oder Kompatibilitätsprobleme eine Fehlfunktion oder ein sicherheitsrelevantes Verhalten des Produktes verursachen könnten. Aus Art. 8 Abs. 2 lit. a PrSG kann auch das Durchführen von Stichproben als geeignete Massnahme zur Gefahrenerkennung abgeleitet werden.[1347] Es handelt sich jedoch nach vorliegend vertretener Meinung nicht um eine zwingende Pflicht, sondern nur um eine mögliche geeignete Präventivmassnahme, um Gefahren zu erkennen.[1348] Stichproben von nicht beanstandeten Produkten sind – unabhängig davon, ob eine gesetzliche Pflicht besteht – mindestens empfohlen.[1349] Eine Pflicht für den Hersteller, Stichproben durchzuführen, gilt mindestens nach erfolgter Beanstandung der Sicherheit eines Produktes gem. Art. 8 Abs. 3 PrSG.[1350] Die Produktbeobachtungspflicht[1351] nach dem PrSG beinhaltet nicht nur das eigene Produkt, son-

1342 Botschaft PrSG, S. 7442; siehe auch: Gerster, Rn. 278; SHK PrSG-Hess, Art. 8 N 17; Fellmann, Jusletter 25.10.2010, Rn. 26.

1343 SHK PrSG-Hess, Art. 8 N 20.

1344 Diese wurde ersetzt durch das Safety Gate, s. u., Rn. 376.

1345 Gerster, Rn. 280; Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 5.

1346 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 5.

1347 Fellmann, Jusletter 25.10.2010, Rn. 37; SHK PrSG-Hess, Art. 8 N 31; Gerster, Rn. 288 f.

1348 Gl.M. wohl Holliger-Hagmann, Fallstricke, 164 ff., welche die Stichproben ausschliesslich in ihrer Kommentierung zu Art. 8 Abs. 3 PrSG erwähnt; ebenso in Holliger-Hagmann, Produktsicherheit und Haftpflicht, S. 52; ebenfalls gl.M. wohl: Bühler, Bestandteil, S. 87; SHK PrSG-Hess, Art. 8 N 31, der die Stichproben nur unter Art. 8 Abs. 3 PrSG behandelt; a.A.: Fellmann, Jusletter 25.10.2010, Rn. 37, spricht sich «unter bestimmten Umständen» für eine Pflicht zu Stichproben nach Art. 8 Abs. 2 lit. a PrSG aus. Nach dieser Argumentation müsste man aber jede geeignete Massnahme als Pflicht anerkennen. M.E. kann der Hersteller selbst geeignete Massnahmen festlegen und muss nicht zwingend Stichproben durchführen; Gerster, Rn. 289.

1349 SHK PrSG-Hess, Art. 8 N 31.

1350 S. u., Rn. 343.

1351 Wie Schmid richtigerweise feststellt, handelt es sich bei der klassischen *Produkt*beobachtung eigentlich um eine *Markt*beobachtung. Dies ändert sich jedoch bei der integrierten Produktbeobachtung, bei welcher das System via Internet Auffälligkeiten direkt an den

dern auch ähnliche Produkte anderer Hersteller aus der Schweiz und dem Ausland oder Produkte, welche «mit möglicherweise gleichem Material, Teilen oder Zubehör» hergestellt wurden.[1352] Wird also bspw. bekannt, dass ein Trainingsdatensatz oder bestimmte KI-Modelle problematisch sind, müssen Hersteller, die diese Datensätze oder Modelle verwendet haben, aufmerksam werden.

1.2. Integrierte aktive Produktbeobachtung

Im Gegensatz zu herkömmlichen Produkten haben Hersteller von Software, die weiterhin mit dem Hersteller in Verbindung steht, die Möglichkeit, kontinuierlich und in Echtzeit Rückmeldungen über ihre Produkte zu erhalten.[1353] Geräte mit Embedded und Stand-alone-Software können so konfiguriert werden, dass sie Abweichungen des aktuellen Systemzustandes vom vorgegebenen Sollzustand transparent machen.[1354] Dies trifft auch auf KI-Systeme und Produkte mit integrierten KI-Systemen zu. Die integrierte Produktbeobachtung bei nach der Inverkehrbringung weiterlernenden KI-Systemen ist besonders wichtig, da diese sich schnell und unvorhergesehen verändern können.[1355] Dies ermöglicht die automatische Erkennung von ungewöhnlichen Betriebszuständen.[1356] SCHMID behandelt diese Möglichkeit als eine zusätzliche Kategorie zur aktiven und passiven Produktbeobachtung und nennt sie «integrierte Produktbeobachtung».[1357] Vorliegend wird die integrierte Produktbeobachtung zur aktiven Produktbeobachtung gezählt. Bei der technischen Vorbereitung zur Ermöglichung der integrierten Produktbeobachtung handelt es sich zwar um eine Tätigkeit, die bereits vor der Inverkehrbringung bei der Konzeption des Produktes stattfinden muss, aber die Auswertung der gesammelten Daten ist eine aktive Produktbeobachtung. Da die klassische aktive Produktbeobachtung auf öffentliche Quellen beschränkt ist und auch nicht alle Gefahren gemeldet werden, wird für diese Art und für die passive Produktbeobach- 327

Hersteller schicken kann, SCHMID, Pflicht, Rn. 9. Deshalb und weil es sich um einen etablierten Begriff handelt, wird vorliegend weiterhin der Begriff «Produktbeobachtung» verwendet.

1352 Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 8 PrSG N 5; siehe auch: Botschaft PrSG, S. 7442; FELLMANN, Jusletter 25.10.2010, Rn. 26; SHK PrSG-HESS, Art. 8 N 20.

1353 OSTER, in: Foerste/Westphalen, § 57 Rn. 25; PIOVANO/SCHUCHT/WIEBE, S. 91.

1354 SCHMID, Pflicht, Rn. 11.

1355 Siehe auch PIOVANO/SCHUCHT/WIEBE, S. 92 f.

1356 SCHMID, Pflicht, Rn. 11.

1357 SCHMID, Pflicht, passim, zum deutschen Recht; ebenfalls ausführlich in seiner Dissertation SCHMID, IT, insbesondere S. 205; siehe auch mit Bezug auf SCHMID PIOVANO/SCHUCHT/WIEBE, S. 91, welche dies «remote-Produktbeobachtung» nennen.

tung eine hohe Dunkelziffer vermutet.[1358] Ausserdem können Nachforschungen und Meldungen relativ lange dauern.[1359] Ein weiterer Nachteil der klassischen Beobachtungspflichten ist, dass sich eine Gefahr zuerst manifestieren muss, damit sie bemerkt werden kann.[1360]

328 Eine Pflicht zur aktiven integrierten Produktbeobachtung kann dem PrSG nicht entnommen werden. Die aktive integrierte Produktbeobachtung könnte aber aufgrund der unvorhersehbaren Tendenzen von KI-Systemen eine angemessene Massnahme zur Erkennung von Gefahren nach Art. 8 Abs. 2 lit. a PrSG darstellen.[1361] Es handelt sich dabei um eine Einzelfallabwägung aufgrund der möglichen Gefahren und der zu tätigenden Aufwände des Herstellers. Eine Pflicht zur aktiven integrierten Produktbeobachtung besteht jedoch für Anbieter von Hochrisiko-KI-Systemen. Diese müssen ihre Systeme nach der Inverkehrbringung gem. Art. 72 Abs. 1 KI-VO überwachen. Dazu ist eine automatische Aufzeichnung von Ereignissen nötig.[1362]

a. System zur Beobachtung nach dem Inverkehrbringen

329 Art. 72 Abs. 2 KI-VO fordert ein «System zur Beobachtung nach dem Inverkehrbringen». Dieses System zur Beobachtung nach dem Inverkehrbringen wird in Art. 3 Ziff. 25 KI-VO definiert als die Gesamtheit aller «Tätigkeiten, die Anbieter von KI-Systemen zur Sammlung und Überprüfung von Erfahrungen mit der Verwendung der von ihnen in Verkehr gebrachten oder in Betrieb genommenen KI-Systeme durchführen, um festzustellen, ob unverzüglich nötige Korrektur- oder Präventivmassnahmen zu ergreifen sind». Auch wenn sich die Definition nach Art. 3 Ziff. 25 KI-VO auf alle KI-Systeme bezieht, gilt die Verpflichtung zur Führung eines solchen Beobachtungssystems nur für Anbieter von Hochrisiko-KI-Systemen gem. Art. 72 KI-VO.[1363] Mit dem nach Art. 72 Abs. 2 KI-VO geforderten System müssen sich die einschlägigen Daten zur Leistung der Hochrisiko-KI-Systeme, die von den Anbietern oder den Betreibern bereitgestellt oder aus anderen Quellen erhoben werden können, über ihre gesamte Lebensdauer hinweg aktiv und systematisch erheben, dokumentieren und analysieren lassen. Die Daten können vom Anbieter selbst kommen oder von Betreibern oder anderen Quellen erhoben werden.[1364] Bei den zu er-

1358 Schmid, Pflicht, Rn. 9.
1359 Schmid, Pflicht, Rn. 9.
1360 Schmid, Pflicht, Rn. 9.
1361 Ähnlich siehe auch Lohmann, Haftungsrahmen, S. 118.
1362 Art. 12 Abs. 1 i.V.m. Abs. 2 lit. b KI-VO.
1363 Feiler/Forgó, Art. 72 N 3; siehe auch Beck KI-VO-Hartmann, Art. 72 N 10.
1364 Art. 72 Abs. 2 KI-VO.

hebenden Daten handelt es sich um Daten über die «Leistung eines KI-Systems», welche in Art. 3 Ziff. 18 KI-VO als «Fähigkeit des KI-Systems seine Zweckbestimmung zu erfüllen» definiert wird.[1365] Das Beobachtungssystem und die Dokumentation müssen im Verhältnis zu den Risiken und der Art der KI-Technik stehen.[1366] Das heisst, es werden wieder «angemessene Massnahmen» verlangt. Das Beobachtungssystem dient vor allem dazu, «möglichen Risiken, die von KI-Systemen ausgehen, die nach dem Inverkehrbringen oder der Inbetriebnahme dazulernen» zu begegnen.[1367] Dies soll jedoch nicht heissen, dass Gefahren, die schon vor der Inverkehrbringung hätten erkannt werden können, ignoriert werden dürfen. Auch wenn Art. 72 KI-VO nicht darauf hinweist, muss hier unter «Inverkehrbringung» auch die Inbetriebnahme mitverstanden werden.[1368]

b. Risikomanagementsystem und Protokollierungspflicht

Weiter muss der Anbieter gem. Art. 72 Abs. 2 KI-VO mit dem System zur Beobachtung «die fortdauernde Einhaltung der in Kapitel III Abschnitt 2 genannten Anforderungen an die KI-Systeme bewerten können». Damit rechtzeitig erkennbar wird, ob Korrektur- oder Präventivmassnahmen nötig sind, muss diese Bewertung fortlaufend erfolgen.[1369] Die in Kapitel III Abschnitt 2 enthaltenen Anforderungen sind in Art. 8 bis 15 KI-VO geregelt. Art. 8, 10 und 13 KI-VO enthalten keine Nachmarktpflichten. Art. 11 Abs. 1 KI-VO enthält die Pflicht, dass die technische Dokumentation, die vor dem Inverkehrbringen bzw. vor der Inbetriebnahme des KI-Systems erstellt werden muss, auf dem neusten Stand gehalten wird. Art. 14 KI-VO regelt die menschliche Aufsicht («human in the loop», «human on the loop», «human in command»)[1370] von Hochrisiko-KI-Systemen, für welche die Vorkehrungen bereits vor der Inverkehrbringung bzw. Inbetriebnahme getroffen werden müssen.[1371] Auf die Cybersicherheit, die in Art. 15 KI-VO verlangt wird, soll hier nicht weiter eingegangen werden.[1372] Es handelt sich bei den Vorschriften in Kapitel III Abschnitt 2 somit vor

330

1365 Beck KI-VO-Hartmann, Art. 72 N 13.

1366 Art. 72 Abs. 1 KI-VO; siehe auch Beck KI-VO-Hartmann, Art. 72 N 1.

1367 ErwG 155 KI-VO.

1368 Die Definition in Art. 3 Ziff. 25 KI-VO erfasst die Inbetriebnahme ebenfalls.

1369 Beck KI-VO-Hartmann, Art. 72 N 11.

1370 Beck KI-VO-Martini, Art. 14 N 25.

1371 Art. 14 Abs. 3 KI-VO.

1372 Art. 15 Abs. 1 KI-VO verlangt, dass Hochrisiko-KI-Systeme während ihres gesamten Lebenszyklus ein angemessenes Mass an Genauigkeit, Robustheit und Cybersicherheit aufrechterhalten. Art. 15 Abs. 5 Uabs. 3 KI-VO verlangt, dass Angriffe auf das Hochrisiko-

allem um Vormarktpflichten, welche teilweise auch Nachmarktpflichten beinhalten. Da in Art. 9 Abs. 2 lit. c und Art. 12 Abs. 2 lit. b KI-VO auf Art. 72 KI-VO referenziert wird und diese Bestimmungen für die Beobachtung relevant sind, wird nachfolgend auf diese zwei Bestimmungen eingegangen.

331 Die möglicherweise auftretenden Risiken auf der Grundlage der Auswertung der Daten aus dem System zur Beobachtung nach Art. 72 KI-VO müssen im Rahmen eines Risikomanagementsystems gem. Art. 9 Abs. 2 lit. c KI-VO bewertet werden. Deshalb ist die Einrichtung, Anwendung, Dokumentation und Aufrechterhaltung eines Risikomanagementsystems nach Art. 9 Abs. 1 KI-VO ebenfalls eine relevante Voraussetzung für die Erfüllung der Pflichten nach Art. 72 KI-VO. Es wird in Art. 9 Abs. 2 KI-VO als «kontinuierlicher iterativer Prozess» beschrieben, «der während des gesamten Lebenszyklus eines Hochrisiko-KI-Systems geplant und durchgeführt wird und eine regelmässige systematische Überprüfung und Aktualisierung erfordert». Ermittelt und analysiert werden müssen nach Art. 9 Abs. 2 lit. a KI-VO die bekannten und vernünftigerweise vorhersehbaren Risiken, die vom Hochrisiko-KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können, wenn es entsprechend seiner Zweckbestimmung verwendet wird. Dazu gehören auch die klassischen aktiven Beobachtungspflichten wie die Auswertung von öffentlich zugänglichen Informationen[1373]. Die Abschätzung und Bewertung der Risiken müssen nach Art. 9 Abs. 2 lit. b KI-VO vorgenommen werden, «wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird». Es müssen also keine missbräuchlichen Verwendungen verantwortet werden.[1374] Eine Ausnahme von der Vorhersehbarkeit ergibt sich aus Art. 9 Abs. 2 lit. c i.V.m. Art. 72 KI-VO: Gem. Art. 9 Abs. 2 lit. c KI-VO müssen auch «andere möglicherweise auftretende Risiken», die aufgrund des Systems zur Beobachtung nach Art. 72 KI-VO erkannt wurden, bewertet werden. Es kann sich dabei auch um Risiken handeln, die *nicht* vorhersehbar waren. Jedoch ist gem. Art. 9 Abs. 2 lit. d KI-VO keine Ergreifung von Risikomanagementmass-

KI-System verhütet und erkannt sowie darauf reagiert, diese beseitigt und kontrolliert werden können.

1373 Beurskens, in: Bomhard et al., § 16 Rn. 112; siehe auch Beck KI-VO-Braun Binder/Egli, Art. 9 N 23, m.w.H.

1374 Arioli, Jusletter IT 04.07.2024, Rn. 24. S. o., Rn. 308. A.A. Beck KI-VO-Braun Binder/Egli, Art. 9 N 27, welche sich dafür aussprechen, dass sogar der unvorhersehbare Missbrauch beobachtet werden muss. Die zitierte Quelle verwendet jedoch den Begriff «misuse», nicht «abuse»; zitiert aus Schuett, S. 11. Nach vorliegender Meinung sind Hersteller und Anbieter in keiner Weise für den Missbrauch ihrer Produkte verantwortlich; zum Unterschied zwischen «misue» und «abuse» siehe auch NHK GPSR-Wiebe, Art. 5 N 24 Fn. 34.

nahmen nötig, wenn unvorhersehbare Risiken nach lit. c entdeckt werden, da lit. d (die Ergreifung von Massnahmen) sich explizit nur auf lit. a (die Ermittlung und Analyse) bezieht.[1375] Die Einrichtung des Risikomanagementsystems ist eine Vormarktpflicht, während die kontinuierliche Weiterentwicklung des Risikomanagementsystems, die Risikoanalyse sowie darauffolgende Massnahmen nach der Inverkehrbringung des Systems stattfinden.

Die Voraussetzung für eine systematische Analyse ist die Aufzeichnungs- oder Protokollierungspflicht[1376] nach Art. 12 KI-VO. Sie dient der Erleichterung der Beobachtung nach dem Inverkehrbringen nach Art. 72 KI-VO.[1377] Die Technik der Hochrisiko-KI-Systeme muss die automatische Aufzeichnung von Ereignissen während des gesamten Lebenszyklus des Systems ermöglichen.[1378] Es handelt sich bei der Protokollierungspflicht um eine Vormarktpflicht, da die Protokollierungsfunktionen bereits vor der Inverkehrbringung technisch sichergestellt werden müssen. 332

c. *Plan für die Beobachtung nach dem Inverkehrbringen*

Die Überwachung und Dokumentation[1379] der Beobachtung von Hochrisiko-KI-Systemen erfolgt auf der Grundlage eines Plans.[1380] Dieser ist inhaltlich nicht deckungsgleich mit dem System zur Beobachtung nach dem Inverkehrbringen.[1381] Der Plan muss «die wesentlichen Elemente» des Beobachtungssystems beinhalten und vor dem Inverkehrbringen festgelegt werden.[1382] Die Europäische Kommission muss mittels Durchführungsrechtsakt bis zum 2. Februar 2026 ein Muster eines solchen Plans sowie eine Liste mit den darin aufzunehmenden Elementen erstellen.[1383] Die Verpflichtung zur Erstellung eines Plans muss bereits vor der Inverkehrbringung bzw. der Bereitstellung er- 333

1375 S. u., Rn. 353.

1376 Zur Protokollierungspflicht sollen bis zum 30. April 25 Normen ausgearbeitet werden, BJ, Rechtliche Basisanalyse KI, S. 116; die Normen sind zurzeit noch «im Aufbau», siehe Website CEN, Arbeitsprogramm, abrufbar unter <https://standards.cencenelec.eu/dyn/www/f?p=205:22:0::::FSP_ORG_ID,FSP_LANG_ID:2916257,22&cs=1B1700B5140A45B45CB5CB68BAF808643>, zuletzt besucht am 31.05.2025.

1377 Art. 12 Abs. 2 lit. b KI-VO.

1378 Art. 12 Abs. 1 KI-VO.

1379 Gemeint ist eine «im Nachhinein abrufbare Speicherung der Information», Beck KI-VO-Hartmann, Art. 72 N 14.

1380 Art. 72 Abs. 3 KI-VO.

1381 Beck KI-VO-Hartmann, Art. 72 N 18.

1382 Beck KI-VO-Hartmann, Art. 72 N 16.

1383 Art. 72 Abs. 3 KI-VO; siehe auch Beck KI-VO-Hartmann, Art. 72 N 16.

füllt werden, da er Teil der technischen Dokumentation[1384] ist.[1385] Es handelt sich bei der Erstellung des Plans somit um eine Vormarktpflicht.

334 Art. 72 Abs. 4 KI-VO legt fest, dass andere Systeme zur Beobachtung, die aufgrund von spezifischen Produktsicherheitsvorschriften (konkret aus den Harmonisierungsvorschriften aus Anhang I Abschnitt A)[1386] bereits früher eingerichtet werden mussten, durch die Elemente des Durchführungsrechtsaktes nach Art. 72 Abs. 3 KI-VO ergänzt werden können, wenn «ein gleichwertiges Schutzniveau erreicht wird».[1387]

1.3. Beispiel – Staubsaugerroboter

335 Das Risiko im Zusammenhang mit KI-Systemen muss immer im Rahmen des konkreten Sachverhalts beurteilt werden. Es kommt also auf die Zweckbestimmung an, ob ein KI-System Gefahren auslösen kann oder nicht.[1388] Gem. WENDEHORST spielt die Unterscheidung der Komponenten[1389] «eine geringe Rolle», da «die Konformität eines KI-Systems immer in seiner konkreten Hardware- und Softwareumgebung zu beurteilen»[1390] sei. Während Art. 72 Abs. 2 KI-VO jedoch festhält, dass die Beobachtung nach dem Inverkehrbringen «gegebenenfalls [...] eine Analyse der Interaktion *mit anderen KI-Systemen*»[1391] umfasst, weitet ErwG 155 diese auf andere «*Geräte und Software*» aus. Diese Ergänzung würde eine uferlose, sehr detaillierte Beobachtungspflicht ganzer Geräte nach sich ziehen. Da sich aber keine entsprechende Regelung im Gesetzestext findet und auch die Interaktion mit anderen KI-Systemen nur «gegebenenfalls»[1392] analysiert werden muss, besteht nach vorliegender Ansicht keine Pflicht zur Beobachtung anderer Komponenten nach der KI-VO.[1393] Dies heisst natürlich nicht, dass in der EU nicht andere (jedoch evtl. weniger strenge) Beobachtungspflichten als jene für Hochrisiko-KI-Systeme auf die restlichen Komponenten eines Gerätes (z.B. nach GPSR oder einem sektorspe-

1384 Art. 72 Abs. 3 KI-VO.
1385 Beck KI-VO-HARTMANN, Art. 72 N 17.
1386 S. o., Rn. 237.
1387 Ausführlich dazu Beck KI-VO-HARTMANN, Art. 72 N 5.
1388 S. o., Rn. 231.
1389 S. o., Rn. 226.
1390 Beck KI-VO-WENDEHORST, Art. 3 N 23.
1391 Mit einer Ausnahme für «sensible operative Daten von Betreibern, die Strafverfolgungsbehörden sind», Art. 72 Abs. 2 KI-VO.
1392 Zur Unklarheit es Bewertungsmassstabes bezüglich der Interaktion mit anderen KI-Systemen siehe Beck KI-VO-HARTMANN, Art. 72 N 13.
1393 A.A., jedoch mit Bezug auf IT-Sicherheitslücken und die Schwierigkeit der Begrenzung ebenfalls hervorhebend BEURSKENS, in: Bomhard et al., § 16 Rn. 181.

zifischen Erlass) anwendbar sind. Sodann ist die Abgrenzung des KI-Systems zu anderen Komponenten doch relevant, was im folgenden Beispiel veranschaulicht werden soll.

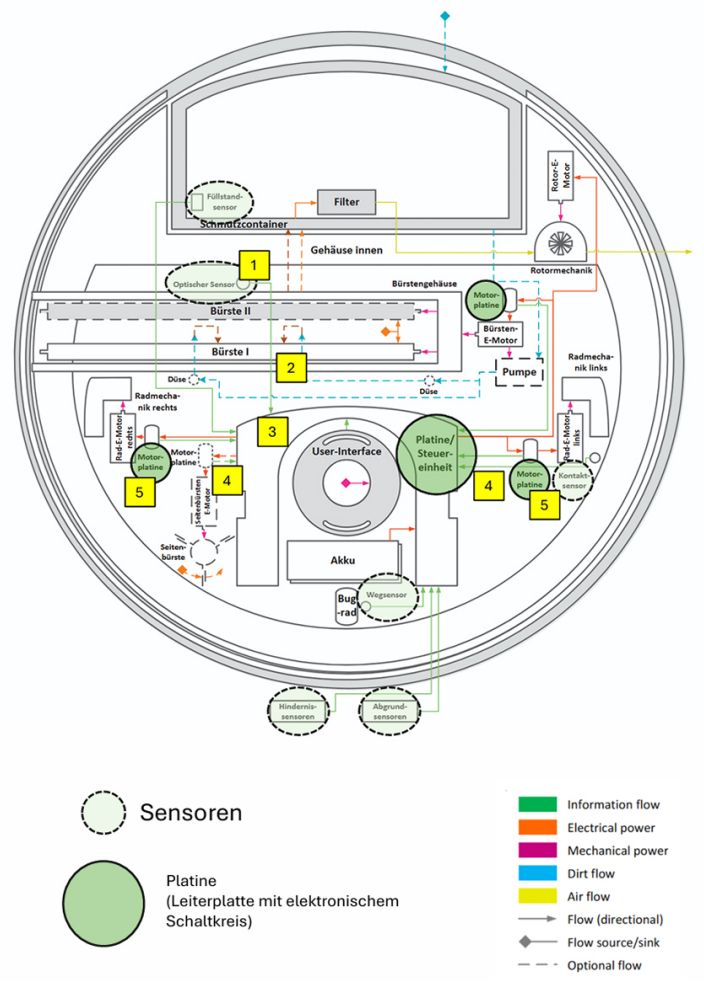

Abbildung 9: *Schema Staubsaugerroboter mit Legende*[1396]

1394 Das Schema ohne die grünen Kreise und gelben Nummern stammt aus GEBHARDT/BAHNS/KRAUSE, S. 79; die Legende zu den Informationsflüssen usw. (rechte Seite) stammt aus KUECHENHOF et al., S. 2279.

336 Untersucht wird ein Staubsaugerroboter mit einem Bilderkennungssystem. Solche Bilderkennungssysteme werden eingesetzt, um Hindernisse automatisch zu erkennen und zu umfahren.[1395] Die nachfolgende Nummerierung bezieht sich auf verschiedene Komponenten und Informationsflüsse des Staubsaugerroboters in Abbildung 9 auf der vorhergehenden Seite.

1. Der optische Sensor nimmt ein Video auf.
2. Die Daten aus dem Video (z.B. einzelne «Frames», wie bspw. ein Bild pro Sekunde) werden an die Platine/Steuereinheit geschickt.
3. Die Software in der Steuereinheit:
    a. Bearbeitet das Bild (z.B. erhöht es den Kontrast) zur besseren Auswertbarkeit.
    b. Übergibt das bearbeitete Bild als Input an die Schnittstelle zum KI-Modell.
    c. Die Schnittstelle zum KI-Modell übergibt den Input ans KI-Modell.
    d. Das KI-Modell analysiert das bearbeitete Bild und erhält das Ergebnis (Output), dass es sich mit 99%iger Wahrscheinlichkeit um ein Kabel handelt.
    e. Das KI-Modell übergibt den Output an die Schnittstelle.
    f. Die Schnittstelle übergibt den Output an die nächste Softwarekomponente.
    g. Die nächste Softwarekomponente kategorisiert das Kabel als «kein Schmutz».
    h. Die Information «kein Schmutz» wird an die nächste Softwarekomponente weitergegeben, die bei «kein Schmutz» den Befehl gibt, zurück und nach rechts zu fahren.
4. Die Daten «zurück und nach rechts fahren» werden an die Motorsteuerungseinheit (im Schema «Motorplatinen») geschickt.
5. Der Motor führt die Bewegungen anhand der Informationen «zurück und nach rechts fahren» aus.

337 Im vorliegenden Beispiel ist die Zweckbestimmung des KI-Systems die Analyse des Bildes, um festzustellen, was sich auf diesem Bild befindet. Das KI-System umfasst hier lediglich das KI-Modell sowie dessen direkte Input- und Output-Schnittstellen (Komponenten 3c bis 3e). Die übrigen Software- und Hardwarekomponenten erfüllen keine eigenständige KI-Funktionalität und es findet

[1395] Das Beispiel ist angelehnt an: Ecovacs Robotics: the AI robotic vacuum cleaner powered by TensorFlow – The TensorFlow Blog, abrufbar unter <https://blog.tensorflow.org/2020/01/ecovacs-robotics-ai-robotic-vacuum.html>, zuletzt besucht am 31.05.2025.

keine gegenseitige Beeinflussung statt.[1396] Es wird bspw. für die Funktionsweise des KI-Systems selbst nicht relevant sein, ob der optische Sensor eine Störung hatte und vielleicht gar kein Video aufgenommen hat (Komponente 1). Es würde bereits bei der Auswertung aus der Interaktion mit der Komponente 3a offensichtlich werden, dass das KI-System gar kein Bild zur Analyse erhalten hat. Wieso es kein Bild bekommen hat, spielt für das KI-System selbst direkt keine Rolle. Die Beobachtungspflicht nach Art. 72 KI-VO ist insbesondere auf Risiken ausgerichtet, die aufgrund des weiterhin möglichen Lernens nach der Inverkehrbringung entstehen.[1397] Sie ist nicht dazu da, den Umgang mit Risiken traditioneller Software oder von Geräten an sich zu regeln. Ebenso wenig spielt es (für das KI-System!) eine Rolle, ob die Ausgabedaten tatsächlich an die Motorsteuerungseinheit geschickt wurden (Komponente 4) und der Motor die Bewegung tatsächlich ausgeführt hat (Komponente 5). Für die Gefährlichkeit des Gerätes an sich spielt es natürlich eine Rolle, ob die Bewegung ausgeführt wird oder nicht. Aber für die Zweckbestimmung des KI-Systems (Bildanalyse) ist es nur wichtig, ob der Gegenstand tatsächlich als Kabel erkannt wurde, damit dieser von der nächsten Komponente als Hindernis kategorisiert werden kann. Die übrigen Software- und Hardwarekomponenten sind daher nicht Gegenstand der Beobachtungspflicht nach Art. 72 Abs. 2 KI-VO.

Im vorliegenden Beispiel kann es sich in der EU um ein Hochrisiko-KI-System zur Bildanalyse handeln, da es als Sicherheitsbauteil[1398] klassifiziert werden kann und wenn nach Art. 17 Abs. 4 lit. a RED i.V.m. Anhang III Modul B Ziff. 1 RED z.B. nicht die einschlägigen harmonisierten Normen verwendet wurden und dann eine Konformitätsbewertung durch Dritte nötig ist. Art. 72 KI-VO wäre also anwendbar auf das vorliegende Hochrisiko-KI-System. In der Schweiz würde der Staubsaugerroboter als Funkanlage von der FAV und als Niederspannungsgerät von der NEV erfasst. Auf das KI-System und die übrige Software wäre Art. 8 Abs. 2 lit. a PrSG anwendbar. 338

2. Passive Beobachtungspflicht

Die passive Produktbeobachtungspflicht beschreibt die Pflicht, auf Rückmeldungen über Produkte zu reagieren.[1399] Der Hersteller muss Informationen zu 339

1396 S. o., Rn. 226.

1397 ErwG 155 KI-VO; Beck KI-VO-Hartmann, Art. 72 N 2.

1398 Zum Bilderkennungssystem als Sicherheitsbauteil s. o., Rn. 230.

1399 Statt vieler Gerster, Rn. 278, insbesondere Fn. 444, wobei nach vorliegender Meinung nicht nur Rückmeldungen von Kunden beachtet werden müssen, m.w.H.; in Bezug auf die GPSR siehe NHK GPSR-Piovano, Art. 9 N 149.

unsicheren Produkten entgegennehmen und diese auswerten.[1400] Die passive Produktbeobachtungspflicht im allgemeinen Produktsicherheitsrecht ist in der Schweiz in Art. 8 Abs. 3 PrSG und in der EU in Art. 9 Abs. 12 GPSR geregelt. Die KI-VO enthält eine passive Beobachtungspflicht in Art. 20 Abs. 2 und in Art. 72 Abs. 2.

2.1. Prüfung von Beschwerden

340 Interne und externe[1401] Beanstandungen, welche die Sicherheit von Produkten betreffen, müssen vom Hersteller gem. Art. 8 Abs. 3 PrSG sorgfältig geprüft werden. In Art. 5 Abs. 1 Uabs. 4 lit. b Produktsicherheitsrichtlinie wurde die Prüfung von Beschwerden lediglich als mögliche Massnahme zur Erkennung von Gefahren aufgelistet. Nun müssen Hersteller gem. Art. 9 Abs. 12 GPSR eingegangene Beschwerden[1402] und Informationen über Unfälle, die die Sicherheit ihrer bereitgestellten Produkte betreffen und vom Beschwerdeführer als gefährlich gemeldet wurden, untersuchen.[1403] Art. 20 Abs. 2 KI-VO schreibt Anbietern von Hochrisiko-KI-Systemen vor, dass sie die Ursachen erkannter Risiken i.S.v. Art. 79 Abs. 1 KI-VO unverzüglich untersuchen müssen. Art. 79 Abs. 1 KI-VO definiert KI-Systeme[1404], die ein Risiko bergen, mit einem Verweis auf Art. 3 Ziff. 19 MÜVO, schränkt die Anwendbarkeit jedoch auf Risiken für die Gesundheit, Sicherheit und Grundrechte von Personen ein. Risiken können bspw. aufgrund einer Meldung eines Betreibers bekannt gemacht werden, der in einem solchen Fall bei der Untersuchung mitwirken muss.[1405] Durch wen oder wie das Risiko erkannt wurde, spielt aber keine Rolle, weshalb bspw. auch Beschwerden von Konsumenten untersucht werden müssen. Zudem weist Art. 72 Abs. 2 KI-VO darauf hin, dass sich Daten zur Leistung von Hochrisiko-KI-Systemen im Rahmen des Systems zur Beobachtung auch aus anderen Quellen erheben lassen als vom Anbieter oder dem Betreiber. Solche anderen Quellen können ebenfalls Beschwerden sein.[1406] Diese müssen wiederum ana-

1400 NHK GPSR-Piovano, Art. 9 N 149.

1401 Botschaft PrSG, S. 7443; neben konventionellen Kundenbeschwerden sind auch Informationen aus «Garantie-Inanspruchnahmen, Gewährleistungsforderungen oder Kundenbefragungen» relevant, SHK PrSG-Hess, Art. 8 N 29; siehe auch Fellmann, Jusletter 25.10.2010, Rn. 36; in Bezug auf die GPSR NHK GPSR-Piovano, Art. 9 N 149.

1402 Die Pflicht nach Art. 9 Abs. 11 GPSR, Möglichkeiten zu schaffen, Beschwerden einzureichen, ist eine Vormarktpflicht.

1403 Siehe auch NHK GPSR-Piovano, Art. 9 N 149.

1404 Gemeint sind nicht nur Hochrisiko-KI-Systeme, sondern alle KI-Systeme, die von der KI-VO erfasst werden, Beck KI-VO-Hartmann, Art. 79 N 1.

1405 Art. 20 Abs. 2 KI-VO.

1406 Siehe auch Beck KI-VO-Hartmann, Art. 72 N 12.

lysiert werden.[1407] Der Aufwand für die Auswertung muss wieder in einem angemessenen Verhältnis zum Gefahrenpotenzial stehen.[1408]

Damit Reklamationen geprüft werden können, müssen sie zunächst beim Hersteller ankommen und erfasst werden. Üblicherweise geschieht dies direkt durch die Konsumenten via Post, Telefon oder E-Mail sowie über Händler oder «Reparatur- und Servicestellen».[1409] Häufiger werden heutzutage Direktnachrichten an den Hersteller via der Produkt zugehörigen App, integrierte Möglichkeiten zur Fehlermeldung durch den Nutzer (z.B. via In-App-Bug-Reporting) oder Beanstandungen über Social Media[1410] sein. Dabei ist zu beachten, dass die GPSR keine aktive Produktbeobachtungspflicht vorschreibt und in der EU deshalb lediglich Beanstandungen, die über direkt vom Hersteller betriebene Social-Media-Profile gemeldet werden, beachtet werden müssen.[1411] 341

2.2. Dokumentation von Beschwerden

In der Schweiz sprechen sich HESS und FELLMANN dafür aus, dass die Verpflichteten sicherstellen müssen, dass sie Reklamationen nicht nur auswerten, sondern auch erfassen.[1412] Damit eine systematische Bearbeitung von sicherheitsrelevanten Beanstandungen möglich sei, sei die Implementation eines Beschwerdemanagements oder Sicherheitsmonitorings nötig.[1413] FELLMANN hält zudem fest, dass die Nachmarktpflichten den Aufbau eines ganzen Produktbeobachtungssystems bedingen. Darin sollen nicht nur Beschwerden, sondern auch weitere «sicherheitsrelevante Informationen» und Notfallpläne[1414] geführt werden.[1415] Die Dokumentation von Beschwerden wird im PrSG nicht explizit vorgeschrieben. Trotzdem ist vor allem bei grösseren Unternehmen schwer vorstellbar, wie Gefahren zuverlässig erkannt werden können, wenn diese nicht systematisch dokumentiert werden.[1416] Das Einrichten einer zentralen Stelle für die Entgegennahme und Auswertung von Beschwerden wird deshalb auch in Bezug auf die GPSR disku- 342

1407 Art. 72 Abs. 2 KI-VO.
1408 S. o., Rn. 309 ff.
1409 Botschaft PrSG, S. 7443; SHK PrSG-HESS, Art. 8 N 29; FELLMANN, Jusletter 25.10.2010, Rn. 35 f.; NHK GPSR-PIOVANO, Art. 9 N 149.
1410 Ausführlich NHK GPSR-PIOVANO, Art. 9 N 149 ff.
1411 NHK GPSR-PIOVANO, Art. 9 N 149, jedoch a.A. in Bezug auf Informationen zu Unfällen, siehe N 152.
1412 SHK PrSG-HESS, Art. 8 N 29; FELLMANN, Jusletter 25.10.2010, Rn. 35 f.
1413 SHK PrSG-HESS, Art. 8 N 29; FELLMANN, Jusletter 25.10.2010, Rn. 35 f.
1414 S. u., Rn. 351.
1415 FELLMANN, Jusletter 25.10.2010, Rn. 11, m.w.H.
1416 Ähnlich NHK GPSR-PIOVANO, Art. 9 N 157.

tiert.[1417] Die Dokumentation von Beschwerden im Rahmen eines Beschwerdebuches war in Art. 5 Abs. 1 Uabs. 4 lit. b Produktsicherheitsrichtlinie als mögliche Massnahme zur Erkennung von Gefahren aufgeführt.[1418] Art. 9 Abs. 12 GPSR verpflichtet den Hersteller nun, ein internes Verzeichnis der erhaltenen Reklamationen und Informationen zu führen. Dabei müssen die Hersteller auch Produktrückrufe und getroffene Massnahmen zur Wiederherstellung der Produktkonformität dokumentieren.[1419] PIOVANO/SCHUCHT/WIEBE schlagen vor, zusätzlich «die Beschwerdeprüfung und das Untersuchungsergebnis» zu dokumentieren.[1420] Eine Pflicht diesbezüglich besteht jedoch nicht. Anbieter von Hochrisiko-KI-Systemen müssen gem. Art. 72 Abs. 2 KI-VO die im System zur Beobachtung nach dem Inverkehrbringen erhobenen Daten – und damit auch Beschwerden – dokumentieren.

2.3. Durchführen von Stichproben nach Beanstandungen

343 Gem. Art. 8 Abs. 3 PrSG müssen Hersteller *nötigenfalls*[1421] Stichproben ihrer Produkte machen, wenn diese beanstandet wurden. Das Durchführen von Stichproben im harmonisierten Bereich der EU ist nach den Musterbestimmungen des Beschlusses 2008/768/EG geregelt und wurde damit auch in verschiedene Sektorrichtlinien übernommen.[1422] Auch nach dem GPSR-Entwurf wären Hersteller zur regelmässigen Durchführung von Stichproben verpflichtet gewesen.[1423] In der finalen GPSR fiel die Regelung jedoch weg.[1424] Auch die KI-VO enthält keine Pflicht zur Durchführung von Stichproben.

344 Stichproben dienen dem Erkenntnisgewinn über «dem Produkt immanente Gefahren und […] riskante Verwendungsarten».[1425] Bei herkömmlichen Produkten lag der Fokus vor allem auf Stichproben im Absatzkanal oder dem Lager des Herstellers, um die Auswirkungen des Transports, der Lagerung oder des Gebrauchs durch Konsumenten zu untersuchen.[1426] Bei KI-Systemen dürf-

1417 NHK GPSR-PIOVANO, Art. 9 N 153, 157, 158.
1418 Siehe auch HOLLIGER-HAGMANN, Fallstricke, S. 164.
1419 Art. 9 Abs. 12 GPSR; siehe auch NHK GPSR-PIOVANO, Art. 9 N 156.
1420 PIOVANO/SCHUCHT/WIEBE, S. 152; ebenso in NHK GPSR-PIOVANO, Art. 9 N 154.
1421 Siehe auch SHK PrSG-HESS, Art. 8 N 33, welcher festhält, dass es bei einer Beanstandung eigentlich kein Szenario gäbe, wo keine Stichproben gemacht werden müssten.
1422 NHK GPSR-PIOVANO, Art. 9 N 147.
1423 Europäische Kommission, Vorschlag GPSR, Art. 15 Abs. 2.
1424 NHK GPSR-PIOVANO, Art. 9 N 148.
1425 Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 8 PrSG N 8.
1426 Botschaft PrSG, S. 7443; SHK PrSG-HESS, Art. 8 N 31; FELLMANN, Jusletter 25.10.2010, Rn. 25, 37.

ten sich die Stichproben sinnvollerweise eher auf Wechselwirkungen mit anderen Systemen (z.B. andere KI-Systeme oder Datenbanken) oder mit bestimmter Hard- und Firmware beziehen. Ein frühzeitiges Erkennen von Problemen in Stichproben ermöglicht eine rasche Reaktion, wie die Bereitstellung von Updates oder anderen geeigneten Massnahmen. In Bezug auf KI-Systeme ergibt es Sinn, dass sich in Verkehr befindende trainierte Systeme kontrolliert werden, weil diese nicht vollständig vorhersehbar sind. Wie schon bei herkömmlichen Produkten, bei welchen klar sein musste, welche Serie potenziell gefährlich sein könnte, muss auch genau jene Version der Software kontrolliert werden, die in Verkehr gebracht wurde.[1427] Befinden sich verschiedene Versionen im Verkehr, müssen alle kontrolliert werden. Stichproben sind am sinnvollsten, wenn die gleiche Ausgangslage wie beim beschwerenden Konsumenten simuliert wird, also z.B. die gleiche Softwareversion in Verbindung mit der gleichen Hardware und dort bei gleicher Firmware.

3. Fazit

Im Rahmen der aktiven Produktbeobachtung müssen Hersteller aktiv nach möglichen vorhersehbaren Gefahren, die durch ihre Produkte ausgelöst werden könnten, recherchieren. Eine solche Pflicht besteht jedoch nur im allgemeinen Produktsicherheitsrecht der Schweiz, nicht aber in jenem der EU. Das heisst, dass nur in der Schweiz eine aktive Beobachtungspflicht für Software nach Art. 8 Abs. 2 lit. a PrSG besteht, nicht aber in der EU. In der Schweiz ist der Hersteller frei, wie er die Gefahrenerkennung umsetzen möchte, solange er angemessene Nachforschungen betreibt. Für Hochrisiko-KI-Systeme werden in der EU hingegen detaillierte Vorgaben zur aktiven Produktbeobachtung gemacht. Die KI-VO enthält aktive Beobachtungspflichten für Anbieter von Hochrisiko-KI-Systemen, da gem. Art. 72 Abs. 2 KI-VO Daten über deren Leistung proaktiv und zielgerichtet[1428] erhoben und analysiert[1429] werden müssen. Dieses System zur Beobachtung nach dem Inverkehrbringen ist zudem Teil des Risikomanagementsystems, nach welchem gem. Art. 9 Abs. 2 KI-VO kontinuierlich Risiken ermittelt und bewertet werden müssen. Ergeben sich aus dem System zur Beobachtung nach dem Inverkehrbringen unvorhersehbare Gefah- 345

[1427] Ein Lösungsansatz zur systematischen Software-Identifikation besteht im Medizinprodukterecht mittels Unique Device Identification Code, siehe Beck KI-VO-Wendehorst, Art. 3 N 118.

[1428] Beck KI-VO-Hartmann, Art. 72 N 14.

[1429] Beck KI-VO-Hartmann, Art. 72 N 15.

ren, müssen diese im Rahmen des Risikomanagementsystems ebenfalls bewertet werden.

346 Auch wenn in der Schweiz keine Pflicht zur aktiven integrierten Produktbeobachtung besteht, ist dem Hersteller das Einrichten von automatischen Rückmeldungen trotzdem stark zu empfehlen, da sie eine schnelle Reaktion und eine verbesserte Fehlerfindung ermöglichen.[1430] Meldet sich ein Konsument über herkömmliche Kanäle, kann es schwierig sein, nur aufgrund einer Fehlerbeschreibung herauszufinden, weshalb oder wie das Produkt auf ungewollte Art reagiert hat. Aus diesem Grund ist es bei der Bearbeitung von Beanstandungen wichtig, dass nachvollzogen werden kann, welche Version eines Systems von der Reklamation betroffen ist. Dies wird bei einer integrierten Produktbeobachtung erleichtert, da die Versionsnummer mit der Systemmeldung an den Hersteller mitgeliefert werden kann. Wie dargelegt, haben nicht alle Arten von Herstellern die gleiche Art von Kontrolle über ihre Produkte.[1431] Realistischerweise haben nur Hersteller, die tatsächlich Teil der Entwicklung der Software waren, auch die Möglichkeit, eine aktive integrierte Produktbeobachtung umzusetzen. Entwickelt ein Dritter die Software für ein Smart Home Device, gibt er dem (Quasi-)Hersteller des Gerätes mit der Software sinnvollerweise auch gleich ein System mit, mit welchem eine aktive integrierte Produktbeobachtung möglich ist. Dies ist sowieso Pflicht bei Hochrisiko-KI-Systemen, da deren Technik nach Art. 12 Abs. 1 KI-VO die automatische Aufzeichnung von Ereignissen ermöglichen muss.

347 Im allgemeinen Produktsicherheitsrecht sind Hersteller in der Schweiz (Art. 8 Abs. 3 PrSG) und der EU (Art. 9 Abs. 12 GPSR) dazu verpflichtet, sicherheitsrelevante Beanstandungen im Rahmen der passiven Produktbeobachtungspflicht entgegenzunehmen und zu untersuchen. Die Dokumentation von Beschwerden wird im PrSG nicht explizit vorgeschrieben, trotzdem ist sie faktisch Pflicht, da ohne Dokumentation kein sinnvolles Beschwerdemanagement möglich ist. Anbieter von Hochrisiko-KI-Systemen müssen Beschwerden ebenfalls untersuchen und dokumentieren (Art. 20 Abs. 2 und Art. 72 Abs. 2 KI-VO). Während für Hersteller in der Schweiz Stichproben aufgrund von Beschwerden vorgeschrieben sind, gibt es eine solche Pflicht in der EU zumindest in der GPSR und der KI-VO nicht. Bis auf das Entgegennehmen von Reklamationen und das darauffolgende Durchführen von Stichproben werden auch in der Schweiz keine spezifischen Massnahmen vorgeschrieben. Welche

1430 Siehe auch Twigg-Flesner, S. 11.

1431 So hat bspw. der Vertreter gem. Art. 2 Abs. 4 lit. b PrSG i.d.R. viel weniger Einfluss auf die Sicherheit eines Produktes als ein «Hersteller i.e.S.» gem. Art. 2 Abs. 4 PrSG, s. o., Rn. 289.

Massnahmen zur Erkennung von Gefahren als angemessen angesehen werden, liegt in der Schweiz und der EU grösstenteils im Ermessen des Herstellers. Auch welche Kanäle zur Entgegennahme von Beschwerden eingerichtet werden, kann der Hersteller selbst entscheiden.

Da die GPSR keine aktive Produktbeobachtungspflicht und keine Durchführung von Stichproben im Rahmen der passiven Produktbeobachtungspflicht vorschreibt, müssen Hersteller, die Produkte in der Schweiz in Verkehr bringen, weitergehende Gefahrenerkennungsmassnahmen durchführen als Hersteller, die Produkte in der EU in Verkehr bringen. Da mit der Einführung des PrSG vor allem das Schutzniveau der EU erreicht werden sollte, damit die wirtschaftliche Kompatibilität gegeben ist, sollten die aktive Produktbeobachtungspflicht und die Durchführung von Stichproben für Hersteller im allgemeinen Produktsicherheitsrecht in der Schweiz gestrichen werden. Stattdessen sollte für Softwareprodukte, die mit einem besonders hohen Risiko verbunden sind (wie bspw. in der KI-VO für Hochrisiko-KI-Systeme) eine aktive integrierte Produktbeobachtungspflicht eingeführt werden, um gefährliche Veränderungen oder Auswirkungen kontinuierlich zu erkennen und Kompatibilität mit der EU zu schaffen. 348

IV. Gefahrenabwendungsmassnahmen

Massnahmen zur Gefahrenabwendung werden jeweils aus einem bestimmten Anlass, z.B. wegen eines eingetretenen Schadens oder einer drohenden Gefahr, getroffen. Der Umfang der Massnahmen richtet sich nach der Grösse der Gefahr, dem zu erwartenden Erfolg der Massnahme und (bis zu einem gewissen Grad) den damit verbundenen Nachteilen für den Hersteller.[1432] Konnte früher nur die Realisierung der Gefahr verhindert werden, nicht aber die Gefahr selbst,[1433] kann nun bei Produkten mit Zugriff via Internet sogar die Gefahr als solche abgewendet werden. Dies zeigt sich bspw. bei einem Rasenmäher: War dieser gefährlich, weil der Griff locker war, konnte der Hersteller eine Warnung publizieren, damit der Konsument die Schrauben regelmässig anzieht. Hat der Konsument die Schrauben nicht angezogen, bleibt das Produkt gefährlich. Der Hersteller hat keinen Einfluss darauf. Ist ein «intelligenter» Rasenmäher z.B. aufgrund der Software immer wieder sehr heiss geworden und konnte den Nutzer bei Berührung verbrennen, kann die Software vom Hersteller u.U. angepasst werden, damit der Mäher nicht mehr heiss wird. Der Her- 349

1432 S. o., Rn. 321.

1433 Ausführlich GERSTER, Rn. 282 f.

steller kann die Gefahr direkt abwenden und ist nicht abhängig von der Umsetzung des Konsumenten. Mit der Möglichkeit, Produkte mit Software oder Stand-alone-Software aus der Ferne zu aktualisieren und damit zu verändern, eröffnen sich neue Gefahrenabwendungsmassnahmen für Smart Home Devices.[1434] Welche Gefahrenabwendungsmassnahmen jeweils erforderlich bzw. angemessen sind, ist wiederum das Resultat einer Risikoanalyse.[1435]

1. (Bereitschaft zur) Gefahrenabwendung

350 Gem. Art. 8 Abs. 2 lit. b PrSG muss der Hersteller angemessene Massnahmen treffen, um allfällige Gefahren abwenden zu können. Gemeint sind bestehende und erkannte Gefahren. Es handelt sich dabei um Gefahren, welche sich erst zeigen, wenn sich das Produkt auf dem Markt oder in der Vertriebskette befindet.[1436] Strittig ist, ob das PrSG eine Pflicht für den Hersteller beinhaltet, dass bei einer erkannten Gefahr tatsächlich Massnahmen getroffen werden müssen,[1437] oder ob sich diese Pflicht auf die «*Bereitschaft* zur Abwendung»[1438] von Gefahren beschränkt. Nach der Botschaft und einem Teil der Lehre (dem hier gefolgt wird) müssen nach Art. 8 Abs. 2 lit. b PrSG bei erkannter Gefahr keine Massnahmen getroffen werden.[1439] Die Pflicht beschränkt sich auf die

1434 Siehe auch NHK GPSR-Piovano, Art. 9 N 98; OECD, Measuring, S. 6.

1435 S. o., Rn. 309.

1436 S. o., Rn. 322.

1437 Folgert aus dem PrSG eine Pflicht zum Treffen von Massnahmen zur Gefahrenabwendung, Fellmann, Jusletter 25.10.2010, Rn. 56 f., 66. Er weist darauf hin, dass die Aussage der Botschaft, dass nur Pflichten zu Massnahmen aus dem Zivilrecht und nicht aus dem PrSG abzuleiten seien, nicht richtig sei. Er vertritt die Meinung, dass diese Pflichten auch aus dem PrSG abgeleitet werden müssen und somit auch das öffentliche Recht verpflichte, Massnahmen zu treffen. Er argumentiert damit, dass es keinen Sinn ergebe, wenn eine Behörde lediglich zivilrechtliche Pflichten verfügen und sogar unter Strafandrohung veranlassen könne; wohl ebenfalls der Meinung, dass nicht nur eine Bereitschaft gemeint sei: Lohmann, Haftungsrahmen, S. 118; Furrer, in: Fellmann/Furrer, Schonzeit, S. 103, welcher feststellt, dass der Hersteller «bereits Massnahmen getroffen haben» müsse, weil er bei einer Meldung an die Behörde sonst gar nicht darüber berichten könne.

1438 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 4.

1439 Botschaft PrSG, S. 7441 f.; Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG Rn. 4, 6, 18; Schwenzer/Schmidt, in: Guillod/Müller S. 258; Bühler, Sicherheit, Rn. 45, 48; Bühler, Bestandteil, S. 90, aber dann scheinbar a.A. auf S. 100; Bühler, Privatrecht, S. 51, hält fest, dass es dem Hersteller freistehe, Massnahmen zu treffen; jedoch unklar in Bühler/Tobler: eher gegen eine Pflicht, tatsächliche Massnahmen zur Gefahrenabwehr treffen zu müssen auf S. 394, aber auf S. 397 feststellend, dass Massnahmen zu treffen seien, jedoch mit der Einschränkung, dass «auf jeden Fall» ein Konzept dazu erstellt werden solle; vermutlich ebenfalls keine Pflicht zum Treffen von Massnahmen sehend SHK PrSG-Hess, Art. 8 N 19, 22; siehe aber auch SHK PrHG-Hess, Art. 4 N 63 Fn. 1413, welcher eine zivilrechtliche

Bereitschaft zum Ergreifen von Massnahmen, falls solche Massnahmen von der zuständigen Behörde gem. Art. 10 Abs. 3 lit. b PrSG verfügt werden.[1440] Befindet die zuständige Behörde die getroffenen oder geplanten Massnahmen als ungenügend, kann diese nämlich andere Massnahmen anordnen oder selbst vollziehen.[1441] Nach einer solchen Verfügung besteht selbstverständlich eine Pflicht zum Treffen der angeordneten Massnahmen. Unbestritten ist, dass das PrSG nicht vorschreibt, *welche* Massnahmen zur Bereitschaft zur Gefahrenabwendung getroffen werden müssen.[1442] Während das PrSG keine Pflicht zur Ergreifung von Massnahmen beinhaltet, kann eine solche Pflicht zur Einschränkung einer Gefahr in der Schweiz aus dem Zivilrecht abgeleitet werden.[1443]

Um die nötige Bereitschaft zur Gefahrenabwendung herzustellen, benötigt der Hersteller einen Notfallplan. Darin werden Massnahmen definiert, die ergriffen werden können, wenn eine Gefahr erkannt wird.[1444] Damit soll sichergestellt werden, dass im Notfall schnell reagiert werden kann und möglichst nicht improvisiert werden muss.[1445] Bestenfalls werden auch gleich Kriterien definiert, die dabei unterstützen, geeignete Massnahmen auszuwählen.[1446] Wie bereits erwähnt, ist der Hersteller aus dem PrSG nicht verpflichtet, Massnahmen zu ergreifen, ohne dass diese angeordnet wurden. Da eine solche Pflicht aber aus dem Zivilrecht abgeleitet wird, empfehlen sich Kriterien zur Auswahl von Massnahmen dennoch. Der Notfallplan ist Teil des Krisenmanagements ei- 351

Rückrufpflicht für lebensbedrohliche Sachverhalte mit vermutetem Verweis auf das PrSG etwas zurückhaltend bejaht; unklar GERSTER, Rn. 282 f.

1440 Botschaft PrSG, S. 7442; Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 8 PrSG N 6; SHK PrSG-HESS, Art. 8 N 19, m.w.H.

1441 Art. 10 Abs. 2 bis 5 PrSG; Botschaft PrSG, S. 7442; FURRER, in: Fellmann/Furrer, Schonzeit, S. 102 f.

1442 Botschaft PrSG, S. 7441, 7443; Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 8 PrSG N 6; FELLMANN, Jusletter 25.10.2010, Rn. 56, 58, m.w.H.; SHK PrSG-HESS, Art. 8 N 22.

1443 Insbesondere aus dem Gefahrensatz, der aus Art. 41 OR abgeleitet wird: Botschaft PrSG, S. 7441 f.; SHK PrSG-HESS, Art. 8 N 6, m.w.H.; Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 8 PrSG N 6; HOLLIGER-HAGMANN, Fallstricke, S. 162; FORNAGE, in: Chappuis/Winiger/Campi S. 218 (nicht aber aus dem PrHG, siehe S. 208); allgemein auf das Zivilrecht verweisend FELLMANN, Jusletter 25.10.2010, Rn. 56; auch kann das Untätigbleiben bei Gefahren zu Deckungsauschlüssen in einer allfälligen Betriebshaftversicherung führen, STUDER, in: Fellmann/Furrer, Schonzeit, S. 159.

1444 FELLMANN, Jusletter 25.10.2010, Rn. 11; SHK PrSG-HESS, 3. Krisenmanagement N 22 f.; siehe auch Haftpflichtkommentar-HOLLIGER-HAGMANN, Art. 8 PrSG N 6, welche den Notfallplan «Rückrufkonzept» nennt. Da aber nicht nur ein möglicher Produkterückruf geregelt werden soll, ist der Begriff nicht optimal.

1445 FELLMANN, Jusletter 25.10.2010, Rn. 32.

1446 Diese sind wiederum abhängig von einer Risikoanalyse, s. o., Rn. 309 ff.

nes Unternehmens.[1447] Ein Krisenmanagement und insbesondere ein Notfallplan sollten bereits im Vormarktstadium vor der Inverkehrbringung des Produktes bestehen, da Gefahren sich durchaus direkt nach der Inverkehrbringung offenbaren können.[1448] Es handelt sich bei der Pflicht zur Bereitschaft der Gefahrenabwehr deshalb eigentlich um eine Vormarktpflicht,[1449] obwohl sie sich gesetzessystematisch bei den Nachmarktpflichten befindet.[1450]

352 Die Pflicht für Hersteller, Massnahmen zu treffen, damit sie zur Abwendung von Gefahren imstande sind, war in der Produktsicherheitsrichtlinie in Art. 5 Abs. 1 Uabs. 3 lit. b geregelt. Auch gem. Art. 5 Abs. 1 Uabs. 5 Produktsicherheitsrichtlinie mussten diese Vorkehrungen lediglich freiwillig «oder auf Aufforderung der zuständigen Behörden» umgesetzt werden. Somit waren Hersteller nach der Produktsicherheitsrichtlinie nicht dazu verpflichtet, Gefahrenabwendungsmassnahmen vorzunehmen, ohne dass sie von den Behörden dazu aufgefordert worden sind.[1451]

353 Anders als nach dem PrSG und der alten Produktsicherheitsrichtlinie besteht gem. Art. 9 Abs. 8 Uabs. 1 lit. a GPSR nun eine konkrete Pflicht zur Gefahrenabwendung, sobald der Hersteller Grund zur Annahme hat oder der Auffassung ist, dass ein von ihm in Verkehr gebrachtes Produkt gefährlich ist. Er muss dann die «erforderlichen Korrekturmassnahmen ergreifen, um die Konformität des Produktes auf wirksame Weise herzustellen, wozu gegebenenfalls auch eine Rücknahme vom Markt oder ein Rückruf gehören können».[1452] Auch Anbieter von Hochrisiko-KI-Systemen haben nach Art. 20 Abs. 1 KI-VO eine Pflicht zur Ergreifung von Korrekturmassnahmen, «um die Konformität dieses Systems herzustellen oder es gegebenenfalls zurückzunehmen, zu deaktivieren oder zurückzurufen», wenn sie annehmen müssen, dass ihr in Verkehr gebrachtes oder in Betrieb genommenes System nicht der KI-VO entspricht. Das heisst, dass «nichtkonforme und unverhältnismässig riskante Hochrisiko-KI-

1447 SHK PrSG-Hess, 3. Krisenmanagement N 11; wird in der deutschen Lehre auch «Rückrufmanagement» genannt, siehe dazu Fellmann, Jusletter 25.10.2010, Rn. 32. Der Begriff «Rückrufmanagement» ist genauso wie «Rückrufkonzept» zu vermeiden.

1448 SHK PrSG-Hess, Art. 8 N 5.

1449 Siehe auch Fellmann, Jusletter 25.10.2010, Rn. 32, der das Krisenmanagement als Teil der «Vorbereitung der Gefahrenabwehr» sieht. Er geht jedoch auch davon aus, dass nicht nur die Pflicht zur Bereitschaft zur Gefahrenabwehr besteht, sondern auch zum effektiven Treffen von Massnahmen.

1450 Ebenso wie die Sicherstellung der Rückverfolgbarkeit nach Art. 8 Abs. 2 lit. c PrSG, s. u., Rn. 383.

1451 Marktakteure mussten lediglich imstande sein, Massnahmen zu treffen, NHK GPSR-Hartmannsberger, Art. 35 N 5.

1452 Art. 9 Abs. 8 Uabs. 1 lit. a GPSR.

Systeme korrigiert oder vom Markt genommen werden»[1453] müssen. Erkannte Gefahren aus der dauerhaften Beobachtung nach Art. 72 KI-VO können also Korrekturmassnahmen gem. Art. 20 Abs. 1 KI-VO nach sich ziehen.[1454] Eine weitere Pflicht, die während des ganzen Lebenszyklus – und somit auch nach der Inverkehrbringung – eines Hochrisiko-KI-Systems wahrgenommen werden muss, ist das Ergreifen von Risikomanagementmassnahmen nach Art. 9 Abs. 2 lit. d KI-VO. Dadurch sollen die ermittelten Risiken nach Art. 9 Abs. 2 lit. a KI-VO bewältigt werden.[1455] Es handelt sich dabei um bekannte oder vernünftigerweise vorhersehbare Risiken für Gesundheit, Sicherheit oder Grundrechte, solange das KI-System nicht missbraucht[1456] wird.[1457] Art. 9 Abs. 3 bis 5 KI-VO spezifizieren, welche Risiken berücksichtigt und wie die Risikomanagementmassnahmen gestaltet werden müssen. Während die Risikomanagementmassnahmen darauf abzielen, ermittelte Risiken vor dem Inverkehrbringen oder der Inbetriebnahme und während des gesamten Lebenszyklus zu reduzieren, zielen die Korrekturmassnahmen darauf ab, konkrete Gefahren nach der Inverkehrbringung oder Inbetriebnahme unter Kontrolle zu bringen. So müssen Korrekturmassnahmen «unverzüglich» ergriffen werden.[1458] Angelehnt an das deutsche Recht wird unter «unverzüglich» auch «ohne schuldhaftes Zögern» verstanden.[1459] Welche Korrekturmassnahmen der Hersteller bzw. der Anbieter trifft, steht ihm nach der GPSR und der KI-VO frei.[1460] Ausgenommen davon ist die Warnung der Konsumenten nach Art. 9 Abs. 8 Uabs. 1 lit. b GPSR, welche immer vorgenommen werden muss, sobald die Voraussetzungen[1461] für die Pflicht zur Gefahrenabwehr gegeben sind.[1462] Die Unterrichtung bzw. Warnung der Konsumenten nach Art. 9 Abs. 8 Uabs. 1 lit. b GPSR ist ebenfalls eine Korrekturmassnahme nach Art. 9 Abs. 8 Uabs. 1 lit. a GPSR.[1463]

Um die Bereitschaft zur Gefahrenabwendung bei Software und KI-Systemen überhaupt zu ermöglichen, muss der Hersteller sein System so einrichten, 354

1453 Beck KI-VO-Eisenberger, Art. 20 N 2.
1454 Beck KI-VO-Hartmann, Art. 72 N 3; Beck KI-VO-Eisenberger, Art. 20 N 6.
1455 Beck KI-VO-Braun Binder/Egli, Art. 9 N 28.
1456 S. o., Rn. 308 und 263.
1457 Art. 9 Abs. 2 lit. a KI-VO.
1458 Art. 9 Abs. 8 GPSR; Art. 20 Abs. 1 KI-VO.
1459 Beck KI-VO-Eisenberger, Art. 20 N 16, mit Verweis auf Linardatos, in: Hilgendorf/Roth-Isigkeit, § 7 Rn. 30; mit dem Hinweis, dass die GPSR jedoch autonom und nicht nach dem deutschen Recht auszulegen sei: NHK GPSR-Piovano, Art. 9 N 89.
1460 NHK GPSR-Piovano, Art. 9 N 98; für die KI-VO Beck KI-VO-Eisenberger, Art. 20 N 17.
1461 Also wenn der Hersteller nach Art. 9 Abs. 8 Uabs. 1 GPSR sein Produkt für gefährlich hält oder halten muss.
1462 Siehe dazu NHK GPSR-Piovano, Art. 9 N 97.
1463 NHK GPSR-Piovano, Art. 9 N 111; siehe auch NHK GPSR-Hartmannsberger, Art. 35 N 1.

dass er die Möglichkeit hat, sich damit zu verbinden oder diese Verbindung ständig beibehält.[1464] Je nach Gefahrenpotenzial ist auch denkbar, dass der Hersteller sich ohne Wissen oder Zustimmung des Konsumenten mit dem Gerät verbindet, um Sicherheitsupdates zu installieren.[1465] Da das PrSG eine Bereitschaft zur Gefahrenabwendung und die GPSR die Gefahrenabwendung als solche vorschreiben und beides bei Produkten mit digitalen Komponenten nicht möglich ist, wenn keine Verbindung mehr zum Hersteller aufgebaut werden kann, könnten Hersteller bei genügend hohem Gefahrenpotenzial faktisch dazu verpflichtet sein, solche Möglichkeiten zur Verbindung einzurichten.[1466] Eine Verbindung zur Auslesung von Daten (also die Protokollierung) ist für Hochrisiko-KI-Systeme nach Art. 12 KI-VO vorgeschrieben. Eine Verbindung auf beiden Seiten (also nicht nur die Datenübertragung des in Verkehr gebrachten Hochrisiko-KI-Systems zum Anbieter, sondern auch die Updatemöglichkeit vom Anbieter zum System) ist immerhin mittelbar durch die in Art. 20 Abs. 1 KI-VO implizierte Deaktivierungsmöglichkeit vorgeschrieben.

355 Obwohl nach dem PrSG keine produktsicherheitsrechtliche Pflicht zum Treffen von konkreten Gefahrenabwendungsmassnahmen besteht, werden in Art. 8 Abs. 5 lit. d PrSG verschiedene Beispiele für Massnahmen genannt. Aufgezählt werden Warnungen, Verkaufsstopps, die Rücknahme vom Markt oder der Rückruf des Produktes. Auch die GPSR zählt als Beispiele die Rücknahme vom Markt oder den Rückruf auf.[1467] In Art. 20 Abs. 1 KI-VO werden als mögliche Korrekturmassnahmen die Rücknahme, die Deaktivierung und der Rückruf aufgezählt.

2. Warnung vor gefährlichen Produkten

356 Die Warnung vor gefährlichen Produkten ist die mildeste Form der Gefahrenabwendung.[1468] Sie besteht für sich allein nur aus einer Information über eine vom Produkt ausgehende Gefahr an den Nutzer des Produktes.[1469] Zu Warnungen von Konsumenten sind Hersteller nach dem PrSG nicht verpflichtet, aus-

1464 S. o., Rn. 84.

1465 NHK GPSR-Piovano, Art. 9 N 104; siehe auch Piovano/Schucht/Wiebe, S. 103; Reusch, Mobile Updates, S. 909.

1466 Siehe auch Oster, in: Foerste/Westphalen, § 57 Rn. 26, der bei einer Aktualisierungspflicht die fehlende Fähigkeit zu Updates als Produktmangel sieht. Eine Aktualisierungspflicht per se gibt es aber weder nach dem PrSG noch nach der GPSR.

1467 Art. 9 Abs. 8 Uabs. 1 lit. a GPSR.

1468 Siehe dazu Röthlisberger, S. 70 f., welcher zwischen der Warnung und der nachträglichen Instruktion differenziert, die sich aber schwer unterscheiden lassen.

1469 Röthlisberger, S. 70.

ser sie werden von den Behörden dazu aufgefordert.[1470] Die KI-VO kennt ebenfalls nur Informationspflichten an Behörden[1471] und Betroffene in der Lieferkette, jedoch nicht für Konsumenten. Anbieter von Hochrisiko-KI-Systemen müssen nach Art. 20 Abs. 1 KI-VO Händler, Betreiber, Bevollmächtigte und Einführer über ergriffene Korrekturmassnahmen informieren. Auch nach Art. 9 Abs. 10 GPSR muss der Hersteller Betroffene in der Lieferkette warnen. Er muss diese sogar über «alle von [ihm] festgestellten Sicherheitsprobleme auf dem Laufenden» halten. Eine einmalige Information reicht demnach nicht.[1472] Ein «Sicherheitsproblem» kann als gegeben angesehen werden, sobald der Hersteller der Meinung ist, dass er Korrekturmassnahmen ergreifen müsse.[1473] Ausführlich geregelt ist in der GPSR im Gegensatz zum PrSG und zur KI-VO die Warnung der Verbraucher: Art. 9 Abs. 8 Uabs. 1 lit. b GPSR verpflichtet den Hersteller explizit dazu, Verbraucher gem. Art. 35 bzw. 36 GPSR über das mit dem Produkt verbundene Risiko und die vorgenommenen Korrekturmassnahmen[1474] zu unterrichten.[1475] Dazu muss der Hersteller gem. Art. 9 Abs. 8 Uabs. 2 GPSR «Angaben zum Risiko für die Gesundheit und Sicherheit von Verbrauchern und zu etwaigen bereits ergriffenen Korrekturmassnahmen sowie, falls verfügbar, zur nach Mitgliedstaat aufgeschlüsselten Anzahl an noch auf dem Markt befindlichen Produkten» machen. Art. 35 GPSR schreibt vor, wie eine Sicherheitswarnung bzw. ein Sicherheitsrückruf durchgeführt werden muss. Art. 36 GPSR präzisiert die Anforderungen an eine schriftliche[1476] Rückrufanzeige.[1477]

Gem. Art. 35 Abs. 1 GPSR müssen Hersteller[1478] alle ermittelbaren betroffenen Verbraucher «direkt und unverzüglich» über einen allfälligen (obligatorischen)[1479] Produktsicherheitsrückruf oder über Informationen, die für eine sichere Verwendung des Produktes nötig sind, informieren. Die Information zur sicheren Verwendung wird in Art. 35 Abs. 1 Satz 1 GPSR als «Sicherheitswarnung» definiert. In Abgrenzung zur öffentlichen Adressierung eines offenen Personenkreises (s.u., Art. 35 Abs. 4 GPSR) ist in Abs. 1 mit «direkt» eine «indi- 357

1470 S. o., Rn. 350.
1471 S. u., Rn. 374.
1472 NHK GPSR-Piovano, Art. 9 N 127.
1473 NHK GPSR-Piovano, Art. 9 N 131.
1474 NHK GPSR-Piovano, Art. 9 N 106.
1475 Siehe auch ErwG 85 GPSR.
1476 A.A. NHK GPSR-Lenz, Art. 36 N 12.
1477 S. u., Rn. 360.
1478 Art. 35 GPSR bezieht sich auf Wirtschaftsakteure (zu welchen der Hersteller gehört) und Anbieter von Online-Marktplätzen.
1479 NHK GPSR-Hartmannsberger, Art. 35 N 14.

viduelle, unmittelbare Kontaktaufnahme» gemeint.[1480] Eine Formvorschrift gibt es für die Sicherheitswarnung nicht.[1481] In Frage kommen also auch Pushnachrichten direkt auf das smarte Produkt bzw. auf das damit verbundene Smartphone via App[1482] oder die Übermittlung der Informationen über Video[1483]. Über Pushnachrichten können bspw. nachträgliche Warnungen oder Instruktionen angezeigt werden. Diese können technisch etwa so eingerichtet werden, dass sie für einige Sekunden nicht weggeklickt werden können oder zumindest bis ans Ende der Nachricht gescrollt werden muss. Kürzere Meldungen sind zu bevorzugen, da längere Texte trotz eben genannter Vorkehrungen zumeist nicht gelesen werden.[1484] Zur Kontaktaufnahme müssen die Verpflichteten die Kundendaten nutzen, die sie erhoben haben.[1485] Art. 35 Abs. 2 GPSR fordert, dass u.a. auch Hersteller, welche Produktregistrierungssysteme oder Kundenbindungsprogramme anbieten, «die die Identifizierung von von Kunden gekauften Produkten zu anderen Zwecken als der Übermittlung von Sicherheitsinformationen an ihre Kunden ermöglichen», ihren Kunden zusätzlich die Möglichkeit geben müssen, «gesonderte Kontaktdaten ausschliesslich zu Sicherheitszwecken zu hinterlegen». Diese zusätzlichen Daten dürfen nur für den Kontakt bei einem Rückruf oder einer Sicherheitswarnung genutzt werden. Art. 35 Abs. 3 GPSR legt fest, dass Durchführungsrechtsakte erlassen werden können, die Registrierungsanforderungen für bestimmte Produkte[1486] vorschreiben, damit Konsumenten sich bei Bedarf direkt über einen Produktrückruf oder eine Sicherheitswarnung benachrichtigen lassen können.[1487] Art. 35 Abs. 4 GPSR hält weiter fest: Falls nicht alle betroffenen Konsumenten kontaktiert werden konnten, müssen die Hersteller «über andere geeignete Kanäle eine klare und sichtbare Rückrufanzeige oder Sicherheits-

1480 NHK GPSR-Hartmannsberger, Art. 35 N 19.

1481 NHK GPSR-Hartmannsberger, Art. 35 N 25.

1482 Ähnlich NHK GPSR-Hartmannsberger, Art. 35 N 19.

1483 Ähnlich in Bezug auf Art. 35 Abs. 4 GPSR NHK GPSR-Hartmannsberger, Art. 35 N 43.

1484 Die in Art. 36 GPSR und in der Vorlage für Rückrufanzeigen namens Berichtigung der Durchführungsverordnung (EU) 2024/1435 der Kommission vom 24. Mai 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates zur Festlegung einer Vorlage für eine Rückrufanzeige (Amtsblatt der Europäischen Union L, 2024/1435, 27. Mai 2024), ABl. L 2024/90426 (zit. Vorlage Rückrufanzeige) festgehaltenen obligatorischen Informationen lassen jedoch nur längere Texte zu.; Die Vorlage sollte eigentlich u.a. einem Informationsüberfluss entgegenwirken, NHK GPSR-Lenz, Art. 36 N 36, m.w.H.; zum Problem des «information overload» siehe auch Heiss/Loacker, in: Heiss/Loacker, § 2 Rn. 2.52.

1485 Art. 35 Abs. 1 GPSR.

1486 Zur Bestimmung dieser Produkte sollen bspw. der Lebenszyklus, die Risiken, die Häufigkeit von Rückrufen und die Nutzerkategorie berücksichtigt werden, ErwG 86 GPSR.

1487 Ausführlich und kritisch dazu NHK GPSR-Hartmannsberger, Art. 35 N 36 ff.

warnung, um die grösstmögliche Reichweite zu gewährleisten, einschliesslich, falls verfügbar, über die Website des Unternehmens, Kanäle auf sozialen Medien, Newsletter und Verkaufsstellen sowie gegebenenfalls Ankündigungen in Massenmedien und anderen Kommunikationskanälen» verbreiten. Zudem müssen diese Informationen «für Menschen mit Behinderungen zugänglich sein». Hier ist HARTMANNSBERGERS einschränkender Auslegung zu folgen: Es wäre unverhältnismässig und unzweckmässig[1488], bereits bei einer einzigen nicht kontaktierbaren Person zu verlangen, dass eine öffentliche Information erfolgen muss.[1489] Vielmehr muss die Anzahl nicht erreichter Verbraucher im Verhältnis zum Total der verkauften Produkte berücksichtigt werden sowie eine Abwägung zwischen der Grösse der Gefahr und dem Erfolg der Massnahme im Verhältnis zum finanziellen und organisatorischen Aufwand des Herstellers stattfinden.[1490] Weiter soll auch die «grösstmögliche Reichweite» dem Verhältnismässigkeitsgrundsatz unterliegen.[1491] Warnungen an Verbraucher seitens Unternehmen können auch direkt über das Safety Business Gateway (ehemals RAPEX)[1492] zur Verfügung gestellt werden.[1493] Auf dem Safety-Gate-Portal können[1494] Hersteller Warnmeldungen für die Öffentlichkeit platzieren. NUSSER spricht sich dafür aus, dass Hersteller eine Pflicht hätten, Verbraucher über Unfälle via das Safety-Gate-Portal zu informieren.[1495] Da die Meldung bei Unfällen nicht an die Verbraucher, sondern an die zuständige Behörde zu richten ist und zudem unabhängig davon erfolgen muss, ob es sich um ein gefährliches Produkt handelt,[1496] kann dieser Auffassung nicht gefolgt werden.

3. Rückruf, Rücknahme vom Markt, Vertriebsstopp

Der Rückruf, die Rücknahme vom Markt und der Vertriebsstopp sind Gefahrenabwendungs- bzw. Korrekturmassnahmen.[1497] Sie zielen alle darauf ab, dass gefährliche Produkte nicht mehr verwendet werden. Hersteller sind nach dem PrSG nicht zu solchen Massnahmen verpflichtet, ausser sie werden von den 358

1488 NHK GPSR-HARTMANNSBERGER, Art. 35 N 42.
1489 NHK GPSR-HARTMANNSBERGER, Art. 35 N 40.
1490 Ähnlich NHK GPSR-HARTMANNSBERGER, Art. 35 N 41.
1491 NHK GPSR-HARTMANNSBERGER, Art. 35 N 44.
1492 S. u., Rn. 376.
1493 Art. 27 Abs. 1, ErwG 68 GPSR; siehe auch NHK GPSR-PIOVANO, Art. 9 N 116, 125.
1494 Art. 9 Abs. 9 GPSR; ebenso NHK GPSR-NUSSER, Art. 34 N 7.
1495 NHK GPSR-NUSSER, Art. 34 N 8.
1496 S. u., Rn. 373.
1497 NHK GPSR-PIOVANO, Art. 9 N 100.

Behörden dazu aufgefordert. Die GPSR und die KI-VO schreiben beide Korrekturmassnahmen vor[1498] und definieren jeweils die Rücknahme[1499] sowie den Rückruf.[1500] Beim Rückruf befindet sich das Produkt bereits am Einsatzort, bei der Rücknahme befindet es sich noch in der Lieferkette. Zusätzlich zum Rückruf und zur Rücknahme wird in Art. 20 Abs. 1 KI-VO auch das «Deaktivieren» genannt. Dieser Begriff wird in der KI-VO nicht definiert. Es handelt sich dabei um «das Ausschalten aus der Ferne».[1501] Das Deaktivieren ist mit einem Rückruf vergleichbar.[1502]

359 Die im letzten Kapitel beschriebene Sicherheitswarnung nach Art. 35 GPSR ist immer nötig, wenn eine Korrekturmassnahme nach Art. 9 Abs. 8 Uabs. 1 lit. a GPSR und eine Meldung nach Art. 9 Abs. 8 Uabs. 1 lit. c GPSR erfolgen, da die Voraussetzungen dieselben sind. Eine Rückrufanzeige nach Art. 35 GPSR ist hingegen nur nötig, wenn das Produkt so gefährlich ist, dass ein Rückruf die einzige wirkungsvolle Korrekturmassnahme des Herstellers nach Art. 9 Abs. 8 Uabs. 1 lit. a GPSR zur Gefahrenabwehr und somit obligatorisch[1503] ist. Das heisst, dass die Vorschriften zur Rückrufanzeige nach Art. 36 GPSR ebenfalls nur bei einem obligatorischen Rückruf beachtet werden müssen.

360 Art. 36 Abs. 1 GPSR bestimmt, wie Rückrufanzeigen zu formulieren sind, falls diese nach Art. 35 Abs. 1 und 4 GPSR schriftlich erfolgen. Art. 36 Abs. 2 GPSR hält fest, dass Rückrufanzeigen für Konsumenten «leicht verständlich» und in den Sprachen der EU-Mitgliedstaaten zu formulieren sind, in denen das Produkt auf dem Markt bereitgestellt wurde. Zudem muss die Anzeige die Überschrift «Produktsicherheitsrückruf» tragen (lit. a), eine «klare Beschreibung des zurückgerufenen Produkts» (lit. b), einschliesslich «Abbildung, Name und Marke» (i), Produktionskennnummern (ii) und, wenn möglich «Angaben dazu, wann, wo und von wem das Produkt verkauft wurde» (iii) enthalten. Weiter muss die Gefahr klar beschrieben werden, wobei verschiedene Formulierungen «zu vermeiden sind», wenn diese «die Risikowahrnehmung der Verbraucher beeinträchtigen können» (lit. c). Lit. d verordnet eine «klare Beschreibung» zum weiteren Vorgehen des Verbrauchers inklusive «einer Anweisung, die Verwendung des zurückgerufenen Produkts unverzüglich einzustellen». Dabei darf nur eine Entsorgung vorgeschrieben werden, wenn diese

1498 S. o., Rn. 353.
1499 Art. 3 Ziff. 26 GPSR; Art. 3 Ziff. 17 KI-VO.
1500 Art. 3 Ziff. 25 GPSR; Art. 3 Ziff. 16 KI-VO.
1501 Beck KI-VO-Eisenberger, Art. 20 N 21.
1502 S. u., Rn. 365.
1503 NHK GPSR-Hartmannsberger, Art. 35 N 14.

«leicht und sicher durchgeführt werden kann».[1504] Lit. e verlangt eine «klare Beschreibung» der verfügbaren Abhilfemassnahmen nach Art. 37 GPSR.[1505] Lit. f verlangt «eine gebührenfreie Telefonnummer oder einen interaktiven Online-Dienst, bei dem Verbraucher mehr Informationen in der oder den jeweiligen Amtssprachen der Union erhalten können». Gem. lit. g muss die Rückrufanzeige zudem eine Aufforderung enthalten, die Informationen über den Rückruf gegebenenfalls an andere Personen weiterzuleiten. Gestützt auf Art. 36 Abs. 3 i.V.m Art. 46 Abs. 2 GPSR hat die Kommission eine Vorlage für Rückrufanzeigen auf dem Weg eines Durchführungsrechtsakts[1506] erlassen, welcher gleichzeitig mit der GPSR in Kraft trat[1507] und noch strengere Vorgaben[1508] als Art. 36 Abs. 2 GPSR vorsieht.

Begründet wird die sehr ausführliche Vorschrift von Art. 36 GPSR damit, dass 361
ein Drittel der Verbraucher gefährliche Produkte weiterverwendet, obwohl sie eine Rückrufanzeige gesehen haben. Dies liege daran, dass die Anzeigen zu kompliziert verfasst seien oder «das Risiko als gering dargestellt wird».[1509] Konsumenten kommen Rückrufen teilweise auch nicht nach, da sie schlicht als zu aufwändig empfunden werden.[1510] Der Rückruf eines Produktes ist für den Hersteller meist die Massnahme, die die grössten Nachteile mit sich bringt. Rückrufe sind meistens teuer, organisatorisch herausfordernd und können zu Reputationsschäden führen.[1511] Diese Nachteile werden für Hersteller aufgrund der einschneidenden Formvorschriften von Art. 36 GPSR und der Abhilfemassnahmen nach Art. 37 GPSR noch verschärft. Diese Verschärfung kann u.U. dazu beitragen, dass ein Rückruf nicht gemacht wird.[1512] Rückrufanzeigen werden z.B. aus Beweisgründen und aufgrund des Aufwands, alternativ alle Betroffenen anzurufen, zumeist schriftlich übermittelt werden und müssen dann die strengen Vorschriften nach Art. 36 GPSR erfüllen. Denkbar wäre es zwar, den Verbrauchern via E-Mail oder über einen anderen Kanal ein Video als Rückrufanzeige zuzustellen. Diese wäre nicht schriftlich und würde damit wohl nicht

1504 Art. 37 Abs. 4 GPSR, siehe auch ErwG 92.
1505 S. u., Rn. 367.
1506 Durchführungsrechtsakte sind rechtlich bindend, siehe Art. 291 Abs. 2 und 3 AEUV.
1507 S. o. zur bereits berichtigten Vorlage Rückrufanzeige Fn. 1487.
1508 NHK GPSR-Lenz, Art. 36 N 38.
1509 ErwG 87 GPSR; siehe auch: NHK GPSR-Lenz, Art. 36 N 6 f. und Kritik m.w.H. in Rn. 14 ff.; Piovano/Schucht/Wiebe, S. 98, m.w.H.
1510 NHK GPSR-Lenz, Art. 36 N 17, m.w.H.; ähnlich Röthlisberger, S. 75 f., m.w.H.
1511 SHK PrSG-Hess, Art. 8 N 13; NHK GPSR-Lenz, Art. 36 N 14; Hartmann/Klindt, S. 76.
1512 NHK GPSR-Lenz, Art. 36 N 28; NHK GPSR-Niermeier, Art. 37 N 35.

den strengen Vorschriften von Art. 36 GPSR unterliegen.[1513] Auch beweisen liesse sich die Zustellung der Information so relativ einfach. Fraglich ist, ob es sich dabei um eine Umgehung von Art. 36 GPSR handeln würde, da die Vorschrift darauf abzielt, dass Konsumenten eindeutige Informationen über Risiken und Möglichkeiten in Zusammenhang mit dem Produktrückruf erhalten.

4. Wiederherstellung der Sicherheit des Produkts

362 Gefahren können auch abgewendet werden, indem die Sicherheit eines Produktes wiederhergestellt wird. Dies geschieht typischerweise durch die Reparatur eines Produktes. Ist die Software reparaturbedürftig, kann diese «over the air» aktualisiert und so eine «Reparatur» des Produktes erwirkt werden.[1514] Ist bei einem Smart Home Device jedoch die Hardware bzw. ein «physisches» Teil des Produktes kaputt, kann dieses natürlich nicht via Update repariert werden. Ist ein Produkt reparaturbedürftig, war traditionellerweise vorgängig eine Warnung nötig, damit der Konsument überhaupt von der Gefahr erfahren und das Produkt zur Reparatur bringen konnte. Software kann nun vom Hersteller (zumindest theoretisch) ohne Meldung an den Konsumenten aktualisiert werden.

363 Eine Reparatur ist neben der herkömmlichen Wiederherstellung der Funktion eines Produktes (bspw. durch den Verbau eines Ersatzteils) auch via Update möglich.[1515] Eine Reparatur mittels Software zur Gefahrenabwendung ist i.d.R. aufwändiger, dafür auch effektiver als eine Warnmeldung. Der Hersteller hat die Möglichkeit, Gefahren zu beheben, indem er Updates zur Verfügung stellt, die entweder vom Nutzer selbst installiert werden können, oder deren Installation er forciert. Dies gilt auch für KI-Systeme.[1516] Zu beachten ist, dass KI-Systeme, die weiterlernen können, und deren Fehler im Lernprozess entstanden sind, nicht durch eine Aktualisierung des Codes «repariert» werden können.[1517] KI-Systeme benötigen in solchen Fällen allenfalls ein erneutes Training, welches z.B. mit anderen Techniken durchgeführt oder mit neuen Trainingsdaten[1518] durchlaufen wird.

1513 Siehe jedoch NHK GPSR-Lenz, Art. 36 N 12, welcher sich dafür ausspricht, dass «alle nicht mündlichen Unterrichtungen der Verbraucher» von Art. 36 GPSR erfasst sein sollen.

1514 Vorbehalten, dass noch eine Verbindung zum Hersteller besteht, siehe Rn. 84.

1515 Siehe auch Art. 37 Abs. 3 GPSR.

1516 Spindler, Vorschläge, Rn. 21.

1517 McGuire, in: Foerste/Westphalen, § 58 Rn. 38 mit Verweis auf Zech, Gutachten, A 72-73.

1518 Siehe dazu bspw. bereits den Vorschlag in Europäische Kommission, Weissbuch KI, S. 18.

Art. 37 Abs. 2 Uabs. 1 lit. a GPSR zählt die Reparatur als eine Abhilfemassnahme auf, die im Falle eines Produktsicherheitsrückrufs angeboten werden kann. Ein Softwareupdate ist nach vorliegender Meinung nicht als Rückruf zu qualifizieren, wenn das Produkt nach dem Update wieder «normal» funktioniert. Die GPSR zielt auf die Sicherheit der Verbraucher in Kombination mit einer Abhilfe[1519] ab. Wird ein Produkt mittels Softwareupdate aktualisiert, ist es möglich, die Sicherheit wiederherzustellen. Die Abhilfe besteht darin, dass das Produkt wieder normal funktionstüchtig ist, gleich wie bei einer herkömmlichen Reparatur. Es handelt sich dann bei der Reparatur in solchen Fällen um eine Gefahrenabwendungs- bzw. Korrekturmassnahme. Durch die Möglichkeit, via Softwareupdate Produkte zu «reparieren», kann der Hersteller auf einen Rückruf und damit auch auf die sehr ausführlichen Rückrufanzeigen verzichten. 364

Wird ein Produkt durch ein Update jedoch unbrauchbar[1520] gemacht, indem Produktfunktionen deaktiviert werden, könnte dies (je nach Ausmass) als Rückruf qualifiziert werden.[1521] Ein Smart Home Device oder eine Software befindet sich dann zwar immer noch beim Konsumenten und wird nicht physisch «zurückgerufen», aber es kann effektiv nicht mehr so genutzt werden, wie dies bspw. beim Kauf vorgesehen war. Das Produkt ist nach einem solchen Update zwar nicht mehr gefährlich, es funktioniert aber auch nicht mehr. 365

5. Weitere Abhilfemassnahmen

Konsumenten tendieren dazu, gefährliche Produkte trotz Warnungen oder Rückrufen weiterhin zu nutzen.[1522] Führt der Hersteller Massnahmen nach Art. 8 Abs. 5 lit. d PrSG durch und verlieren Konsumenten dadurch die Möglichkeit, ihr Produkt zu nutzen, werden sie regelmässig einen Vermögensschaden erleiden. Aus dem PrSG ergibt sich keine Pflicht, für Kosten aufzukommen.[1523] Es handelt sich in der Schweiz um ein rein privatrechtliches Thema.[1524] 366

1519 S. u., Rn. 367.

1520 So forcierte Samsung zwischen 2017 und 2018 mittels Softwareupdate, dass die Ladekapazität des Galaxy Note 7 auf 0 % reduziert wurde, um Konsumenten dazu zu bewegen, das Smartphone zurückzubringen. Die Batterie des Gerätes konnte so stark überhitzen, dass sie anfing zu brennen. OECD, Measuring, S. 9.

1521 Nennt dies «Remote-Sperrung und digitale Deaktivierung» NHK GPSR-Piovano, Art. 9 N 104; In Art. 20 Abs. 1 KI-VO wird das Deaktivieren ebenfalls als Korrekturmassnahme genannt.

1522 Europäische Kommission, CASP 2020, S. 12; implizit Röthlisberger, S. 130.

1523 Botschaft PrSG, S. 7443.

1524 Botschaft PrSG, S. 7443; siehe auch: SHK PrSG-Hess, Art. 8 N 10, Art. 10 N 25; Holliger-Hagmann, Fallstricke, S. 163.

367 Die GPSR verpflichtet in Art. 37 Abs. 1 GPSR den für den Rückruf «verantwortlichen Wirtschaftsakteur»[1525] dazu, Verbrauchern «wirksame, kostenfreie und zeitnahe Abhilfe» anzubieten. Dies gilt unabhängig davon, ob der Wirtschaftsakteur den Rückruf selbst einleitet oder eine zuständige Behörde diesen anordnet. Muss vom Hersteller ein Produktrückruf veranlasst werden, muss er dem Verbraucher eine «Reparatur, Ersatz oder angemessene Erstattung[1526] des Wertes des zurückgerufenen Produkts» anbieten.[1527] Wenn nicht unmöglich oder unverhältnismässig, müssen mindestens zwei dieser Optionen angeboten werden.[1528] Kann der Hersteller keine Reparatur oder keinen Ersatz «innerhalb angemessener Frist und ohne erhebliche Unannehmlichkeiten für den Verbraucher» anbieten, kann sich der Konsument den Wert immer erstatten lassen.[1529] Art. 37 Abs. 3 GPSR hält fest, dass eine Reparatur durch den Verbraucher selbst nur dann als Abhilfemassnahme angeboten werden darf, «wenn sie vom Verbraucher leicht und sicher durchgeführt werden kann und dies in der Rückrufanzeige vorgesehen ist».[1530] Konsumenten müssen dann Anweisungen, Ersatzteile oder – ebenfalls explizit genannt – Software-Aktualisierungen kostenlos zur Verfügung gestellt werden. Art. 37 Abs. 4 GPSR regelt die Entsorgung des Produktes durch Verbraucher. Art. 37 Abs. 5 GPSR hält weiter fest, dass die Abhilfemassnahmen «keine erheblichen Unannehmlichkeiten für den Verbraucher mit sich bringen» und diesem auch keine Kosten in diesem Zusammenhang (z.B. für Versand oder sonstige Rückgabe) auferlegt werden dürfen. Für nicht transportable Produkte muss sogar eine Abholung organisiert werden.

368 Niermeier bezeichnet die Abhilfemassnahmen zu Recht als «Fremdkörper in der GPSR», da sie nicht der öffentlich-rechtlichen präventiven Gefahrenabwehr dienen.[1531] In ErwG 88 der GPSR wird ausgeführt, dass Abhilfemassnahmen bei einem Produktrückruf andere Ziele verfolgen als vertragliche Abhil-

1525 Gemeint ist derjenige, der den Produktsicherheitsrückruf eingeleitet hat oder von der Behörde dazu verpflichtet wurde. Dies wird bei der Anordnung durch die Behörde jeweils der Hersteller sein, ausser dieser hat seinen Sitz nicht in der EU, NHK GPSR-Niermeier, Art. 37 N 14 f.

1526 Zum Erstattungsbetrag siehe auch die Ausführungen in ErwG 91 GPSR.

1527 Art. 37 Abs. 2 Uabs. 1 lit. a–c GPSR, ErwG 91 GPSR.

1528 Art. 37 Abs. 2 Uabs. 2 i.V.m. Art. 37 Abs. 2 Uabs. 1 GPSR.

1529 Art. 37 Abs. 2 Uabs. 3 GPSR; zur einschneidenden Konsequenz dieser Bestimmung für den Hersteller siehe NHK GPSR-Niermeier, Art. 37 N 45.

1530 Siehe auch ErwG 92 GPSR, mit Beispielen.

1531 NHK GPSR-Niermeier, Art. 37 N 8.

fen.[1532] Erstere würden dazu dienen, «gefährliche Produkte vom Markt zu nehmen», und «als eine angemessene Wiedergutmachung für den Verbraucher».[1533] Letztere sollen die Vertragswidrigkeit der Ware beheben. Aus diesen Gründen soll die Inanspruchnahme von Abhilfemassnahmen bei Produktrückrufen keiner zeitlichen Beschränkung unterliegen und Verbraucher müssten nicht nachweisen, dass vom Produkt eine Gefahr ausgehe. Die neuen Abhilfemassnahmen der GPSR sind sehr einschneidend für Hersteller und können für diese zu hohen, nicht voraussehbaren Kosten führen.[1534] Das trifft insbesondere auf die Erstattung des Kaufpreises[1535] und die Übernahme der Kosten für die Rückgabe[1536] zu. Dies könnte dazu führen, dass ein freiwilliger Rückruf nur noch getätigt wird, wenn dieser absolut nötig ist und so gerade einen negativen Einfluss auf die Produktsicherheit hat.[1537] Ausserdem sind die Abhilfemassnahmen zeitlich nicht beschränkt.[1538]

6. Fazit

Die Möglichkeit, Produkte mit integrierter oder eigenständiger Software aus der Ferne zu aktualisieren und dadurch zu verändern, schafft neue Ansätze zur Gefahrenabwehr bei Smart Home Devices. Während in der Schweiz im allgemeinen Produktsicherheitsrecht lediglich die Bereitschaft zur Gefahrenabwendung (Art. 8 Abs. 2 lit. b PrSG) sichergestellt werden muss, sind Hersteller in der EU zu Korrekturmassnahmen zur Gefahrenabwendung (Art. 9 Abs. 8 Uabs. 1 lit. a GPSR) verpflichtet. Einer Pflicht zur Ergreifung von Korrekturmassnahmen nach Art. 20 Abs. 1 KI-VO und von Risikomanagementmassnahmen nach Art. 9 Abs. 2 lit. d KI-VO unterliegen auch Anbieter von Hochrisiko-KI-Systemen. Welche Korrekturmassnahmen ergriffen werden müssen, ist grösstenteils nicht vorgegeben. Nach Art. 9 Abs. 8 Uabs. 1 lit. b GPSR müssen Hersteller die Verbraucher über gefährliche Produkte unterrichten. Nach Art. 9 Abs. 10 GPSR müssen sie Betroffene über Sicherheitsprobleme auf dem Laufenden halten. Auch nach Art. 20 Abs. 1 KI-VO besteht eine Informationspflicht an Betroffene in der Lieferkette über ergriffene Korrekturmassnahmen 369

1532 Die GPSR verweist in ErwG 88 auf zwei Richtlinien, welche vertragliche Abhilfemassnahmen regeln. Konsumenten können jedoch nicht zweimal Abhilfe erhalten. Siehe dazu ErwG 90.

1533 Siehe dazu sehr kritisch NHK GPSR-Niermeier, Art. 37 N 35.

1534 Ausführlich Hartmann/Klindt, S. 76 f.

1535 NHK GPSR-Niermeier, Art. 37 N 21 f., 34 f.

1536 NHK GPSR-Niermeier, Art. 37 N 59.

1537 NP GPSR-Schucht/Wiebe, § 7 N 4.

1538 NHK GPSR-Niermeier, Art. 37 N 34; Hartmann/Klindt, S. 76.

für Anbieter von Hochrisiko-KI-Systemen. Damit Hersteller ihrer Pflicht zur Gefahrenabwendung bei Software und KI-Systemen überhaupt nachkommen können, müssen sie technische Möglichkeiten zur dauerhaften oder zumindest reaktivierbaren Verbindung mit der in Verkehr gebrachten Software vorsehen.

370 Obwohl in der Schweiz keine Pflicht zur Gefahrenabwendung besteht, werden beispielhaft verschiedene Gefahrenabwendungsmassnahmen in Art. 8 Abs. 5 lit. d PrSG genannt. Auch die GPSR und die KI-VO zählen Massnahmen auf. Die wichtigsten Gefahrenabwendungsmassnahmen sind die Warnung der Konsumenten vor gefährlichen Produkten, der Rückruf bzw. die Deaktivierung von sich bereits beim Konsumenten befindenden Produkten, die Rücknahme aus der Lieferkette sowie der Vertriebsstopp und die Wiederherstellung der Sicherheit bspw. durch «Reparaturen» via Updates. Sind Hersteller nach der GPSR zu Korrekturmassnahmen verpflichtet, sind sie gleichzeitig auch zu einer Sicherheitswarnung nach Art. 35 GPSR verpflichtet. Ist sogar ein Rückruf nötig, sind sie zu einer Rückrufanzeige nach Art. 35 GPSR verpflichtet. Zur Sicherheitswarnung und insbesondere zur Rückrufanzeige existieren in Art. 35 und Art. 36 GPSR detaillierte weitere Pflichten. Zudem sind Hersteller nach Art. 37 Abs. 1 GPSR bei einem Rückruf zu weitgehenden Abhilfemassnahmen verpflichtet. In der Schweiz wäre die Umsetzung der neuen Vorgaben der EU eine grosse Einschränkung der Wirtschaftsfreiheit für die Hersteller.[1539] Insbesondere die detaillierten Vorgaben zur Sicherheitswarnung und zur Rückrufanzeige sowie die Abhilfemassnahmen würden dem Hersteller grosse finanzielle Aufwände auferlegen, die schlussendlich für Konsumenten zu teureren Produkten führen könnten.[1540] Sowieso wird in Frage gestellt, ob diese Pflichten sinnvoll sind.[1541]

371 Sinnvoller ist die Fokussierung auf die Wiederherstellbarkeit der Sicherheit bei Produkten, bei denen der Hersteller sich auch nach der Inverkehrbringung noch mit ihnen verbinden kann. Eine solche Verbindung eröffnet dem Hersteller neue Optionen, bei welchen Gefahren direkt korrigiert werden können. Vor allem senken diese Möglichkeiten das Risiko, dass weiterhin gefährliche Produkte auf dem Markt sind, obwohl Verbraucher bereits gewarnt wurden. So sind bei Software und Produkten mit integrierter Software keine weitgehen-

1539 Ähnlich zum deutschen Recht NHK GPSR-Lenz, Art. 36 N 16.

1540 Siehe auch NP GPSR-Schucht/Wiebe, § 7 N 4.

1541 NHK GPSR-Hartmannsberger, Art. 35 N 39; NHK GPSR-Niermeier, Art. 37 N 35; NHK GPSR-Lenz, Art. 36 N 14 f.; NP GPSR-Schucht/Wiebe, § 7 N 4; Hartmann/Klindt, S. 75 ff.; Ackermann/Golling, S. 71.

den Abhilfemassnahmen nötig, wenn der Hersteller bspw. einfach ein Sicherheitsupdate «pushen» und «over the air» installieren kann.

V. Meldepflichten an Behörden

Im allgemeinen Produktsicherheitsrecht der Schweiz werden Hersteller, die ein Produkt in Verkehr gebracht haben, von Art. 8 Abs. 5 PrSG verpflichtet, Gefahren für die Sicherheit oder Gesundheit von natürlichen Personen, die von ihren Produkten ausgehen, an das zuständige Vollzugsorgan zu melden. In der Schweiz müssen bei der Meldung an das zuständige Vollzugsorgan nach Art. 8 Abs. 5 PrSG Angaben zur Identifizierung des Produktes (lit. a), eine Beschreibung der Gefahr, die vom Produkt ausgehen kann (lit. b), Angaben zur Rückverfolgbarkeit (lit. c) und zu den Massnahmen, welche getroffen wurden, um die Gefahr abzuwenden (lit. d), gemacht werden. Die Meldepflicht nach Art. 8 Abs. 5 PrSG gilt nur für Konsumentenprodukte, da Art. 8 Abs. 1 PrSG alle «Bestimmungen dieses Artikels» auf Konsumentenprodukte einschränkt.[1542] Bei herkömmlichen Produkten können gem. Art. 8 Abs. 5 lit. a PrSG bspw. die «Produktart und – soweit bekannt – Marke, besondere Ausstattung, Sonderausführung, Fabrikationsland, Typenbezeichnung, Produktionszeitraum, Seriennummer, Chargennummer, Hersteller-, Importeur- oder Händleradresse»[1543] zu den Identifikationsmerkmalen gehören. Bei Software ist zudem wichtig, dass die richtige Versionsnummer angegeben wird.[1544] Kann der Hersteller nicht herausfinden, welche Softwareversion genau eine Gefahr mit sich bringt, könnte die Behörde unter Umständen davon ausgehen, dass alle Versionen betroffen sind, und als Konsequenz Massnahmen für alle Versionen verordnen. Es liegt also im Interesse des Herstellers, das gefährliche Produkt und somit die betroffene Softwareversion möglichst genau bestimmen zu können.[1545] Bei der Beschreibung der Gefahr nach Art. 8 Abs. 5 lit. b PrSG ist der potenziell resultierende Schaden zu nennen. Ist bereits ein Schaden entstanden, muss dieser ebenfalls beschrieben werden.[1546] Zur Auslösung der Meldepflicht muss jedoch nicht zwingend ein Schaden entstanden sein. Die begründete

372

1542 A.A. Gerster, Rn. 304 ff., der einen Widerspruch zwischen den Formulierungen in Art. 8 Abs. 1 und 5 PrSG sieht. Ein solcher Widerspruch kann nicht erkannt werden, da die Anwendbarkeit der Bestimmung auf Konsumentenprodukte (Art. 8 Abs. 1 PrSG) dem geschützten Personenkreis von allen Verwendern (und damit inklusive Konsumenten) und Dritten (Art. 8 Abs. 5 PrSG) nicht entgegensteht.

1543 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 15.

1544 S. o., Rn. 83.

1545 Siehe auch Furrer, in: Fellmann/Furrer, Schonzeit, S. 91 f.

1546 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 16.

Annahme einer reinen – jedoch konkreten – ernsthaften Gefahr[1547] reicht aus.[1548] Im Gegensatz zum PrHG spielt der Entwicklungsfehler im PrSG keine Rolle und es müssen auch Gefahren gemeldet werden, die bereits während des Inverkehrbringens erkennbar gewesen wären.[1549] Art. 8 Abs. 5 lit. c PrSG verlangt, dass alle verfügbaren Angaben zur Rückverfolgbarkeit[1550] gemacht werden. Dies soll es den Vollzugsorganen ermöglichen, nicht nur Massnahmen bezüglich der Produkte, die sich bereits bei Konsumenten oder «in den Verkaufskanälen» befinden, zu treffen. Produkte, die in Lagern von Zwischenhändlern, Importeuren und Herstellern liegen, sollen rückverfolgt und wenn nötig durch Massnahmen ungefährlich gemacht werden.[1551] Angaben zu Endkonsumenten müssen nicht gemacht werden können, da die Rückverfolgungspflicht nur bis zur letzten Vertriebsstufe gilt.[1552] Weiter müssen gem. Art. 8 Abs. 5 lit. d PrSG alle Massnahmen genannt werden, die zur Gefahrenabwendung bereits getroffen wurden. Da jedoch nach dem PrSG keine Verpflichtung zur Ergreifung von Massnahmen besteht, ohne dass eine Behörde diese verordnet hat, ist es für die Meldung nicht nötig (aber empfohlen!), dass bereits Massnahmen getroffen wurden.[1553] Beispielhaft aufgezählt werden Warnungen, Verkaufsstopps, Rücknahmen vom Markt und der Rückruf von Produkten. Da diese Massnahmen nicht abschliessend sind,[1554] können bspw. auch Softwareupdates als Massnahme zur Gefahrenabwendung gemeldet werden. Art. 8 Abs. 5 lit. d PrSG gewährt dem Hersteller die Freiheit, selbst angemessene Massnahmen vorzuschlagen und zu ergreifen.[1555] Hält die Behörde die Massnahmen für ausreichend, hat er so die Chance, dass keine weitergehenden Massnahmen verfügt werden.

373 Nach Art. 9 Abs. 8 Uabs. 1 lit. c GPSR müssen Hersteller gefährliche Produkte an die Marktüberwachungsbehörden der Mitgliedstaaten, in denen das Produkt auf dem Markt bereitgestellt wurde, melden. Bei der Zurverfügungstellung der Informationen über gefährliche Produkte an die Marktüberwa-

1547 S. o., Rn. 316.

1548 SHK PrSG-Hess, Art. 8 N 41 m.w.H.; Holliger-Hagmann, Fallstricke, S. 168; Fellmann, Jusletter 25.10.2010, Rn. 39, 41; zustimmend Gerster, Rn. 303.

1549 SHK PrSG-Hess, Art. 8 N 39 Fn. 124, mit Verweis auf Holliger-Hagmann, Fallstricke, S. 168, welche a.A. ist.

1550 Die Sicherstellung der Rückverfolgbarkeit nach Art. 8 Abs. 2 lit. c PrSG ist eine Vormarktpflicht und wird deshalb nicht im Detail ausgeführt, s. u., Rn. 383.

1551 Botschaft PrSG, S. 7443.

1552 Botschaft PrSG, S. 7442; siehe auch: Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 17; Fellmann, Jusletter 25.10.2010, Rn. 33.

1553 A.A. Furrer, in: Fellmann/Furrer, Schonzeit, S. 103.

1554 Botschaft PrSG, S. 7443; siehe auch: Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 18; Fellmann, Jusletter 25.10.2010, Rn. 54.

1555 Furrer, in: Fellmann/Furrer, Schonzeit, S. 102 f.

chungsbehörden müssen gem. Art. 9 Abs. 8 Uabs. 2 GPSR «insbesondere Angaben zum Risiko für die Gesundheit und Sicherheit von Verbrauchern und zu etwaigen bereits ergriffenen Korrekturmassnahmen sowie, falls verfügbar, zur nach Mitgliedstaat aufgeschlüsselten Anzahl an noch auf dem Markt befindlichen Produkten» gemacht werden. Art. 20 Abs. 1 GPSR sieht bei einem Unfall, der durch ein in Verkehr gebrachtes oder bereitgestelltes Produkt verursacht wurde, eine Meldepflicht an die Behörde vor, selbst wenn es sich nicht per se um ein gefährliches Produkt handelt.[1556] Ein Unfall kann jedoch auf eine potenzielle Gefahr hinweisen.[1557] Die Meldung über Unfälle nach Art. 20 Abs. 1 GPSR an die Behörde «umfasst die Art und die Identifikationsnummer des Produkts sowie die Umstände des Unfalls, sofern bekannt». Gem. Art. 20 Abs. 2 GPSR meldet der Hersteller «für die Zwecke des Absatzes 1 [...] die im Zusammenhang mit der Verwendung eines Produkts eingetretenen Vorkommnisse, die zum Tod eines Menschen oder zu schwerwiegenden dauerhaften oder zeitweiligen nachteiligen Auswirkungen auf die Gesundheit und Sicherheit dieses Menschen, einschliesslich Verletzungen, anderer körperlicher Schädigungen, Krankheiten und chronischer Gesundheitsauswirkungen, geführt haben».

Auch nach der KI-VO besteht für Anbieter eine Meldepflicht für gefährliche Hochrisiko-KI-Systeme nach Art. 20 Abs. 2 KI-VO und schwerwiegende Vorfälle gem. Art. 73 Abs. 1 KI-VO. Bei einem erkannten Risiko für die Gesundheit, Sicherheit oder Grundrechte von Personen muss der Anbieter eines Hochrisiko-KI-Systems nach Art. 20 Abs. 2 i.V.m. Art. 79 Abs. 1 KI-VO unverzüglich die Marktüberwachungsbehörden und gegebenenfalls die notifizierten Stellen informieren. Zu melden sind nach Art. 20 Abs. 2 KI-VO insbesondere die Art der Nichtkonformität und die bereits ergriffenen relevanten Korrekturmassnahmen. Ziel dieser Pflicht ist es, der Marktüberwachungsbehörde und der notifizierten Stelle die erforderlichen Informationen zu übermitteln, damit sie ihre Aufgaben erfüllen können.[1558] Gem. Art. 73 Abs. 1 KI-VO besteht eine weitere Meldepflicht für Anbieter von Hochrisiko-KI-Systemen. Schwerwiegende Vorfälle müssen demnach an die Marktüberwachungsbehörden des EU-Mitgliedstaates gemeldet werden, in welchem der Vorfall stattgefunden hat. Die Drohung einer Gefahr genügt somit nicht für eine Meldepflicht nach Art. 73 KI-VO, da ein Vorfall bereits stattgefunden haben muss. Dies im Gegensatz zur Meldepflicht nach Art. 20 Abs. 2 KI-VO. Die Erkennung von schwerwiegenden Vorfällen kann bspw. durch die Beobachtung nach dem Inverkehrbringen gem. 374

1556 NHK GPSR-Wiebe, Art. 20 N 2.
1557 ErwG 43 GPSR; NHK GPSR-Wiebe, Art. 20 N 2.
1558 Beck KI-VO-Eisenberger, Art. 20 N 23.

Art. 72 Abs. 1 KI-VO[1559] oder Art. 9 Abs. 2 KI-VO geschehen. Weiter können Anbieter durch Betreiber über schwerwiegende Vorfälle informiert werden.[1560] Ein schwerwiegender Vorfall ist in Art. 3 Ziff. 49 KI-VO definiert als «ei[n] Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat: den Tod oder die schwere gesundheitliche Schädigung einer Person [lit. a], eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen [lit. b], die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte [lit. c]» oder «schwere Sach- oder Umweltschäden [lit. d]».[1561] Während Art. 3 Ziff. 49 lit. a KI-VO die im Produktsicherheitsrecht klassischerweise geschützten Rechtsgüter «Sicherheit» und «Gesundheit» schützt, schützen lit. b bis d zusätzliche Rechtsgüter. Vorausgesetzt wird ein Kausalzusammenhang zwischen dem Vorfall bzw. der Fehlfunktion und den Folgen nach lit. a bis d.[1562] Möglich ist gem. Art. 73 Abs. 5 KI-VO auch eine unvollständige Meldung, der eine vollständige Nachmeldung folgt. Gem. Art. 73 Abs. 7 KI-VO stellt die EU bis zum 25. August 2025 Leitlinien zur Verfügung, die die Einhaltung von Art. 73 Abs. 1 KI-VO erleichtern sollen. Das Verfahren zur Meldung eines schwerwiegenden Vorfalls gem. Art. 73 ist Teil des Qualitätsmanagements.[1563] Nach einer Meldung gem. Art. 73 Abs. 1 KI-VO muss der Anbieter eines Hochrisiko-KI-Systems «unverzüglich die erforderlichen Untersuchungen im Zusammenhang mit dem schwerwiegenden Vorfall und dem betroffenen KI-System» durchführen.[1564] Zur Untersuchung gehören gem. Art. 73 Abs. 6 Uabs. 1 KI-VO eine Risikobewertung des Vorfalls und Korrekturmassnahmen. Nach Art. 73 Abs. 6 Uabs. 2 KI-VO muss der Anbieter bei der Untersuchung mit den zuständigen Behörden und allenfalls der notifizierten Stelle zusammenarbeiten. Er darf zudem keine Untersuchung vornehmen, «die zu einer Veränderung des betroffenen KI-Systems in einer Weise führt, die möglicherweise Auswirkungen auf eine spätere Bewertung der Ursachen des Vorfalls hat, bevor er die zuständigen Behörden über solche Massnahmen nicht unterrichtet hat».[1565] Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko[1566] müssen gem. Art. 55 Abs. 1 lit. c KI-VO Informationen über schwerwiegende Vorfälle und mögliche Abhilfe-

1559 Siehe auch Beck KI-VO-Hartmann, Art. 73 N 2.
1560 Beck KI-VO-Hartmann, Art. 73 N 2.
1561 Siehe auch ErwG 155 KI-VO.
1562 Beck KI-VO-Hartmann, Art. 73 N 8.
1563 Art. 17 Abs. 1 lit. i KI-VO.
1564 Art. 73 Abs. 6 Uabs. 1 KI-VO.
1565 Art. 73 Abs. 6 Uabs. 2 KI-VO.
1566 S. o., Rn. 133.

massnahmen erfassen, dokumentieren und melden. Empfänger der Meldung sind hier das Büro für Künstliche Intelligenz sowie gegebenenfalls die zuständigen nationalen Behörden.

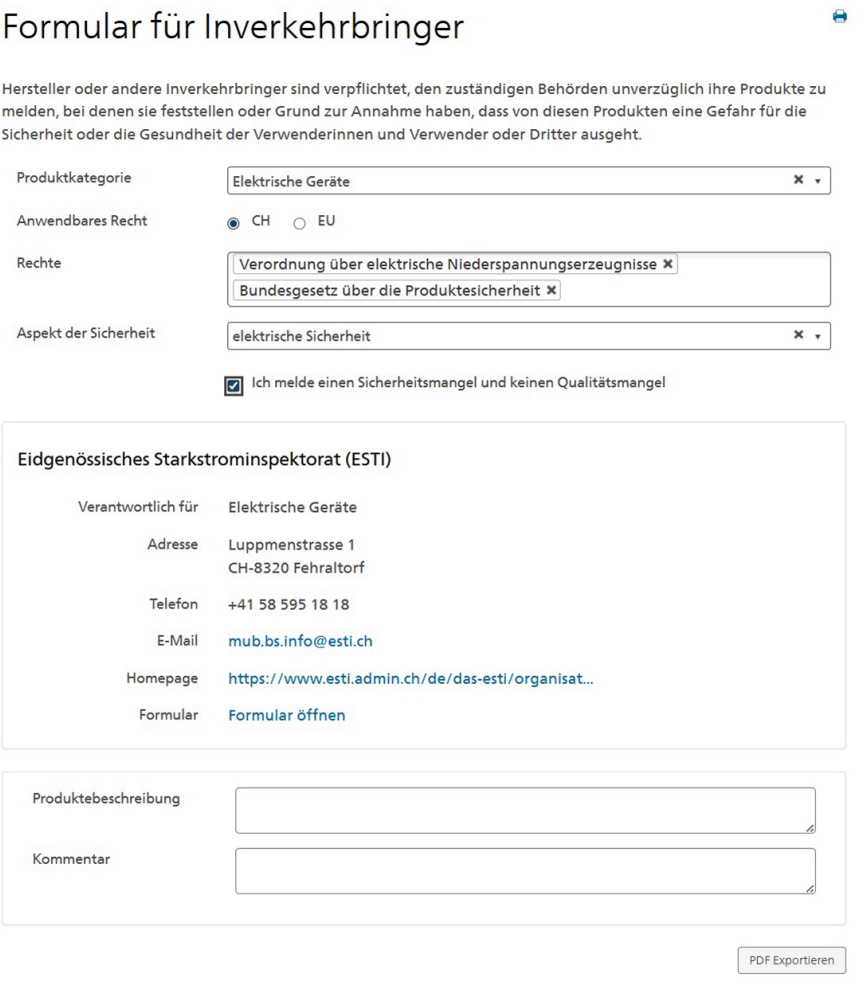

Abbildung 10: *Formular für Inverkehrbringer*[1569]

[1567] Formular für Inverkehrbringer, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Arbeit/Arbeitsbedingungen/Produktsicherheit/meldung_gefaehrlicher_produkte/meldung_gefaehrlicher_produkte_inverkehrbringer.html>, zuletzt besucht am 31.05.2025.

375 Obwohl in der Schweiz keine Formvorschrift zur Meldung besteht, wird eine einheitliche Art zur Meldung angestrebt.[1568] Auf der Website des SECO können Hersteller und andere Inverkehrbringer zur Meldung ein Onlineformular ausfüllen.[1569] Unter Einbezug der gewählten Produktkategorie, des anwendbaren Sektorrechts und gegebenenfalls weiterer Angaben (wie des Verwendungsbereichs oder Aspekten der Sicherheit) wird (meistens) ein weiteres Formular generiert und die zuständige Stelle angezeigt, an welche gemeldet werden muss (Abbildung 10).

376 Die Meldung gem. Art. 9 Abs. 8 Uabs. 1 lit. c GPSR an die Marktüberwachungsbehörde erfolgt via Safety Business Gateway. Das Safety Gate (ehemals RAPEX) ist ein Webportal[1570] der EU, das als Meldeplattform für gefährliche Non-Food-Produkte dient, und besteht aus dem Schnellwarnsystem Safety Gate[1571], dem Safety-Gate-Portal[1572] und dem Safety Business Gateway[1573].[1574] Das Schnellwarnsystem Safety Gate dient dem Informationsaustausch über Massnahmen im Zusammenhang mit gefährlichen Produkten zwischen Behörden und der Europäischen Kommission.

1. Meldefrist

377 Wie bereits nach Art. 5 Abs. 3 Produktsicherheitsrichtlinie müssen Meldungen gem. Art. 8 Abs. 5 PrSG, Art. 9 Abs. 8 Uabs. 1 GPSR, Art. 20 Abs. 1 GPSR und Art. 35 Abs. 1 GPSR «unverzüglich» erfolgen. Die – nun ausser Kraft getretene – europäische Leitlinie zur Meldung nach Art. 5 Abs. 3 Produktsicherheitsrichtlinie gab eine maximale Frist von zehn («nach dem Vorliegen meldefähiger Informationen über die Existenz eines gefährlichen Produkts, auch bei noch laufenden Untersuchungen») bzw. drei (bei einem ernsten Risiko) Kalendertagen an.[1575]

1568 Siehe auch SHK PrSG-Hess, Art. 8 N 44.

1569 Formular für Inverkehrbringer, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Arbeit/Arbeitsbedingungen/Produktsicherheit/meldung_gefaehrlicher_produkte/meldung_gefaehrlicher_produkte_inverkehrbringer.html>, zuletzt besucht am 31.05.2025.

1570 Safety Gate: the EU rapid alert system for dangerous non-food products, abrufbar unter <https://ec.europa.eu/safety-gate-alerts/screen/search?resetSearch=true>, zuletzt besucht am 31.05.2025.

1571 Art. 25 GPSR.

1572 Art. 34 GPSR.

1573 Art. 27 GPSR.

1574 ErwG 68 GPSR.

1575 Entscheidung der Kommission vom 14. Dezember 2004 zur Festlegung von Leitlinien für die Meldung gefährlicher Verbrauchsgüter bei den zuständigen Behörden der Mitgliedstaaten durch Hersteller und Händler nach Artikel 5 Absatz 3 der Richtlinie 2001/95/

Für die Schweiz führen die – rechtlich nicht verbindlichen – FAQ des SECO in Kapitel D.8 «1 oder 2 Tage, je nach Auswirkung des Sicherheitsmangels auf die Sicherheit und Gesundheit von Personen» auf. Die FAQ begründen die Frist als so kurz, weil vom Vollzugsorgan nötigenfalls weitere Massnahmen gem. Art. 10 PrSG angeordnet werden müssen.[1576] Als Beispiel wird die Warnung der Bevölkerung genannt, falls diese nicht rechtzeitig durch den Hersteller oder Importeur erfolgt.[1577] Es ist nachvollziehbar, dass das Ressort Produktesicherheit des SECO, welches die FAQ erstellt hat, möglichst kurze Fristen vorzieht, da ihm (bzw. der vom SECO dazu beauftragten BFU) damit die Aufsicht erleichtert wird. Unternehmen haben in derartigen Konstellationen jedoch regelmässig ein Eigeninteresse daran, möglichst zeitnah Massnahmen zu ergreifen – etwa zum Schutz ihrer Reputation oder zur Abwehr möglicher Ansprüche aus Gewährleistung und Haftung.[1578] Gem. h.L. ist diese Frist zu kurz, da zuerst relevante Informationen aufgearbeitet werden müssen und abgeklärt werden muss, ob überhaupt eine Meldepflicht besteht.[1579] Vertreten wird, dass die Meldung «ohne schuldhaftes Zögern» erfolgen soll, da eine starre Frist nicht sinnvoll ist und es auf den Einzelfall ankommt.[1580] Eine gestaffelte Rapportierung – wie von Hess vorgeschlagen[1581] – lehnt Fellmann ab, da die Behörde erst geeignete Massnahmen treffen kann, wenn sie über alle Informationen verfügt.[1582] Eine Meldung soll aber nicht erfolgen müssen, wenn die Gefahr nicht genügend substantiiert ist.[1583] 378

Nachdem im Entwurf zur GPSR noch feste Fristen vorgeschlagen wurden, wurde in der finalen Fassung bewusst darauf verzichtet.[1584] Da der Hersteller die Behörden nach Art. 9 Abs. 8 Uabs. 1 lit. c GPSR auch über die Korrekturmassnahmen nach Art. 9 Abs. 8 Uabs. 1 lit. a GPSR informieren muss, muss er zuerst darüber entscheiden, welche Korrekturmassnahmen angemessen und 379

EG des Europäischen Parlaments und des Rates, ausser Kraft, Anhang Ziff. 4.3; siehe auch: Fellmann, Jusletter 25.10.2010, Rn. 51; NHK GPSR-Piovano, Art. 9 N 90 f.; NHK GPSR-Wiebe, Art. 20 N 19.

1576 Siehe auch Haas/Leutwiler, S. 458, ohne diese kurze Frist zu hinterfragen.

1577 SECO, FAQ, S. 12.

1578 Furrer, in: Fellmann/Furrer, Schonzeit, S. 105, mit ausführlicher Kritik an den FAQ.

1579 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 14; Furrer, in: Fellmann/Furrer, Schonzeit, S. 103 ff.; Fellmann, Jusletter 25.10.2010, Rn. 51.

1580 Haftpflichtkommentar-Holliger-Hagmann, Art. 8 PrSG N 14; Fellmann, Jusletter 25.10.2010, Rn. 51; Furrer, in: Fellmann/Furrer, Schonzeit, S. 105.

1581 SHK PrSG-Hess, Art. 8 N 43.

1582 Fellmann, Jusletter 25.10.2010, Rn. 52.

1583 S. o., Rn. 372.

1584 NHK GPSR-Piovano, Art. 9 N 91, m.w.H.

durchzuführen sind.[1585] Nach der Entscheidung über die Korrekturmassnahmen muss die Meldung an die Behörde erfolgen.[1586] Bei der Meldung eines Unfalls ist die Frist ebenfalls flexibel.[1587] Die Frist beginnt gem. Art. 20 Abs. 1 GPSR, sobald der Hersteller Kenntnis vom Unfall hat. Das heisst, dass ein blosser Verdacht nicht ausreicht, gleichzeitig aber auch nicht alle Einzelheiten bekannt sein müssen.[1588] WIEBE schlägt im Sinne einer «grobe[n] Orientierungshilfe»[1589] vor, im Einklang mit der obengenannten Leitlinie auf die Folgenschwere abzustellen und bei «schweren Gesundheitsschäden» innerhalb von drei Kalendertagen bzw. bei Todesfolge «auf schnellstem Wege» zu melden.[1590] Ebenfalls «unverzüglich» muss die Information an Verbraucher bezüglich einer Sicherheitswarnung oder eines Produktsicherheitsrückrufs nach Art. 35 Abs. 1 GPSR erfolgen. Auch hier wird eine starre Frist als nicht angemessen beurteilt und festgestellt, dass eine Einzelfallbeurteilung nötig ist.[1591] Startzeitpunkt dieser Frist ist jener Moment, in dem der Hersteller feststellt, dass er eine Pflicht hat, ein Produkt zurückzurufen[1592] bzw. eine Sicherheitswarnung auszusprechen. Danach wird der Hersteller einige Werktage benötigen, um die Meldung an die Verbraucher aufzubereiten und die zu informierenden Kunden zu ermitteln.[1593] Je grösser die Gefahr ist, desto schneller muss der Hersteller melden.[1594]

380 Die Meldung muss grundsätzlich sofort erfolgen, sobald der Anbieter einen Kausalzusammenhang zwischen dem KI-System und dem schwerwiegenden Vorfall feststellt oder ein solcher Zusammenhang wahrscheinlich ist.[1595] Art. 73 Abs. 3 KI-VO verlangt eine unverzügliche Meldung ohne Verweis auf einen nötigen Kausalzusammenhang, mit einer Verlängerung dieser Frist auf maximal zwei Tage, nachdem der Anbieter Kenntnis vom Vorfall erlangt hat. Da die Definition des schwerwiegenden Vorfalls nach Art. 3 Ziff. 49 KI-VO bereits einen Kausalzusammenhang zwischen dem Vorfall bzw. der Fehlfunktion und den aufgelisteten Folgen voraussetzt, kann es gar keine Meldung ohne festgestellte

1585 NHK GPSR-PIOVANO, Art. 9 N 92, 95, m.w.H.
1586 NHK GPSR-PIOVANO, Art. 9 N 95.
1587 NHK GPSR-WIEBE, Art. 20 N 19.
1588 NHK GPSR-WIEBE, Art. 20 N 21.
1589 NHK GPSR-WIEBE, Art. 20 N 20.
1590 NHK GPSR-WIEBE, Art. 20 N 19.
1591 NHK GPSR-HARTMANNSBERGER, Art. 35 N 21.
1592 NHK GPSR-HARTMANNSBERGER, Art. 35 N 21.
1593 NHK GPSR-HARTMANNSBERGER, Art. 35 N 21.
1594 NHK GPSR-PIOVANO, Art. 9 N 95; NHK GPSR-WIEBE, Art. 20 N 19; NHK GPSR-HARTMANNSBERGER, Art. 35 N 21.
1595 Art. 73 Abs. 2 bis 4 KI-VO; siehe auch Beck KI-VO-HARTMANN, Art. 73 N 10.

Kausalität geben.[1596] Die Meldung eines schwerwiegenden Vorfalles muss aber spätestens 15 Tage nach dem Zeitpunkt gemacht werden, an dem der Anbieter davon erfahren hat.[1597] Starb eine Person aufgrund des zu meldenden Vorfalles, muss der Anbieter gem. Art. 73 Abs. 4 KI-VO spätestens 10 Tage nach dem Datum, an dem er vom Vorfall erfahren hat, eine Meldung erstatten.[1598] Der Anbieter muss schwerwiegende Vorfälle, die nach Art. 3 Ziff. 49 lit. b KI-VO eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen zur Folge haben oder einem «weitverbreiteten Verstoss» entsprechen, spätestens nach zwei Tagen, nachdem er Kenntnis darüber erlangt hat, melden.[1599] Je schwerer die Folgen des Vorfalls sind, desto schneller muss die Meldung geschehen.[1600] Gem. der Meldepflicht nach Art. 20 Abs. 2 KI-VO ist die Information an die Marktüberwachungsbehörden und allenfalls die notifizierte Stelle unverzüglich, also wieder «ohne schuldhaftes Zögern» geschuldet.[1601]

2. Empfänger der Meldung

Das zuständige Vollzugsorgan, an welches eine Meldung nach Art. 8 Abs. 5 PrSG erfolgt, ist abhängig vom gefährlichen Produkt.[1602] Hinweise zum zuständigen Vollzugsorgan finden sich in der PrSV, der ZustV-PrSV[1603] und den verschiedenen sektorrechtlichen Erlassen. Die Stelle, an die zu melden ist, lässt sich in der Praxis am einfachsten via Meldeformular für Inverkehrbringer des SECO finden.[1604] Dies ist bei Smart Home Devices bspw. gem. Art. 4 Abs. 1 NEV i.V.m Art. 2 Abs. 1 lit. f ESTI-Verordnung[1605] das Eidgenössische Starkstrominspektorat (ESTI).[1606] Das ESTI ist die Marktüberwachungsbehörde für elektri- 381

1596 Ebenso und ausführlich mit Verweis auf den Entwurf zur KI-VO, dem dieser Widerspruch entstammt, weil ursprünglich potenzielle Folgen ebenfalls vom schwerwiegenden Vorfall erfasst waren: Beck KI-VO-Hartmann, Art. 73 N 11.

1597 Art. 73 Abs. 2 Uabs. 1 KI-VO.

1598 Art. 73 Abs. 4 KI-VO.

1599 Art. 73 Abs. 3 KI-VO.

1600 Art. 73 Abs. 2 Uabs. 2 KI-VO.

1601 Siehe auch Beck KI-VO-Eisenberger, Art. 20 N 27 f.

1602 Furrer, in: Fellmann/Furrer, Schonzeit, S. 106.

1603 Verordnung des WBF über den Vollzug der Marktüberwachung nach dem 5. Abschnitt der Verordnung über die Produktesicherheit vom 18. Juni 2010, SR 930.111.5 (zit. ZustV-PrSV).

1604 S. u., Rn. 375.

1605 Verordnung über das Eidgenössische Starkstrominspektorat vom 7. Dezember 1992, SR 734.24 (zit. ESTI-Verordnung).

1606 Auch für Funkanlagen ist das ESTI für Aspekte betreffend den Schutz der Gesundheit und Sicherheit die zuständige Behörde nach Art. 36 Abs. 1 FAV.

sche Niederspannungserzeugnisse.[1607] Es spricht bspw. Verkaufsverbote aus und publiziert Rückrufe sowie Sicherheitswarnungen.[1608] Anerkennt man Software als eigenständiges Produkt und ist diese unabhängig von einem elektrischen Gerät oder einem anderen sektorrechtlich erfassten Produkt[1609] zu beurteilen, fällt Software (und damit auch KI) unter das PrSG. Die zuständige Behörde für solche «übrigen» Produkte, die unter keinen Spezialerlass fallen, ist die BFU.[1610] Art. 23 GPSR und Art. 3 Ziff. 25 KI-VO halten fest, dass die EU-Mitgliedstaaten eigene nationale Marktüberwachungsbehörden bezeichnen, und verweisen weitgehend auf die MÜVO. Welche Marktüberwachungsbehörden in der EU für Software und KI zuständig sind, ist vorliegend irrelevant.

3. Fazit

382 Das PrSG, die GPSR und die KI-VO kennen alle Meldepflichten an Behörden. Im allgemeinen Produktsicherheitsrecht der Schweiz werden Hersteller, die ein Produkt in Verkehr gebracht haben, von Art. 8 Abs. 5 PrSG verpflichtet, gefährliche Produkte an das zuständige Vollzugsorgan zu melden. In der EU unterliegen Hersteller ebenfalls einer Meldepflicht gem. Art. 9 Abs. 8 Uabs. 1 lit. c GPSR über gefährliche Produkte und gem. Art. 20 Abs. 1 GPSR über Unfälle an die zuständigen Behörden. Auch nach der KI-VO besteht für Anbieter eine Meldepflicht für gefährliche Hochrisiko-KI-Systeme nach Art. 20 Abs. 2 KI-VO und schwerwiegende Vorfälle gem. Art. 73 Abs. 1 KI-VO. In der GPSR werden Meldungen über Unfälle verlangt, unabhängig davon, ob ein Produkt tatsächlich gefährlich ist. Dies geht über die Meldepflicht des PrSG hinaus. Das PrSG und die GPSR kennen nach der Meldung keine Verpflichtungen mehr, wenn sie nicht von den Behörden angeordnet werden. Die KI-VO hingegen verpflichtet Anbieter in Art. 73 Abs. 6 KI-VO nach einem Vorfall zu einer unverzüglichen Untersuchung und verbietet Änderungen am Hochrisiko-KI-System, bevor die Behörden über solche Massnahmen informiert sind. Während das PrSG und die GPSR keine starren Meldefristen vorschreiben, gibt es diese in der KI-VO. In allen Erlassen gilt aber, dass umso schneller zu melden ist, je grösser die Gefahr ist.

1607 Siehe auch ESTI, Aufsichts- und Kontrollaufgaben, S. 89.

1608 ESTI, Tätigkeitsbericht, S. 16.

1609 S. o., Rn. 178 f.

1610 Art. 20 Abs. 1 lit. b PrSV; Art. 3 i.V.m. Anhang lit. h Ziff. 2 ZustV-PrSV; siehe auch: BVGer C-1177/2012 vom 12.06.2014, E.1.2.; Produktesicherheit – Übersicht, abrufbar unter <https://www.seco.admin.ch/seco/de/home/Arbeit/Arbeitsbedingungen/Produktsicherheit.html>, zuletzt besucht am 31.05.2025.

VI. Aufbewahrungs- und Aktualisierungspflichten

Nach Art. 8 Abs. 2 lit. c PrSG muss der Hersteller ein Produkt, das er in Verkehr bringt, rückverfolgen können. Damit ein Produkt innerhalb der Lieferkette zurückverfolgt werden kann, müssen die Voraussetzungen (z.B. Vergeben einer Versionsnummer, Dokumentation, wann das Produkt wem zugänglich gemacht wurde) bereits vor der Inverkehrbringung sichergestellt werden. Es handelt sich bei der Sicherstellung der Rückverfolgbarkeit deshalb um eine Vormarktpflicht. Damit die Rückverfolgung jedoch möglich ist, müssen die dazugehörigen Informationen aufbewahrt werden. Bei der Aufbewahrungspflicht der Informationen zur Rückverfolgung handelt es sich deshalb um eine Nachmarktpflicht, die sich aus Art. 8 Abs. 2 lit. c PrSG ergibt. Art. 10 Abs. 1 PrSV schreibt zudem vor, dass zum Nachweis der Erfüllung der Anforderungen nach Art. 3 bis 5 PrSG alle erforderlichen technischen Unterlagen sowie die Konformitätserklärung während der Gebrauchsdauer[1611] und mindestens während zehn Jahren ab der Herstellung beigebracht werden können müssen.[1612] Es wird in Art. 10 Abs. 1 PrSV explizit festgelegt, dass die Frist bei der Herstellung von Serienprodukten erst mit dem letzten Exemplar zu laufen beginnt. 383

Auch die GPSR enthält Pflichten, bestimmte Informationen aufzubewahren. So verpflichtet Art. 9 Abs. 3 GPSR den Hersteller, seine technischen Unterlagen aktuell und für zehn Jahre ab dem Inverkehrbringen bereitzuhalten, falls sie von einer Marktüberwachungsbehörde verlangt werden sollten. Es wird insbesondere verlangt, dass Informationen über Massnahmen inklusive Beschreibung des mit dem Produkt verbundenen Risikos, der damit in Zusammenhang stehenden Beschwerden und der bekannten Unfälle sowie allenfalls der ergriffenen Korrekturmassnahmen zehn Jahre lang ab Bezug oder Lieferung aufbewahrt werden.[1613] Zudem müssen auch nach der GPSR Informationen zur Rückverfolgbarkeit aufbewahrt werden. Explizit genannt ist u.a., dass die Information über alle Wirtschaftsakteure, von denen der Hersteller eine Software, die in das Produkt eingebettet ist, bezogen hat, für sechs Jahre aufbewahrt werden muss.[1614] 384

Die KI-VO enthält ebenfalls Aufbewahrungs- und Aktualisierungspflichten. Art. 18 Abs. 1 KI-VO verpflichtet den Anbieter von Hochrisiko-KI-Systemen dazu, verschiedene Unterlagen (lit. a bis e) für zehn Jahre nach dem Inverkehr- 385

1611 S. u., Rn. 395 ff.

1612 Siehe auch BVGer A-2734/2020 vom 02.08.2021, E. 6.6.

1613 Art. 15 Abs. 2 i.V.m. Abs. 4 GPSR.

1614 Art. 15 Abs. 3 i.V.m. Abs. 5 GPSR.

bringen oder der Inbetriebnahme für die zuständigen nationalen Behörden aufzubewahren. Es handelt sich dabei um die in Art. 11 KI-VO genannte technische Dokumentation (lit. a), die Dokumentation zum in Art. 17 KI-VO genannten Qualitätsmanagementsystem (lit. b), die Dokumentation über etwaige von notifizierten Stellen genehmigte Änderungen (lit. c), gegebenenfalls die von den notifizierten Stellen ausgestellten Entscheidungen und sonstigen Dokumente (lit. d) und die in Art. 47 KI-VO genannte EU-Konformitätserklärung (lit. e). Gem. Art. 18 Abs. 2 KI-VO müssen die Mitgliedstaaten selbst die Bedingungen zur Bereithaltung der Unterlagen festlegen, falls der Anbieter vor Ablauf der zehn Jahre in Konkurs geht oder seine Tätigkeit aufgibt. Die Dokumentation ist vor der Inverkehrbringung zu erstellen[1615] und enthält bspw. auch den Plan für die Beobachtung nach dem Inverkehrbringen[1616]. Art. 19 Abs. 1 KI-VO schreibt dem Anbieter von Hochrisiko-KI-Systemen vor, dass er die automatisch erzeugten Protokolle gem. Art. 12 Abs. 1 KI-VO[1617] mindestens für sechs Monate aufbewahren muss.[1618] Weiter müssen diese Anbieter gem. Art. 21 Abs. 1 KI-VO «auf begründete Anfrage einer zuständigen nationalen Behörde nachweisen» können, dass sie die Anforderungen nach Abschnitt 2 KI-VO erfüllen. Die KI-VO schreibt an mehreren Orten vor, dass Pflichten, die bereits vor der Inverkehrbringung oder Inbetriebnahme von KI-Systemen erfüllt werden müssen, während deren Lebenszyklen an neue Begebenheiten angepasst werden müssen. So ist bspw. das Risikomanagementsystem nach Art. 9 Abs. 2 KI-VO regelmässig zu aktualisieren. Auch Art. 11 Abs. 1 Uabs. 1 KI-VO schreibt vor, dass die technische Dokumentation von Hochrisiko-KI-Systemen während des ganzen Lebenszyklus auf dem neusten Stand gehalten werden müssen. Da es sich bei diesen Pflichten jedoch um Vormarktpflichten handelt, die lediglich aufrechterhalten werden müssen, wird nicht weiter darauf eingegangen.

VII. Ergänzung: Nachmarktpflichten in der Schweiz für Smart Home Devices

386 Die obengenannten Nachmarktpflichten gelten für Software, wenn diese unabhängig von einem Niederspannungserzeugnis oder einer Funkanlage zu be-

1615 Art. 11 Abs. 1 Uabs. 1 KI-VO.

1616 Art. 18 Abs. 1 lit. a i.V.m. Art. 72 Abs. 3 KI-VO.

1617 S. o., Rn. 332.

1618 Dies gilt gem. Art. 19 Abs. 1 KI-VO nur, wenn weder im Unionsrecht noch im nationalen Recht etwas anderes vorgesehen ist.

urteilen ist. Ergänzend sollen hier deshalb kurz die in der Schweiz für Smart Home Devices geltenden Nachmarktpflichten dargelegt werden.

Die Verordnung enthält in Art. 24 NEV Pflichten zur «Marktbeobachtung durch die Wirtschaftsakteurinnen». Die Hersteller (als Wirtschaftsakteure) müssen gem. Art. 24 Abs. 1 NEV «die von ihnen in Verkehr gebrachten oder auf dem Markt bereitgestellten Erzeugnisse» beobachten, wenn dies «angesichts der von diesen Erzeugnissen ausgehenden Risiken für die Gesundheit und Sicherheit notwendig erscheint». Zudem müssen sie gem. Art. 24 Abs. 2 NEV dazu Stichproben nehmen und begründete Hinweise verfolgen, die darauf hindeuten, dass ihr Erzeugnis nicht den Vorschriften entspricht. Dies muss dokumentiert werden. Abs. 3 hält fest, dass sie «die notwendigen Massnahmen [treffen] und [...], soweit aufgrund der Risiken notwendig, unverzüglich die Kontrollstelle über die festgestellten Mängel und die getroffenen Massnahmen [informieren müssen]». Welche Massnahmen notwendig sind, ist nicht geregelt. Weiter müssen Hersteller nach der Inverkehrbringung eines Niederspannungserzeugnisses gem. Art. 8 Abs. 5 NEV ihre Konformitätserklärungen aktuell halten und diese gem. Art. 9 NEV für zehn Jahre aufbewahren. Auch die technischen Unterlagen müssen gem. Art. 12 Abs. 4 NEV für zehn Jahre aufbewahrt werden. Im Gegensatz zum PrSG haben Hersteller von Niederspannungserzeugnissen aufgrund der zusätzlich geschützten Rechtsgüter bspw. auch eine Beobachtungs- und Gefahrenabwendungspflicht bezüglich Gefahren für die Sicherheit von Haustieren und Sachen gem. Art. 3 NEV. 387

Der 4. Abschnitt der FAV regelt die Pflichten der Wirtschaftsakteurinnen. Art. 23 FAV trägt den Titel «Verfolgungspflichten» und enthält Nachmarktpflichten. Nach der Inverkehrbringung verpflichtet Art. 23 Abs. 1 FAV Hersteller, wenn dies aufgrund «der von einer Funkanlage ausgehenden Gefahren gerechtfertigt erscheint», zur Entnahme und Prüfung von Stichproben «zum Schutz der Gesundheit und der Sicherheit der Endnutzerinnen». Weiter müssen sie, «wenn nötig [...] ein Beschwerdeverzeichnis der nichtkonformen Funkanlagen und deren Rückrufe» führen und «die Händlerinnen über diese Verfolgung auf dem Laufenden» halten.[1619] Art. 23 Abs. 2 FAV verpflichtet Hersteller, «die der Auffassung sind oder Grund zu der Annahme haben, dass eine von ihnen in Verkehr gebrachte Funkanlage nicht dieser Verordnung entspricht», sofort erforderliche Korrekturmassnahmen zu ergreifen, damit die Konformität hergestellt wird. Alternativ müssen sie ihre Funkanlagen «zurücknehmen oder zurückrufen».[1620] Art. 23 Abs. 4 FAV enthält eine Meldepflicht für 388

1619 Art. 23 Abs. 1 FAV.
1620 Art. 23 Abs. 2 FAV.

Hersteller ans BAKOM, wenn «mit der Funkanlage Risiken verbunden» sind. Hersteller von Funkanlagen müssen gem. Art. 21 Abs. 2 FAV Informationen zur Rückverfolgung zehn Jahre lang nach dem Bezug von sowie nach der Abgabe an einen anderen Wirtschaftsakteur aufbewahren. Art. 7 Abs. 1 lit. a FAV erfasst nicht nur den Schutz der Gesundheit und Sicherheit von Menschen, sondern auch von Haus- und Nutztieren. Zudem wird der Schutz von Gütern erfasst.

389 Im Gegensatz zum PrSG müssen Hersteller bei Smart Home Devices also Gefahrenabwendungsmassnahmen treffen. Die blosse Bereitschaft dazu reicht nicht aus. Des Weiteren sind nicht nur die Gesundheit und Sicherheit von Menschen, sondern auch Haus- respektive Nutztiere sowie Sachen geschützt.

VIII. Fazit

390 Nachmarktpflichten sind Pflichten, die von den Wirtschaftsakteuren selbstständig und ohne Aufforderung einer Behörde nach der Inverkehrbringung oder der Inbetriebnahme im eigenen Unternehmen zu erfüllen sind. Die produktsicherheitsrechtlichen Nachmarktpflichten setzen sich aus Gefahrenerkennungsmassnahmen bzw. der Beobachtung nach der Inverkehrbringung, Gefahrenabwendungsmassnahmen, Melde- sowie Aufbewahrungs- und Aktualisierungspflichten für Produkte, die nicht missbräuchlich verwendet wurden, zusammen. Diese Massnahmen und Pflichten müssen immer in einem angemessenen Rahmen ergriffen und erfüllt werden, der abhängig vom Risiko ist.

391 Zur rechtzeitigen Gefahrenerkennung müssen Hersteller ihre Produkte nach dem Inverkehrbringen aktiv und passiv beobachten, um Risiken zu erfassen, die erst danach auftreten. Bereits vor der Inverkehrbringung erkennbare Gefahren sind hingegen schon vorher zu beseitigen. Nach schweizerischem Recht besteht gem. Art. 8 Abs. 2 lit. a PrSG eine Pflicht für Hersteller zur aktiven Produktbeobachtung, wobei ihnen die konkrete Umsetzung überlassen bleibt. Im EU-Recht gilt eine solche Pflicht nicht generell, sondern nur spezifisch für Anbieter von Hochrisiko-KI-Systemen nach der KI-VO. Diese verlangt gem. Art. 72 Abs. 2 und Art. 9 Abs. 2 KI-VO eine proaktive, zielgerichtete Erhebung und Auswertung von Leistungsdaten sowie eine kontinuierliche Risikobewertung nach dem Inverkehrbringen. In der Schweiz besteht zwar keine Pflicht zur aktiven integrierten Produktbeobachtung, doch ist deren Umsetzung sehr zu empfehlen, da automatische Rückmeldungen die Fehleridentifikation und schnelle Reaktion erleichtern. Durch die automatische Übermittlung von Systemmeldungen mit Versionsnummer wird insbesondere die Bearbeitung von Beschwerden vereinfacht. Allerdings können faktisch nur

Hersteller, die aktiv an der Softwareentwicklung beteiligt sind, eine solche integrierte Beobachtung eigenständig umsetzen. Deshalb sollten Dritte, die Software für Smart Home Devices entwickeln, dem (Quasi-)Hersteller entsprechende Beobachtungssysteme bereitstellen. Für Hochrisiko-KI-Systeme ist eine automatische Ereignisaufzeichnung ohnehin gem. Art. 12 Abs. 1 KI-VO vorgeschrieben. Hersteller sind laut allgemeinem Produktsicherheitsrecht in der Schweiz (Art. 8 Abs. 3 PrSG) und der EU (Art. 9 Abs. 12 GPSR) verpflichtet, sicherheitsrelevante Beschwerden entgegenzunehmen und zu untersuchen (passive Produktbeobachtung). Zwar ist die Dokumentation von Beschwerden nach dem PrSG nicht explizit vorgeschrieben, faktisch jedoch für ein effektives Beschwerdemanagement notwendig. Für Hochrisiko-KI-Systeme in der EU besteht explizit eine Pflicht zur Untersuchung und Dokumentation (Art. 20 Abs. 2 und Art. 72 Abs. 2 KI-VO). In der Schweiz werden Stichproben als obligatorisch angesehen, in der EU nicht. Konkrete Massnahmen zur Gefahrenerkennung und Beschwerdekanäle stehen sowohl in der Schweiz als auch in der EU weitgehend im Ermessen des Herstellers. Da die GPSR im Gegensatz zum PrSG weder eine aktive Produktbeobachtungspflicht noch Stichproben bei der passiven Produktbeobachtung verlangt, müssen Hersteller in der Schweiz strengere Gefahrenerkennungsmassnahmen durchführen als in der EU. Um das ursprüngliche Ziel einer Angleichung an das EU-Schutzniveau zu erreichen, sollten diese zusätzlichen Schweizer Pflichten gestrichen werden und es könnte stattdessen spezifisch für besonders risikoreiche Softwareprodukte (analog zur KI-VO für Hochrisiko-KI-Systeme) eine aktive integrierte Produktbeobachtungspflicht eingeführt werden.

Die Möglichkeit zur Fernaktualisierung softwaregestützter Smart Home Devices eröffnet neue Wege zur Gefahrenabwehr. Schweizer Hersteller müssen nach Art. 8 Abs. 2 lit. b PrSG nur zur Gefahrenabwehr bereit sein, während in der EU (Art. 9 Abs. 8 GPSR) und für Hochrisiko-KI-Systeme (Art. 20 Abs. 1 KI-VO, Art. 9 Abs. 2 lit. d KI-VO) explizit Korrektur- und Risikomanagementmassnahmen vorgeschrieben sind. Zudem besteht in der EU eine Informationspflicht gegenüber betroffenen Verbrauchern (Art. 9 Abs. 8 lit. b, Art. 9 Abs. 10 GPSR; Art. 20 Abs. 1 KI-VO). Um diesen Pflichten nachzukommen, müssen Hersteller eine technische Verbindung zur ausgelieferten Software vorsehen. Obwohl in der Schweiz keine Pflicht zur Gefahrenabwendung besteht, nennt Art. 8 Abs. 5 lit. d PrSG beispielhafte Massnahmen, ähnlich wie die GPSR und KI-VO. Wichtigste Massnahmen sind Sicherheitswarnungen, Rückrufe, Deaktivierungen, Rücknahmen aus der Lieferkette, Vertriebsstopps und Sicherheitswiederherstellung durch Updates. Die GPSR verpflichtet Hersteller zudem explizit zu Sicherheitswarnungen und Rückrufanzeigen (Art. 35 und 36

392

GPSR) sowie Abhilfemassnahmen (Art. 37 GPSR). Solche detaillierten Vorgaben und eine Übernahme von Abhilfemassnahmen führen zu erheblichen finanziellen Belastungen für Hersteller. Es ist deshalb nicht empfohlen, diese ins Schweizer Recht zu übernehmen. Sinnvoller ist es, auf die Wiederherstellung der Sicherheit durch Fernverbindungen zu setzen. Hersteller können Gefahren direkt korrigieren und dadurch vermeiden, dass gefährliche Produkte trotz Warnungen auf dem Markt verbleiben. Bei Softwareprodukten genügt oft schon ein einfaches Sicherheitsupdate, wodurch umfangreichere Massnahmen entfallen.

393 Das PrSG, die GPSR und die KI-VO sehen alle Meldepflichten an Behörden bei gefährlichen Produkten vor (Art. 8 Abs. 5 PrSG, Art. 9 Abs. 8 lit. c GPSR, Art. 20 Abs. 2 und Art. 73 Abs. 1 KI-VO). Die GPSR verlangt zusätzlich Unfallmeldungen auch ohne festgestellte Produktgefahr (Art. 20 Abs. 1 GPSR). Während gem. PrSG und GPSR keine weiteren Pflichten nach der Meldung bestehen, schreibt die KI-VO eine unverzügliche Untersuchung sowie behördliche Information vor Systemänderungen vor (Art. 73 Abs. 6 KI-VO). Meldefristen gibt es explizit nur in der KI-VO, grundsätzlich gilt jedoch überall: Je höher die Gefahr, desto schneller ist zu melden.

394 Hersteller müssen gem. Art. 8 Abs. 2 lit. c PrSG die Rückverfolgbarkeit ihrer Produkte vor dem Inverkehrbringen sicherstellen (Vormarktpflicht) und die entsprechenden Informationen danach aufbewahren (Nachmarktpflicht). Technische Unterlagen und Konformitätserklärungen müssen gem. Art. 10 Abs. 1 PrSV mindestens zehn Jahre ab Herstellung (bei Serienprodukten ab letztem Exemplar) verfügbar sein. Nach der GPSR besteht eine ähnliche zehnjährige Aufbewahrungspflicht technischer Unterlagen sowie eine sechsjährige Aufbewahrungspflicht von Rückverfolgbarkeitsinformationen, u.a. zu Softwarelieferanten (Art. 9 Abs. 3 GPSR). Die KI-VO verlangt ebenfalls eine zehnjährige Aufbewahrung spezifischer technischer Dokumentationen, Qualitätsmanagement- und Konformitätsunterlagen (Art. 18 Abs. 1 KI-VO) sowie mindestens sechs Monate für automatische Protokolle (Art. 19 Abs. 1 KI-VO).

F. Ende der Nachmarktpflichten für Hersteller von Software- und KI-Produkten

Die meisten Nachmarktpflichten im allgemeinen Produktsicherheitsrecht sind von der Gebrauchsdauer eines Produktes abhängig. Wie die Gebrauchsdauer zu bestimmen ist, soll in den nachfolgenden Kapiteln aufgezeigt werden. Während die Dauer der Aufbewahrungspflichten in Jahren geregelt ist, sind die Abhilfemassnahmen nach Art. 37 GPSR nicht zeitlich beschränkt.[1621] Die Beobachtungspflicht für Anbieter von Hochrisiko-KI-Systemen nach Art. 72 KI-VO sowie die darin verankerte Verpflichtung zur Aufrechterhaltung eines Systems zur Beobachtung nach der Inverkehrbringung sind während der gesamten Lebensdauer eines Produktes zu beachten.[1622] Die KI-VO hält weiter fest, dass das Risikomanagement[1623] und die automatische Protokollierung[1624] des Hochrisiko-KI-Systems während seines ganzen Lebenszyklus aufrechterhalten werden müssen. Die erwartete Lebensdauer muss in der Betriebsanleitung des Hochrisiko-KI-Systems angegeben werden.[1625] Braun Binder/Egli definieren den Lebenszyklus als den Zeitraum von der «Konzeption bis zur Stilllegung».[1626] Nach einer Stilllegung darf ein KI-System nicht mehr weiterverwendet werden.[1627] Die Stilllegung erfolgt durch den Beschluss des Anbieters.[1628] 395

I. Ende der Gebrauchsdauer

Mit Ablauf der angegebenen oder vernünftigerweise vorhersehbaren Gebrauchsdauer laufen auch die Nachmarktpflichten nach Art. 8 PrSG für Hersteller aus.[1629] Dabei wird primär auf die Angabe des Inverkehrbringers abgestellt. 396

1621 S. o., Rn. 368.

1622 Art. 72 Abs. 2 KI-VO; Beck KI-VO-Hartmann, Art. 72 N 1, 10.

1623 Art. 9 Abs. 2 KI-VO.

1624 Art. 12 Abs. 1 KI-VO.

1625 Art. 13 Abs. 3 lit. e KI-VO, siehe auch ErwG 71 KI-VO.

1626 Mit Hinweis auf das Gesetzgebungsverfahren Beck KI-VO-Braun Binder/Egli, Art. 9 N 18 f.

1627 Beck KI-VO-Braun Binder/Egli, Art. 9 N 18.

1628 Beck KI-VO-Braun Binder/Egli, Art. 9 N 18.

1629 Zum Ablauf der Produktbeobachtungspflichten, Botschaft PrSG, S. 7442. Auch wenn nur in Art. 8 Abs. 2 PrSG auf die Gebrauchsdauer verwiesen wird, hängt die Dauer aller Nachmarktpflichten von der Gebrauchsdauer ab. S. o., Rn. 292.

Macht dieser keine Angabe, zählt die voraussichtliche Gebrauchsdauer.[1630] Die voraussichtliche Gebrauchsdauer muss sich am durchschnittlichen Gebrauch eines Produktes orientieren.[1631] In der Folgenabschätzung zum Entwurf der GPSR wurde die traditionelle Bedeutung des Begriffs des Inverkehrbringens der Produktsicherheitsrichtlinie in Frage gestellt, da sich Produkte mit Software im Laufe der Zeit verändern können.[1632] Aus diesem Grund wurde gefordert, dass in der neuen GPSR festgelegt werden sollte, dass Produkte während ihrer gesamten erwarteten Lebensdauer sicher sein müssen.[1633] Art. 5 GPSR legt fest, dass nur sichere Produkte in Verkehr gebracht oder bereitgestellt werden dürfen. In Art. 3 Ziff. 2 GPSR wird klargestellt, dass ein «sicheres Produkt» während seiner tatsächlichen Gebrauchsdauer sicher ist. Das heisst, dass auch nach der GPSR Produkte während ihrer gesamten Lebensdauer sicher sein müssen.[1634] Somit enden die Nachmarktpflichten auch nach der GPSR für ein Produkt mit dessen Gebrauchsdauer. Gemeint ist nach der GPSR nicht die vom Hersteller angegebene Lebensdauer, sondern eine «übliche bzw. voraussichtliche Gebrauchsdauer», welche länger sein kann als die vom Hersteller angegebene.[1635]

397 Für den Hersteller von Smart Home Devices mit integrierter Software und Software an sich wird es regelmässig schwierig sein, genau festzulegen, wie lange sein Produkt gefahrlos verwendet werden kann.[1636] Haushaltsgeräte haben eigentlich eine sehr lange Lebensdauer, wenn sie nicht einer geplanten Obsoleszenz zum Opfer fallen. Dies kann es für den Hersteller aufgrund der schnellen technologischen Entwicklung irgendwann schwierig machen, Software für alte Hardware kompatibel zu gestalten.[1637] Die Gebrauchsdauer hängt u.a. von der Stärke und Schnelligkeit der Veränderung des Produktes ab: Verändert sich ein Produkt über die Jahre nur minim (bspw. durch leichten Verschleiss), wird die Gebrauchsdauer länger ausfallen als bei einem Produkt, welches sich in kurzer Zeit sehr stark verändert.[1638] Ebenso relevant sind «der

1630 Botschaft PrSG, S. 7437, 7442; siehe auch: Fellmann, Jusletter 25.10.2010, Rn. 59; SHK PrSG-Hess, Art. 8 N 16.

1631 Botschaft PrSG, S. 7442; siehe auch mit ausführlicher Diskussion Gerster, Rn. 211 ff., m.w.H.

1632 S. o., Rn. 293.

1633 Europäische Kommission, Impact Assessment GPSR, S. 14.

1634 Siehe auch explizit ErwG 23 GPSR; NHK GPSR-Wiebe, Art. 5 N 26. Zum sicheren Produkt s. o., Rn. 261.

1635 NHK GPSR-Wiebe, Art. 5 N 26.

1636 Mit Bezug auf Elektrogeräte Botschaft PrSG, S. 7437; siehe auch SHK PrSG-Hess, Art. 8 N 35.

1637 Siehe auch in Bezug auf Fahrzeuge May/Gaden, S. 116.

1638 Siehe auch Botschaft PrSG, S. 7437, wo auf die Häufigkeit der Benutzung und die dort angewandte Sorgfalt, Wartung und Aufbewahrung abgestellt wird. Dies hat wiederum Aus-

wissenschaftliche und technische Fortschritt».[1639] Neue Entwicklungen können die Gebrauchsdauer verkürzen, da mit laufender Entwicklung Risiken, die heute akzeptiert sind, später nicht mehr toleriert[1640] werden.[1641] In diesem Zusammenhang sei jedoch auf Art. 3 Abs. 5 PrSG («Ein Produkt ist nicht allein deshalb als gefährlich zu betrachten, weil ein sichereres Produkt in Verkehr gebracht wurde») und Art. 6 Abs. 2 GPSR («Die Möglichkeit, ein höheres Sicherheitsniveau zu erreichen, oder die Verfügbarkeit anderer Produkte, von denen ein geringeres Risiko ausgeht, ist kein Grund, ein Produkt als gefährliches Produkt anzusehen») hingewiesen.

Die Gebrauchsdauer muss – wenn möglich – direkt auf dem Produkt angegeben werden.[1642] Bei Software könnte dies bspw. in den Einstellungen erfolgen. Insbesondere bei mit Trainingsdaten trainierten KI-Systemen kann ein Hinweis nützlich sein, dass sich das Training jeweils auf einen limitierten Zeitraum bezieht und das KI-System deshalb bspw. nach zwei Jahren nicht mehr aktuell ist und für gewisse Anwendungen nicht mehr benutzt werden sollte.[1643] Auch die Angabe, ob das System mit neuen Daten aktualisiert wird, und dann wiederum «länger» gültig sein kann, wäre nützlich. Werden die Karten eines Navigationsgerätes bspw. nach einiger Zeit nicht mehr aktualisiert, sollte dies angegeben werden, da der Inhalt irgendwann zu weit von der Realität abweicht. 398

II. Unrealistisch kurz angegebene Gebrauchsdauer

Unklar ist, was geschieht, wenn der Hersteller eine sehr kurze Lebensdauer für sein Produkt angibt[1644] und so seine Nachmarktpflichten faktisch stark einschränkt. Gerster geht – auf die Botschaft gestützt – davon aus, dass «die verpflichteten Personen […] die Dauer der Nachmarktpflichten aktiv gestalten»[1645] 399

wirkung darauf, wie stark und schnell ein Produkt sich verändert; ähnlich SHK PrSG-Hess, Art. 3 N 35 mit einer Aufzählung von Veränderungen in Fn. 70 nach Beck ProdSG-Kapoor, § 6 N 11.

1639 Botschaft PrSG, S. 7437.

1640 S. o., Rn. 310.

1641 Botschaft PrSG, S. 7437; siehe auch SHK PrSG-Hess, Art. 3 N 36.

1642 Botschaft PrSG, S. 7442; Wichtig ist, dass dem Anwender klar ist, wie lange er ein Produkt gefahrlos nutzen kann. Siehe dazu SHK PrSG-Hess, Art. 3 N 34 m.w.H.

1643 Trainingsdaten zeigen eine Momentaufnahme des Zeitpunkts ihrer Erhebung. Sie können daher einem historischen Bias unterliegen. S. o., Rn. 264.

1644 Zitieren diesbezüglich diskussionslos die Botschaft PrSG, S. 7437 respektive 7442: Bühler, Bestandteil, S. 50, 84 ff., 146; Bühler/Tobler, S. 387 f., 395 f.; SHK PrSG-Hess, Art. 3 N 36, Art. 8 N 14, 16; Fellmann, Jusletter 25.10.2010, Rn. 59, 61; ebenfalls nicht auf diesen Punkt eingehend: Haftpflichtkommentar-Holliger-Hagmann, Art. 3 PrSG N 12 f.

1645 Gerster, Rn. 276.

und so ihre «verwaltungsrechtlichen Risiken [...] minimieren»[1646] können. Er weist jedoch darauf hin, dass ein Produkt bei einer zu kurz angegebenen Dauer als qualitativ minderwertig erscheine, was «dem Kunden nur schwer zu erklären» sei.[1647] Bei einem offensichtlich unrealistisch gewählten Enddatum muss es nach vorliegend vertretener Meinung möglich sein, auf den durchschnittlichen Gebrauch des Produktes abzustellen.[1648] Ansonsten könnten die Nachmarktpflichten durch eine unrealistisch kurze Angabe ausgehebelt werden. Da die Nachmarktpflichten der Sicherheit von Personen dienen, dürfen sie nicht einfach mittels (zu) kurz angegebener Gebrauchsdauer «wegbedungen» werden können. Auch wenn eine zehnjährige haftungsrechtliche Verantwortung für Produktfehler gem. Art. 10 Abs. 1 PrHG gilt,[1649] genügt dies nicht, da durch das öffentliche Produktsicherheitsrecht andere Ziele verfolgt werden.[1650] Das «fehlerhafte» Produkt ist auch nicht dasselbe wie das «unsichere» bzw. «gefährliche» Produkt.[1651] Ein Produkt kann bspw. unsicher sein, ohne dass es fehlerhaft ist. Weder die angegebene noch die geschätzte Gebrauchsdauer des Produktes beeinflussen die Dauer der zivilrechtlichen Haftung.[1652]

III. Mindestdauer

400 Weder das schweizerische noch das europäische[1653] allgemeine Produktsicherheitsrecht kennen eine Mindestgebrauchsdauer. Das europäische Ökodesignrecht könnte jedoch ein «Orientierungspunkt» zur Ermittlung der Gebrauchsdauer sein.[1654] Ein Anhaltspunkt zur Mindestdauer, während derer der Hersteller Nachmarktpflichten erfüllen muss, ist der Zeitraum, in welchem der Hersteller das Produkt anbietet. Gestattet der Hersteller nur den Gebrauch eines Produktes und entlässt er es nicht vollständig aus seinem Herrschaftsbereich, ist er während der ganzen Dauer für die Sicherheit des Produktes ver-

1646 Gerster, Rn. 215.
1647 Gerster, Rn. 215 Fn. 346.
1648 Ebenso Fornage, in: Chappuis/Winiger/Campi S. 217.
1649 Die Haftung verwirkt zehn Jahre nach dem Tag der Inverkehrbringung Wildhaber/Rey, Rn. 1487; siehe auch Fellmann, Jusletter 25.10.2010, Rn. 60, mit einem konkretem Vergleich von PrHG und PrSG.
1650 S. o., Rn. 148.
1651 Bühler/Tobler, S. 126.
1652 Botschaft PrSG, S. 7442; Wildhaber/Rey, Rn. 1495; Haftpflichtkommentar-Holliger-Hagmann, Art. 3 PrSG N 12; Fellmann, Jusletter 25.10.2010, Rn. 61.
1653 NHK GPSR-Wiebe, Art. 5 N 27.
1654 NHK GPSR-Wiebe, Art. 5 N 27, m.w.H.

antwortlich, während derer das Produkt in Verkehr ist.[1655] Demzufolge ist die Gebrauchsdauer bei Produkten, die sich mindestens teilweise noch im Herrschaftsbereich des Herstellers befinden, mindestens so lange, wie er das Produkt zur Verfügung stellt. Dies muss nach vorliegend vertretener Ansicht auch dann gelten, wenn der Hersteller eine kürzere Gebrauchsdauer angegeben hat.[1656] Ein Beispiel ist Software, die ein Hersteller online zum Download anbietet.

IV. Ende der Geschäftstätigkeit des Herstellers

Weiter enden die in Art. 8 PrSG vorgeschriebenen Pflichten mit dem Ende der Geschäftstätigkeit, also des beruflichen Handelns des Herstellers,[1657] z.B. infolge dessen Konkurses.[1658] Die GPSR sowie die Kommentierung dazu äussern sich diesbezüglich nicht. Dies führt aber nicht zwingend dazu, dass gefährliche Produkte auf dem Markt bleiben, da auch Händler und Importeure gewisse Nachmarktpflichten haben.[1659] Die KI-VO schreibt in Art. 18 Abs. 2 für Hochrisiko-KI-Systeme vor, dass die EU-Mitgliedstaaten Bedingungen zur Bereithaltung von Unterlagen festlegen müssen, sollte der Anbieter vor Ablauf von zehn Jahren Konkurs gehen oder seine Tätigkeiten aufgeben.[1660] 401

V. Fazit

Je nach Nachmarktpflicht gestaltet sich deren zeitliche Aufrechterhaltung unterschiedlich. Die Aufbewahrung ist fast immer für zehn Jahre zu beachten. Einzig die Logs aus der obligatorischen Protokollierung bei einem Hochrisiko-KI-System müssen für mindestens sechs Monate aufbewahrt werden. Die übrigen Nachmarktpflichten für Anbieter von Hochrisiko-KI-Systemen müssen während der ganzen Lebensdauer bis zur Stilllegung z.B. durch Deaktivierung umgesetzt werden. In der Schweiz und der EU enden die Nachmarktpflichten aus dem allgemeinen Produktsicherheitsrecht entweder mit dem Ende der Geschäftstätigkeit des Herstellers oder mit dem Ende der Gebrauchsdauer des Produktes. Ausgenommen davon sind die obengenannten Aufbewahrungs- 402

1655 Haftpflichtkommentar-Holliger-Hagmann, Art. 2 PrSG N 19 f. mit der Äusserung, dass die SECO-Einschränkungen diesbezüglich unzutreffend seien. S. o., Rn. 297 f.

1656 Siehe soeben, Rn. 399.

1657 S. o., Rn. 272.

1658 SHK PrSG-Hess, Art. 8 N 12.

1659 Art. 8 Abs. 2, 4 und 5 PrSG; Art. 11 und 12 GPSR.

1660 S. o., Rn. 385.

und Aktualisierungspflichten, bei welchen die Dauer fest in Jahren angegeben ist, und die Abhilfemassnahmen nach Art. 37 GPSR, welche gar keiner zeitlichen Limitierung unterliegen. Während nach dem PrSG primär auf die vom Hersteller angegebene Gebrauchsdauer (ausser diese ist völlig unrealistisch) abgestellt wird, endet diese in der EU mit der voraussichtlichen Gebrauchsdauer. Ausserdem enden die Nachmarktpflichten in der Schweiz und der EU für ein Produkt nicht, solange sich dieses noch mindestens teilweise im Herrschaftsbereich des Herstellers befindet und von diesem bspw. laufend aktualisiert wird.

Teil 4:
Zusammenfassung und Fazit

Das letzte Kapitel dieser Arbeit enthält eine Zusammenfassung inklusive Übersichtstabelle. Ausserdem werden die wichtigsten Unterschiede der produktsicherheitsrechtlichen Nachmarktpflichten für Hersteller von Software- und KI-Produkten in der Schweiz und der EU dargelegt und Vorschläge für die Schweiz zu Anpassungen im PrSG und zu einer möglichen KI-Regulierung ausformuliert. 403

A. Zusammenfassung

404 Das schweizerische und europäische Produktsicherheitsrecht hat zwei Hauptaufgaben: Erstens soll die Sicherheit und Gesundheit[1661] von Menschen geschützt werden, indem die Gefahren, die von Produkten ausgehen, abgewendet werden, und zweitens sollen Handelshemmnisse zwischen der EU und der Schweiz bzw. innerhalb der EU beseitigt werden. Wo einheitliche Regelungen sinnvoll sind, wird die Produktsicherheit horizontal geregelt. In der Schweiz findet dies im PrSG und in der EU in der GPSR statt. Beide Erlasse sind Auffanggesetze und lediglich subsidiär anwendbar mit einigen Ausnahmen.[1662]

405 Software und KI – als eine Form von Software – werden sowohl in der Schweiz als auch in der EU als Produkte vom allgemeinen Produktsicherheitsrecht erfasst.[1663] Das PrSG und die GPSR und die dort geregelten Nachmarktpflichten finden nur auf Software Anwendung, solange diese nicht unter spezielles Sektorrecht fällt. Dies ist aber nur ausnahmsweise der Fall. Da die EU KI-Systeme in der KI-VO regelt, hat diese als lex specialis vor der GPSR Vorrang. Die KI-VO beinhaltet jedoch nur Nachmarktpflichten für Hochrisiko-KI-Systeme. Deshalb gelten die Nachmarktpflichten der GPSR für alle anderen KI-Systeme und für herkömmliche Software.[1664] In der EU gelten ab dem 02. August 2026 für Hochrisiko-KI-Systeme nach Anhang III KI-VO und ab dem 02. August 2027 für Hochrisiko-KI-Systeme nach Art. 6 Abs. 1 KI-VO spezifische Nachmarktpflichten.[1665] Bis dann gelten die Nachmarktpflichten der GPSR für alle KI-Systeme. Ab dem 02. August 2026 bzw. 02. August 2027 gelten die Nachmarktpflichten der GPSR nur noch subsidiär für Nicht-Hochrisiko-KI-Systeme. In der Schweiz bestehen keine spezifischen Nachmarktpflichten für KI-Systeme; es gelten die allgemeinen Nachmarktpflichten gem. Art. 8 PrSG.[1666] Die Nachmarktpflichten des PrSG und der GPSR beziehen sich ausschliesslich auf Konsumentenprodukte. Im Gegensatz dazu müssen Hersteller von Hochrisiko-KI-Systemen in der EU auch im B2B-Bereich Nachmarktpflichten wahrnehmen.

406 In der Schweiz und der EU werden Herstellern nach dem allgemeinen Produktsicherheitsrecht ab der Inverkehrbringung von Software Nachmarkt-

1661 Geschützt sind die physische und psychische Gesundheit s. o., Rn. 268.
1662 S. o., Rn. 182.
1663 S. o., Rn. 239.
1664 S. o., Rn. 183.
1665 S. o., Rn. 160, 228.
1666 S. o., Rn. 391 ff.

pflichten auferlegt.[1667] Nach der GPSR gilt der gewerbliche Eigengebrauch des Herstellers nicht als Inverkehrbringen und begründet daher noch keine Nachmarktpflichten für Software. Nach dem PrSG gilt der gewerbliche Eigengebrauch als Inverkehrbringen und nach der KI-VO als Inbetriebnahme, sodass er in der Schweiz für Software und nach der KI-VO für Hochrisiko-KI-Systeme Nachmarktpflichten auslöst.[1668] Nachmarktpflichten aus dem allgemeinen Produktsicherheitsrecht gelten in der Schweiz und der EU bis zum Ende der Geschäftstätigkeit des Herstellers oder bis zum Ende der Gebrauchsdauer des Produktes. Gemäss dem PrSG richtet sich das Ende der Nachmarktpflichten primär nach der vom Hersteller angegebenen Gebrauchsdauer (sofern diese nicht offensichtlich unrealistisch ist), während sie in der EU mit Ablauf der voraussichtlichen Gebrauchsdauer endet. Ausgenommen sind die Aufbewahrungs- und Aktualisierungspflichten mit festen Jahresfristen sowie die Abhilfemassnahmen der GPSR, die keiner zeitlichen Begrenzung unterliegen. Solange sich das Produkt ferner ganz oder teilweise im Herrschaftsbereich des Herstellers befindet, etwa weil er es laufend aktualisiert, bestehen die Nachmarktpflichten fort.[1669]

Die produktsicherheitsrechtlichen Nachmarktpflichten umfassen Gefahrenerkennungsmassnahmen bzw. die Beobachtung nach der Inverkehrbringung, Gefahrenabwendungsmassnahmen, Melde- sowie Aufbewahrungs- und Aktualisierungspflichten.[1670] Die nachfolgende Tabelle 5 fasst die Rechtslage für die produktsicherheitsrechtlichen Nachmarktpflichten von Herstellern von Software und KI in der Schweiz und der EU zusammen. Eine ausformulierte Darstellung findet sich oben in den Fazits zu den entsprechenden Nachmarktpflichten. 407

1667 S. o., Rn. 303.
1668 S. o., Rn. 304.
1669 S. o., Rn. 402.
1670 S. o., Rn. 319.

Tabelle 5: Nachmarktpflichten für Software und KI

Geografischer Geltungsbereich			**Schweiz**	**EU**	**KI-VO**
Erlass			**PrSG**	**GPSR**	**KI-VO**
Anwendbarkeit der Nachmarktpflichten			**nur Konsumentenprodukte**		**alle Hochrisiko-KI-Systeme**
Geltung seit/ab			**01.07.2010**	**13.12.2024**	**Für Hochrisiko-KI-Systeme nach Anhang III KI-VO: 02.08.2026 Art. 6 Abs. 1 KI-VO: 02.08.2027**
Nachmarktpflichten / Pflichten nach dem Inverkehrbringen	**Beobachtung nach Inverkehrbringen**	**Aktiv**	Ja, Art. 8 Abs. 2 lit. a PrSG	Nein	Ja, Art. 72 Abs. 2 und Art. 9 Abs. 2 KI-VO
		Passiv	Ja, Art. 8 Abs. 3 PrSG	Ja, Art. 9 Abs. 12 GPSR	Ja, Art. 20 Abs. 2 und Art. 72 Abs. 2 KI-VO
	Gefahrenabwendungsmassnahmen		Nein, Art. 8 Abs. 2 lit. b PrSG, nur Erstellung der Bereitschaft zur Gefahrenabwehr bereits vor Inverkehrbringen	Ja, Korrektur- und Risikomanagementmassnahmen: Art. 9 Abs. 8 GPSR Informationspflichten: Art. 9 Abs. 8 lit. b und Art. 9 Abs. 10 GPSR Sicherheitswarnungen und Rückrufanzeigen: Art. 35 und 36 GPSR Abhilfemassnahmen: Art. 37 GPSR	Ja, Korrektur- und Risikomanagementmassnahmen: Art. 20 Abs. 1 und Art. 9 Abs. 2 lit. d KI-VO Informationspflicht: Art. 20 Abs. 1 KI-VO

Geografischer Geltungsbereich		**Schweiz**	**EU**	**KI-VO**
Erlass		**PrSG**	**GPSR**	**KI-VO**
Anwendbarkeit der Nachmarktpflichten		**nur Konsumentenprodukte**		**alle Hochrisiko-KI-Systeme**
	Meldepflichten an Behörden	Ja, Art. 8 Abs. 5 PrSG	Ja, Art. 9 Abs. 8 lit. c GPSR Unfallmeldungen auch ohne festgestellte Produktgefahr: Art. 20 Abs. 1 GPSR	Ja, Art. 20 Abs. 2 und Art. 73 Abs. 1 KI-VO inkl. unverzüglicher Untersuchung sowie behördlicher Information vor Systemänderungen nach Art. 73 Abs. 6 KI-VO
	Aufbewahrungs- und Aktualisierungspflichten	Ja, Art. 8 Abs. 2 lit. c PrSG i.V.m. Art. 10 Abs. 1 PrSV	Ja, Art. 9 Abs. 3 GPSR	Ja, Art. 18 Abs. 1 und Art. 19 Abs. 1 KI-VO
Anwendbar auf folgende Produktarten	**Physische Produkte**	Ja	Ja	Nein
	Embedded-Software	Ja	Ja	Ja, aber nur wenn Hochrisiko-KI-System
	Stand-alone-Software	Ja (h.L.)	Ja (vorliegend vertreten)	Ja, aber nur wenn Hochrisiko-KI-System
	KI-System	Ja (vorliegend vertreten)	Ja (vorliegend vertreten)	Nein
	Hochrisiko-KI-System nach KI-VO	Keine Anwendung in der Schweiz	Nein, da lex generalis zu KI-VO	Ja
	Klassische Dienstleistungen	Nein	Nein	Nein

Nachmarktpflichten bestehen nur bei einer vernünftigerweise vorhersehbaren Verwendung des Produktes. Für eine missbräuchliche Verwendung trägt der 408

Hersteller keine Verantwortung.[1671] Innerhalb dieser Pflichten sind angemessene Massnahmen zu ergreifen, deren Umfang sich am Risiko orientiert: Je höher das Risiko, desto weitreichender die Massnahmen. Die Angemessenheit bestimmt sich nach der Grösse der Gefahr und dem erwarteten Erfolg der Massnahme. Nachteile für den Hersteller dürfen mitberücksichtigt werden. Eine Bagatellgrenze schliesst Pflichten bei nur geringfügigen Gefahren aus. Was als nicht mehr geringfügige und somit nicht mehr tolerierte Gefahr gilt, richtet sich nach dem gesellschaftlich akzeptierten Risikoniveau und ergibt sich aus einer einzelfallbezogenen Risikobewertung.[1672]

409 Die für Software- und KI-Produkte charakteristische Veränderlichkeit und Komplexität führen zu einer immer höheren Bedeutung von Nachmarktpflichten.[1673] Insbesondere die Produktbeobachtung wird durch die weiterhin bestehende Verbindung mit der Software umso relevanter, weil gefährliche Veränderungen oder bisher unerkannt gebliebene Gefahren nicht nur frühzeitig erkannt, sondern sogar behoben werden können.[1674] Mangels Körperlichkeit lösen Software und KI physische und psychische Gefahren nur über ein physisches Gerät aus. Sie sind nicht für sich selbst gefährlich, können aber gefährliche Situationen herbeiführen.[1675]

410 Auch wenn mit der Verbreitung von Smart Home Devices, Software und KI immer wieder auf Risiken[1676] hingewiesen wird, sollten die Vorteile, die damit verbunden sind, nicht vernachlässigt werden. Durch diese neuen Entwicklungen können Produkte sicherer konstruiert werden[1677] und Hersteller haben auch nach deren Inverkehrbringung die Möglichkeit, Gefahren zu beseitigen.[1678]

1671 S. o., Rn. 320.
1672 S. o., Rn. 321.
1673 S. o., Rn. 63.
1674 S. o., Rn. 362 ff.
1675 S. o., Rn. 33.
1676 S. o., Rn. 35 ff.
1677 S. o., Rn. 58.
1678 S. o., Rn. 59.

B. Unterschiede zwischen der Schweiz und der EU

Die wichtigsten Unterschiede bei den produktsicherheitsrechtlichen Nachmarktpflichten für Hersteller von Software- und KI-Produkten in der Schweiz und der EU sind die seit Inkrafttreten der GPSR unterschiedlichen Nachmarktpflichten im allgemeinen Produktsicherheitsrecht[1679] und die spezifische Regulierung von KI-Systemen in der EU[1680]. Wohl auch deshalb wird das PrSG derzeit teilrevidiert.[1681] 411

Im allgemeinen Produktsicherheitsrecht der Schweiz bestehen im Vergleich zum europäischen Recht höhere Anforderungen an die Produktbeobachtung. Im Gegensatz zur alten Produktsicherheitsrichtlinie verpflichtet die GPSR nicht mehr zu einer aktiven Produktbeobachtung. Demgegenüber wird die aktive Produktbeobachtung in der EU für Hochrisiko-KI-Systeme ausführlich geregelt.[1682] Im PrSG bestehen dafür wiederum weniger hohe Anforderungen an die Gefahrenabwendung, weil Korrekturmassnahmen in der GSPR und der KI-VO für den Hersteller bzw. Anbieter verpflichtend sind, sobald ein Produkt als gefährlich einzustufen ist. In der Schweiz muss jedoch nur die *Bereitschaft* zur Gefahrenabwendung sichergestellt werden.[1683] Zudem schreibt die GPSR genau vor, wie eine Sicherheitswarnung und die Rückrufanzeige ausgestaltet werden müssen. Solche Vorschriften gibt es im allgemeinen Produktsicherheitsrecht der Schweiz nicht.[1684] Obwohl Meldepflichten an Behörden vom PrSG, von der GPSR und von der KI-VO vorgeschrieben werden, sind diese unterschiedlich. Die GPSR verlangt Unfallmeldungen unabhängig davon, ob das Produkt tatsächlich gefährlich ist, und geht damit über das PrSG hinaus. Im Gegensatz zur KI-VO bestehen nach dem PrSG und der GPSR nach der Meldung keine weiteren Pflichten, sofern sie nicht von der Behörde angeordnet werden. Starre Meldefristen fehlen in PrSG und GPSR, existieren aber in der KI-VO.[1685] Insgesamt gelten in der EU für Software fast überall und für Hochrisiko-KI-Systeme überall strengere Nachmarktpflichten als in der 412

1679 S. o., Rn. 390 ff.
1680 S. o., Rn. 158.
1681 S. o., Rn. 4.
1682 S. o., Rn. 345 ff.
1683 S. o., Rn. 369.
1684 S. o., Rn. 370.
1685 S. o., Rn. 382.

Schweiz. Aus der obenstehenden Tabelle 5 können die unterschiedlichen Nachmarktpflichten im Detail ausgelesen werden.

413 Ein weiterer relevanter Unterschied zum PrSG betrifft die in der GPSR geregelten Abhilfemassnahmen.[1686] Obwohl die Ziele der GPSR primär darin bestehen, das Funktionieren des Europäischen Binnenmarktes zu verbessern und die Sicherheit und Gesundheit von Verbrauchern zu gewährleisten,[1687] werden damit auch ökonomische Interessen der Verbraucher geschützt. Eine weitere Differenz zeigt sich im weitergehenden Gesundheitsbegriff in der EU im Vergleich zum Verständnis in der Schweiz. Es könnte deshalb zur Anwendung unterschiedlicher Massstäbe kommen, wenn es um die Analyse von Beeinträchtigungen der Gesundheit geht.[1688] Hier zeigt sich, dass der Konsumentenschutz in der EU grundsätzlich höher ist als in der Schweiz.[1689]

1686 S. o., Rn. 366 ff.
1687 S. o., Rn. 157.
1688 S. o., Rn. 252, 268.
1689 S. o., Rn. 189.

C. Vorschläge für die Schweiz

Anpassungen des PrSG sind aus zwei Gesichtspunkten sinnvoll: Erstens sind generelle Anpassungen des PrSG nötig, z.B. in Bezug auf die Systematik des Gesetzes. Zweitens ist die Beseitigung von technischen Handelshemmnissen für die Schweiz aus wirtschaftlicher Sicht essenziell und eines der zwei wichtigsten Ziele des allgemeinen Produktsicherheitsrechts.[1690] Die wirtschaftliche Kompatibilität soll deshalb weiterhin sichergestellt werden, indem das Schweizer Produktsicherheitsrecht so weit wie nötig an jenes der EU angepasst und das MRA erweitert wird.[1691] Da es nicht sinnvoll ist, alle neuen europäischen Vorschriften zu übernehmen, wird nachfolgend aufgezeigt, wo der Fokus der Schweiz liegen sollte. 414

I. Generelle Anpassungen des PrSG

Im PrSG sind mehrere Anpassungen vorzunehmen. Es sollte klargestellt werden, dass sich die Gebrauchsdauer auch auf die Pflichten gem. Art. 8 Abs. 3 bis 5 PrSG bezieht.[1692] Zudem sollte ergänzt werden, dass alle Nachmarktpflichten angemessen sein müssen, nicht nur jene in Art. 8 Abs. 2 PrSG.[1693] Zusätzlich befindet sich mit der Pflicht zur Sicherstellung der Rückverfolgbarkeit nach Art. 8 Abs. 2 lit. c PrSG eine Vormarktpflicht im 3. Abschnitt «Pflichten nach dem Inverkehrbringen».[1694] Solche Unklarheiten und systematischen Probleme machen es den Herstellern nicht einfacher, das PrSG richtig anzuwenden, und sollten deshalb verbessert werden. Da es sich beim PrSG um nachvollzogenes EU-Recht handelt und dieses sowieso europakonform ausgelegt werden muss, sollte dies im Gesetz auch so vermerkt werden. Als Vorlage könnte – je nach Ausgestaltung – Art. 1 MaschV dienen. Auch dies würde die Auslegung des Gesetzes einfacher machen und es wäre klar, welche Materialien beizuziehen wären.[1695] Wie im europäischen Produktsicherheitsrecht sollte das PrSG im Singular benannt werden und künftig «Bundesgesetz über die Produktsicherheit» statt «Bundesgesetz über die Produktesicherheit» heissen.[1696] Die momentan 415

1690 S. o., Rn. 182.
1691 S. o., Rn. 64. Siehe auch ROSENTHAL, Jusletter 05.08.2024, Rn. 90.
1692 S. o., Rn. 292.
1693 S. o., Rn. 309.
1694 S. o., Fn. 1257.
1695 Siehe dazu den Vorschlag von KRAMER/ARNET, S. 357 Fn. 1109.
1696 S. o., Rn. 142.

uneinheitliche Terminologie in der EU und der Schweiz erschwert die Recherche zum Produktsicherheitsrecht unnötig. Dasselbe gilt für das PrHG. Zudem sollte das Verhältnis zwischen Sektorrecht und PrSG klarer ausgestaltet werden. Es sollte bspw. klar geregelt sein, dass das PrSG ein Mindestschutzniveau enthält.[1697] Die Teilrevision des PrSG bietet die Chance, das Gesetz systematisch neu zu strukturieren, Unklarheiten zu bereinigen und den Gesetzestitel leicht anzupassen.

II. Explizite Erfassung von Software im PrSG

416 Obwohl Software und damit KI-Systeme vorliegend als Produkte i.S.d. PrSG anerkannt werden,[1698] sollte Art. 2 Abs. 1 PrSG zugunsten der Rechtssicherheit geändert werden. Am klarsten wäre eine Ergänzung, dass Software ebenfalls als Produkt erfasst ist. Dies könnte bspw. analog der Aufzählung von Elektrizität in Art. 3 Abs. 1 lit. b PrHG geschehen. Eine solche Änderung würde den Produktebegriff im PrSG und im PrHG künftig kompatibel halten, da sich die Entwicklung des PrHG ebenfalls in Richtung Erfassung von Software als Produkt entwickelt.[1699] Ganz generell sollten das PrSG und das PrHG nicht unabhängig voneinander revidiert werden, weil die Produktsicherheit und die Produkthaftpflicht eng verbunden sind.[1700] Durch die klare Erfassung von Software im PrSG kann auch eine Kompatibilität mit dem EU Recht sichergestellt werden, da Software in der GPSR[1701] und der PLD 2024[1702] ebenfalls als Produkt erfasst ist. Eine explizite Nennung von KI im Gesetz ist nicht nötig, da es sich dabei immer um Software handelt und sie somit miterfasst wird. Es ist jedoch wichtig, dass KI-Systeme als Produkte i.S.d. PrSG angesehen werden, da so zumindest auch in der Schweiz minimale Produktsicherheitsvorschriften und damit auch Nachmarktpflichten gelten.

417 Auf eine Unterscheidung zwischen Embedded und Stand-alone-Software sollte verzichtet werden, da sie nicht mehr zeitgemäss ist.[1703] Die Unterscheidung zwischen Individual- und Standardsoftware wird auch immer undeutli-

1697 S. o., Rn. 183.
1698 S. o., Rn. 216.
1699 Zum PrHG wird ebenfalls eine Klarstellung gefordert Batache, Rn. 408, m.w.H.; Fellmann, Haftpflichtrecht, S. 107; Wildhaber, Einführung, S. 40.
1700 Siehe auch Spindler, in: Lohsse/Schulze/Staudenmayer, Liability for AI & IoT, S. 142. S. o., Rn. 148.
1701 Wenn auch nicht explizit s. o., Rn. 223 f.
1702 S. o., Rn. 234.
1703 S. o., Rn. 34.

cher und Software ist deshalb unabhängig davon zu beurteilen, ob sie für viele oder einen Einzelnen entwickelt wurde.[1704] Auch digitale Dienstleistungen wie SaaS sind vom PrSG erfasst,[1705] was bei einer Revision des Gesetzes ebenfalls besser zum Ausdruck gebracht werden könnte. Hier würde die Kompatibilität mit der EU ebenfalls beibahlten werden, da digitale Dienste auch unter die PLD 2024 fallen.[1706] Wichtig ist, dass klare Kriterien entwickelt werden, um eine Abgrenzung zwischen Dienstleistungen und Produkten zu ermöglichen.[1707]

III. Vorschläge zu Nachmarktpflichten

Seit Inkrafttreten der GPSR unterscheiden sich die Nachmarktpflichten im allgemeinen Produktsicherheitsrecht der Schweiz und der EU deutlich. Insbesondere gehen die Pflichten der GPSR zur Vornahme von Korrekturmassnahmen und zur Information von Verbrauchern auf eine strikt regulierte Weise erheblich weiter als die Pflichten in der Schweiz. Umgekehrt kennt die GPSR – anders als das PrSG – weder eine aktive Beobachtungspflicht noch eine Pflicht zur Stichprobenentnahme im Rahmen der passiven Beobachtung. Angesichts des Ziels, mit dem PrSG das Schutzniveau der EU zu erreichen und die wirtschaftliche Kompatibilität zu sichern, erscheint es vertretbar, die aktive Produktbeobachtungs- und die Stichprobenpflicht in der Schweiz aufzuheben.[1708] Dafür müsste für eine Kompatibilität des Sicherheitsniveaus mit der EU in der Schweiz zumindest die Pflicht zur Durchführung von Korrekturmassnahmen übernommen werden.[1709] 418

Nicht empfohlen ist die Übernahme der detaillierten Vorschriften zur formellen Ausgestaltung von Sicherheitswarnungen und Rückrufanzeigen sowie der Abhilfemassnahmen aus dem allgemeinen Produktsicherheitsrecht der EU. In der Schweiz würde die Übernahme der neuen EU-Vorgaben eine erhebliche Einschränkung der Wirtschaftsfreiheit der Hersteller darstellen. Insbesondere die detaillierten Anforderungen an Sicherheitswarnungen und Rückrufanzeigen sowie die vorgesehenen Abhilfemassnahmen würden beträchtliche Kosten verursachen und könnten sich in höheren Preisen für Konsumenten nieder- 419

1704 S. o., Rn. 214.
1705 S. o., Rn. 212.
1706 S. o., Rn. 238.
1707 S. o., Rn. 213.
1708 S. o., Rn. 348.
1709 S. o., Rn. 369.

schlagen. Der Nutzen dieser Pflichten ist zudem umstritten.[1710] Bei den Abhilfemassnahmen handelt es sich zudem nicht um öffentliches Produktsicherheitsrecht und solche Vorschriften wären (wenn überhaupt) im Privatrecht zu regeln.[1711] Ebenfalls nicht empfohlen, ist die Meldepflicht bei Unfällen ohne festgestellte Produktgefahr nach Art. 20 Abs. 1 GPSR.[1712]

420 Stattdessen sollten die Vorteile der technologischen Entwicklung genutzt werden. Im Gegensatz zu herkömmlichen Produkten haben Hersteller von Software, zu welcher weiterhin eine Verbindung aufgebaut werden kann, die Möglichkeit, kontinuierlich und in Echtzeit Rückmeldungen über ihre Produkte zu erhalten.[1713] Das Einrichten von automatischen Rückmeldungen ermöglicht eine schnelle Reaktion und eine verbesserte Fehlerfindung und trägt damit zur Produktsicherheit bei. Zudem soll auf die Wiederherstellung der Sicherheit und die direkte Korrektur von Gefahren «over the air» fokussiert werden. Auch diese Möglichkeiten senken das Risiko, dass weiterhin gefährliche Produkte auf dem Markt sind, obwohl Konsumenten bereits gewarnt wurden. So sind bei Software und Produkten mit integrierter Software keine weitgehenden Abhilfemassnahmen nötig, wenn der Hersteller bspw. einfach ein Sicherheitsupdate installieren kann.[1714] Dies gilt nicht nur für KI-Systeme, sondern für jede Software.[1715]

421 Damit Hersteller ihre Pflicht zur Gefahrenabwehr bei Software- und KI-Systemen erfüllen können, ist es erforderlich, technische Vorkehrungen für eine dauerhafte oder zumindest wiederherstellbare Verbindung mit der in Verkehr gebrachten Software zu schaffen. Da Hersteller bei vernetzten Produkten weiterhin Einflussmöglichkeiten besitzen, sollten sie verpflichtet sein, diese ab einem bestimmten Gefahrenpotenzial auch wahrzunehmen. Realistischerweise können nur jene Hersteller, die an der Entwicklung der Software beteiligt waren, eine aktive integrierte Produktbeobachtung tatsächlich umsetzen.[1716] Solche Pflichten können deshalb eigentlich auch nur von diesen Herstellern verlangt werden. Da mit Einführung des PrSG eine Angleichung des Schutzniveaus an jenes der EU angestrebt wurde,[1717] würde es Sinn ergeben, den Herstellerbegriff

1710 S. o., Rn. 370.
1711 S. o., Rn. 366, 368.
1712 S. o., Rn. 373.
1713 S. o., Rn. 327.
1714 S. o., Rn. 371.
1715 S. o., Rn. 346.
1716 S. o., Rn. 346.
1717 S. o., Rn. 148.

gleich wie in der EU zu definieren.[1718] Problematisch ist jedoch, dass die tatsächlichen Erschaffer von Produkten in der EU nicht als Hersteller zu klassifizieren sind, ausser wenn sie ihre Produkte unter ihrem Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen.[1719] Das heisst dass der Hersteller i.e.S. ohne eine Vermarktung seines Produktes nur in der Schweiz als Hersteller gilt.[1720] Der Hersteller i.e.S. kennt sein Produkt i.d.R. aber besser und hat auch mehr direkten Einfluss darauf, da er das Produkt tatsächlich erschaffen hat. Das ist bspw. in Bezug auf Nachmarktpflichten relevant, da ein Hersteller i.w.S. ein Produkt weniger genau beobachten und vielleicht gar nicht aktualisieren kann.[1721] Will man den Hersteller zu einer erweiterten Produktbeobachtung oder zur Aufrechterhaltung der Möglichkeit zur Aktualisierung seiner Produkte «over the air» verpflichten, muss klar sein, wem eine solche Pflicht realistischerweise auferlegt werden kann. Insgesamt kann die verbleibende Kontrolle des Herstellers über sein Produkt nach dessen Inverkehrbringung zu mehr Nachmarktpflichten führen.

IV. KI-Regulierung in der Schweiz

Um die Definition des KI-Systems bestehen noch immer Unsicherheiten.[1722] KI wird nicht einmal in allen neuen EU-Regulierungen gleich definiert. Die Schweiz müsste sich also nicht zwingend an der KI-VO orientieren, wenn sie KI selbständig definieren und bspw. eine weniger umfassende, liberalere Definition verwenden möchte. Trotzdem ist es aus Sicht einer weiterhin gewünschten wirtschaftlichen Kompatibilität wenig sinnvoll, die Definition abweichend von den drei Definitionen der KI-VO, der OECD und des Europarates, die alle sehr ähnlich sind, zu regulieren.[1723] Die Schweiz befindet sich mitten im Regulierungsprozess für KI. Die Regulierung von KI soll in der Schweiz – wo möglich – technologieneutral ausgestaltet werden. Es könnte auch auf eine eigene KI-Definition verzichtet werden. Auf jeden Fall sollte nicht ein noch umfassenderer Ansatz als jener der EU gewählt werden. 422

Die Gefahren, die durch Software verursacht werden können, können von KI zwar verstärkt werden, sind aber nicht davon abhängig. Das heisst, dass viele der vorliegend beschriebenen Gefahren gar keine KI «benötigen», sondern das 423

1718 S. o., Rn. 288.
1719 S. o., Rn. 276.
1720 S. o., Rn. 288.
1721 S. o., Rn. 289.
1722 S. o., Rn. 140.
1723 S. o., Rn. 140.

Gefahrenpotenzial in der Nutzung von Software generell liegt. Zudem gibt es innerhalb der Kategorie der KI-Systeme unterschiedlich hohe Risiken. Die EU beachtet das ebenfalls, weil vor allem Hochrisiko-KI-Systeme reguliert werden und nicht «normale» KI. Aufgrund ihrer dynamischen Veränderungsmöglichkeit durch selbständiges Lernen und ihrer Opazität sind durch KI verursachte Gefahren grundsätzlich weniger vorhersehbar als beim Einsatz von anderen Arten von Software. Zudem haben Hersteller weniger Kontrolle bei lernfähigen Produkten.[1724] Für die Gefahrenerkennung ist deshalb relevant, dass nachvollzogen werden kann, was die Ursache für eine allfällige Gefahr ist. Kann die Ursache erkannt werden, kann die Sicherheit eines Produktes bspw. durch ein Update wiederhergestellt werden. Auch die verschiedenen Einsatzmöglichkeiten beeinflussen das Risikopotenzial von KI-Systemen.[1725] Gehen mit gewissen KI-Systemen deshalb erhöhte Risiken einher, sollten diese im entsprechenden Sektorrecht geregelt werden, anstatt erhöhte Anforderungen für alle KI-Systeme im PrSG oder einem anderen Gesetz zu schaffen.[1726] Eine besondere Regelung von KI sollte sich sinnvollerweise am von der KI ausgehenden Risiko orientieren. Der risikobasierte Ansatz der KI-VO, der lediglich Herstellern von Hochrisiko-KI-Systemen Nachmarktpflichten auferlegt, stellt sich deshalb auch als gangbarer Weg für die Schweiz heraus. Auf Nicht-Hochrisiko-KI-Systeme können die Nachmarktpflichten aus dem PrSG als Auffanggesetz angewandt werden. Somit existieren bereits Mindestvorschriften für KI im PrSG. Um mit der EU kompatibel zu bleiben, könnten diese im sinnvollen Rahmen entlang der GPSR[1727] ausgebaut werden.

1724 S. o., Rn. 62.
1725 S. o., Rn. 231.
1726 Siehe auch BAKOM, Überblick Sektorregulierung KI, S. 7 f.
1727 S. o., Rn. 417 ff.

Diese Publikation untersucht die produktsicherheitsrechtlichen Nachmarktpflichten für Hersteller von Software- und KI-Produkten unter Berücksichtigung ihrer technischen Veränderlichkeit nach dem Inverkehrbringen am Beispiel von Smart Home Devices. Im Zentrum steht ein Rechtsvergleich zwischen der Schweiz und der EU, wobei das schweizerische Produktesicherheitsgesetz (PrSG) der europäischen Produktsicherheitsverordnung (GPSR) und der KI-Verordnung (KI-VO/AI Act) gegenübergestellt wird. Ein wesentlicher wissenschaftlicher Beitrag ist die Auslegung von Stand-alone-Software als Produkt. Die Arbeit evaluiert Anforderungen an die produktsicherheitsrechtlichen Nachmarktpflichten, bestehend aus Gefahrenerkennungsmassnahmen bzw. die Beobachtung nach dem Inverkehrbringen, Gefahrenabwendungsmassnahmen, Melde- sowie Aufbewahrungs- und Aktualisierungspflichten. Sie schliesst mit Reformvorschlägen für die Schweiz.