3. Kapitel: Die Resilienz in der DSGVO

Der nachfolgend zu untersuchende Rechtsbegriff „Resilienz" wird in Art. 32 DSGVO eingeführt, der nach seiner Überschrift die „Sicherheit der Verarbeitung" zum Gegenstand hat.[153]

Um die Bedeutung dieses Rechtsbegriffs vollständig verstehen zu können, muss zunächst der Anwendungsbereich und der Normauftrag des Art. 32 innerhalb der DSGVO bestimmt werden (A.). Anschließend wird unter B. herausgearbeitet, welchem Schutzgut Art. 32 DSGVO und damit auch die Sicherstellung der Resilienz dient, wobei auch hierfür zunächst die Frage der Schutzgüter der DSGVO als solcher beantwortet werden muss.

Unter C. folgt die eigentliche Auslegung und Begriffsbestimmung der Resilienz. Im letzten Schritt dieses Teils (D.) wird die datensicherheitsrechtliche Bedeutung der so definierten Resilienz anhand der Manipulation personalisierter Dienste mit ihrer im vorangegangenen Teil dargestellten Funktionsweise demonstriert.

A. Anwendungsbereich von Art. 32 DSGVO

Zunächst wird der Anwendungsbereich von Art. 32 DSGVO dargestellt. Zur Gewährleistung der „Sicherheit der Verarbeitung" verpflichtet Abs. 1 den Verantwortlichen sowie den Auftragsverarbeiter zur Vornahme geeigneter technischer und organisatorischer Maßnahmen (toM). Diese Handlungspflicht findet sich in der DSGVO als solche auch in den Art. 24 und 25 DSGVO. Dadurch ist die Maßnahmenpflicht nun deutlich breiter ausgestaltet, als dass dies bislang durch § 9 BDSG i.V.m. der zugehörigen Anlage der Fall war.

153 In Deutschland war die Datensicherheit bis dahin ausschließlich in § 9 BDSG a.F. i.V.m. der zugehörigen Anlage geregelt. Nach dieser Vorschrift hatten die Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, „technische[n] und organisatorische[n] Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Jedoch verfolgen diese drei Normen mit der Pflicht zur Implementierung von toM jeweils eigene Schutzzwecke:

Art. 24 spricht insoweit allgemein von der Sicherstellung und Nachweisbarkeit der Einhaltung der DSGVO, Art. 25 Abs. 1 von der wirksamen Umsetzung der Datenschutzgrundsätze nach Art. 5 DSGVO und der Aufnahme notwendiger Garantien (Datenschutz durch Technikgestaltung) bzw. Art. 25 Abs. 2 von der Gewährleistung von Datenschutz durch datenschutzfreundliche Voreinstellungen. Schließlich zielt Art. 32 unter der Überschrift „Sicherheit der Verarbeitung" auf die Gewährleistung eines dem Risiko für Rechte und Freiheiten natürlicher Personen angemessenen Schutzniveaus ab.

Eine trennscharfe Abgrenzung der Anwendungsbereiche ist mit dieser Feststellung jedoch insbesondere zwischen Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) (Grundsatz der Integrität und Vertraulichkeit) und Art. 32 DSGVO noch nicht erreicht. Im Weiteren folgt daher die Bestimmung des Anwendungsbereichs des Art. 32 DSGVO in zwei Schritten: Im ersten Schritt wird eine Normenübersicht der Art. 24, 25 und 32 DSGVO vorgenommen (I.). Im zweiten Schritt (II.) folgt auf dieser Grundlage die Einordnung des Art. 32 DSGVO und die Abgrenzung seines Anwendungsbereichs gegenüber dem sachnähesten Art. 25 Abs. 1 i.V.m. Art 5 Abs. 1 lit f) DSGVO.

I. Normenübersicht

Zunächst wird eine systematische Normenübersicht vorgenommen, wobei eine Dekomposition der Normen in ihre unterschiedlichen Bestandteile erfolgt (1.). Diese werden im Anschluss in einer Tabelle gegenübergestellt (2.)

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

I. Dekomposition der einzelnen Normen

a. Art. 24 DSGVO

Art. 24 DSGVO bildet als erste Norm des Abschnitts die Grund- bzw. Generalnorm.[154] Sie verlangt von dem Verantwortlichen unter „Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen [zu treffen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt."

Aus ihr lassen sich bereits vier für den Vergleich der Normen wichtige Kernelemente identifizieren: Zunächst die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung als „*Modalitäten der Verarbeitung*" (1.). Darauf folgt das „*Risiko*" (2.), beschrieben anhand der Merkmale der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere in Bezug auf die Rechte und Freiheiten natürlicher Personen.[155] Diese beiden Elemente sind die in allen drei Normen enthaltenden Kriterien, die es bei der Bestimmung von Art und Umfang der zu treffenden toM zu berücksichtigen gilt. Darauf folgt das ebenfalls in allen drei Normen vertretene Element des *Handlungsauftrags* (3.), nämlich die Pflicht zur Vornahme von toM. Schließlich besteht das divergierende Element des *Schutzzwecks (4.)*, hier in Form der Sicherstellung und des Nachweises der Einhaltung der DSGVO im Rahmen der Verarbeitung.

Allen Normen ist außerdem gemein, dass sie den Handlungsauftrag an das Risiko knüpfen, d.h. einen risikobasierten Ansatz verfolgen.[156] Daraus folgt auch, dass bei dem Pflichtenkanon der Art. 24, 25, 32 DSGVO stets eine Kosten-Nutzen-Analyse vorzunehmen ist, anhand derer die Risikoreduktion durch die Maßnahmen mit dem hierfür notwendigen Aufwand abgewogen werden muss.[157]

---

154 *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 24, Rn. 9; *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 24, Rn. 5.

155 Vgl. EG 75 DSGVO.

156 Vgl. *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 2.

157 Ausführlich zur Angemessenheit: S. 167 f. Dabei wird nicht übersehen, dass in Art. 24 DSGVO ein expliziter Verweis auf die Implementierungskosten fehlt. Gleichwohl ergibt sich bereits aus Art. 52 Abs. 1 S. 2 GRC, dass der Verantwortliche nur

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

b. Art. 25 DSGVO

Die soeben vorgezeichnete Grundstruktur hält auch Art. 25 Abs. 1 DSGVO bei. Bei den zu berücksichtigenden Kriterien tritt nun jedoch zusätzlich der „Stand der Technik" sowie die „Implementierungskosten" hinzu.

Der Schutzzweck ist gegenüber Art. 24 DSGVO konkretisiert:[158] Er betrifft nun nicht mehr allgemein die Einhaltung der DSGVO, sondern nach Art. 25 Abs. 1 DSGVO sollen die *Datenschutzgrundsätze nach Art. 5 DSGVO wirksam umgesetzt* werden und es sollen die notwendigen Garantien getroffen werden, um den Anforderungen der DSGVO zu genügen. Nach Art. 25 Abs. 2 DSGVO sollen darüber hinaus toM zur Gewährleistung von datenschutzfreundlichen Voreinstellungen getroffen werden.

Zu den Datenschutzgrundsätzen gehört insbesondere auch Art. 5 Abs. 1 lit f) DSGVO, nämlich die Verarbeitung in einer Weise, „die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung […] (‚Integrität und Vertraulichkeit')". Die toM nach Art. 25 Abs. 1 DSGVO sollen damit in Umsetzung dieses Grundsatzes insbesondere die *Integrität und Vertraulichkeit von personenbezogenen Daten gewährleisten*. Zusätzlich wird auch das Schutzziel der *Verfügbarkeit* in diesen Grundsatz hineingelesen,[159] wofür insbesondere die Beeinträchtigungsalternativen des unbeabsichtigten Verlusts und der unbeabsichtigten Zerstörung von personenbezogenen Daten sprechen.

Daneben enthält Art. 25 Abs. 1 DSGVO ein *perspektivisches Element*. Der Verantwortliche soll die entsprechenden toM sowohl „zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung" treffen. Der Zeitpunkt der Festlegung der Mittel ist jener, „in dem der Verantwortliche entscheidet, wie die Verarbeitung durchgeführt wird, wie die Verarbeitung abläuft und welche Mechanismen

---

verhältnismäßige Maßnahmen treffen muss, wobei insbesondere die Risiken den Kosten gegenüberzustellen sind, *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 11; zum Teil wird das Merkmal der Angemessenheit außerdem auch aus der Pflicht zur Vornahme „geeigneter" Maßnahmen herausgelesen, *Mantz*, in: Sydow/Marsch, DS-GVO, BDSG, 3. Auflage 2022, Art. 32, Rn. 30 f.

158 *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 25, Rn. 8.

159 *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 5, Rn. 167.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

für die Durchführung der Verarbeitung genutzt werden."[160] Durch die Bezugnahme auf diesen Zeitpunkt bringt der Gesetzgeber zum Ausdruck, dass diese toM bereits frühestmöglich im Rahmen der Konzeption und der Entwicklung der Datenverarbeitungsvorgänge zu treffen sind und daher im Idealfall zu einem von vorneherein „eingebauten Datenschutz" führen.[161] Während der „eigentlichen Verarbeitung" muss der Verantwortliche dann die entsprechenden Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen aufrechterhalten, was insbesondere fortwährende Neubewertungen der Risiken sowie des Stands der Technik beinhaltet und -bei entsprechend erkanntem Bedarf- eine Aktualisierung der Maßnahmen erfordert.[162]

c. Art 32 Abs. 1 DSGVO

Art. 32 Abs. 1 verpflichtet zunächst anders als die übrigen genannten Normen bezüglich der Adressaten neben dem Verantwortlichen auch den Auftragsverarbeiter. Die zu berücksichtigenden Faktoren sind dagegen deckungsgleich zu Art. 25 Abs. 1 DSGVO (Stand der Technik, Implementierungskosten, Modalitäten der Verarbeitung sowie das Risiko). Der Schutzzweck hingegen besteht nun darin ein „dem Risiko angemessenes Schutzniveau zu gewährleisten."

Als weitere Besonderheit wird in Art. 32 DSGVO der Handlungsauftrag näher konkretisiert. Die toM schließen demnach „gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit [Resilienz] der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

160 EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 12, Rn. 35.
161 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 25, Rn. 16 f. mit Verweis auf andere Sprachfassungen; *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 25, Rn. 1.
162 EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 12, Rn. 37 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung."

Schließlich werden in Art. 32 Absatz 2 ähnlich Art. 5 Abs. 1 lit f) DSGVO zu vermeidende Ereignisse definiert, deren zugehörige Risiken entsprechend zu berücksichtigen sind: „Demnach sind bei der Beurteilung eines angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind." Auch hierin sind die *Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit* zu sehen.[163] *Perspektivisch* ist hier zu beachten, dass die Daten dem Wortlaut nach bereits „verarbeitet wurden", d.h. es wird von einer bestehenden Verarbeitung ausgegangen. Zur Verdeutlichung folgt nun unter 2. noch eine tabellarische Übersicht der genannten Normen.

2. Tabellarische Übersicht

Tabelle 1: Art. 24/25/32 DSGVO

	Art. 24 Abs. 1	**Art. 25 Abs. 1**	**Art. 32 Abs. 1, 2**
Einheitliche, zu berücksichtigende Kriterien	Modalitäten der Verarbeitung (Art, Umfang, Umstände, Zwecke), Risiko für Rechte und Freiheiten natürlicher Personen		
Besondere, zu berücksichtigende Kriterien		Stand der Technik Implementierungskosten	Stand der Technik Implementierungskosten
Schutzzweck:	nachweisbare Einhaltung der DSGVO	Wirksame Umsetzung der Datenschutzgrundsätze + entsprechender Garantien	Gewährleistung eines risikoangemessenen Schutzniveaus
Handlungsauftrag:	Geeignete technische und organisatorische Maßnahmen		

163 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 60; *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 61.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Adressat:	Verantwortlicher	Verantwortlicher	Verantwortlicher + Auftragsverarbeiter
Gewährleistung von Vertraulichkeit und Integrität bzw. Verfügbarkeit		*i.V.m. Art. 5 Abs. 1 lit f):* in einer Weise verarbeitet werden, die insb. Schutz gewährt vor: unbefugter oder unrechtmäßiger Verarbeitung; unbeabsichtigtem/er Verlust, Zerstörung, Schädigung	Minimierung von Risiken durch unbefugte Offenlegung unbefugten Zugang unbeabsichtigte oder unrechtmäßige(r) Vernichtung, Verlust oder Veränderung von personenbezogen Daten, die verarbeitet wurden

II. Verhältnis der Art. 25 Abs. 1, 32 DSGVO

Im Weiteren soll die konkrete Einordnung von Art. 32 DSGVO erfolgen. Dabei wird nun die Abgrenzung von Art. 25 Abs. 1 i.V.m. dem Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit f) DSGVO zu Art. 32 DSGVO vorgenommen, um den Anwendungsbereich von letzterem und damit auch der Resilienz zu bestimmen.

Zwar konkretisiert nämlich auch Art. 32 DSGVO den genannten Grundsatz,[164] gleichwohl ist davon auszugehen, dass sowohl dem Datenschutz durch Technikgestaltung in Umsetzung dieses Grundsatzes (Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f. DSGVO) als auch der Datensicherheit nach Art. 32 DSGVO jeweils eigenständige Anwendungsbereiche und Normaufträge zukommen.

164 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn 2; *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 1; *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 1 m.w.N.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Entscheidend für diese Abgrenzung sind insbesondere die inhaltlichen Unterschiede zwischen diesen Normen (1.), die nun gegenübergestellt werden. Anschließend wird EG 83 der DSGVO betrachtet, der übergeordnete Hinweise zum Anwendungsbereich der jeweiligen Normen enthält (2.). Schließlich werden unter 3. die so voneinander abgegrenzten Normaufträge noch einmal zusammengefasst.

1. Inhaltliche Unterschiede der Normen

Bei den inhaltlichen Unterschieden fallen zunächst (a.) die unterschiedlichen Perspektiven (Art. 25 DSGVO: Gestaltung der Verarbeitung, Art. 32 DSGVO: Sicherung der bestehenden Verarbeitung) auf. Weiterhin (b.) ist zu beachten, dass nur Art. 32 Abs. 1 lit b) DSGVO explizit auch die verarbeitenden Systeme und Dienste anspricht. Außerdem werden unterschiedliche Rollen (Verantwortlicher und/oder Auftragsverarbeiter) adressiert (c.) und es werden unterschiedliche Schutzrichtungen bei den drei Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität beschrieben (d.).

a. Perspektiven

Nach Art. 25 Abs. 1 DSGVO sind die Maßnahmen zur Umsetzung der Datenschutzgrundsätze wie beschrieben schon zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung zu treffen. Die Mittel meinen dabei die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird,“[165] mithin die Gestaltung des Verarbeitungsvorgangs. Durch den Verweis auf den „Zeitpunkt dieser Gestaltung“ wird deutlich, dass die toM in den Gestaltungsvorgang implementiert werden sollen, die Verarbeitung also gleichermaßen mitgestalten.[166] Korrespondierend verlangt auch Art. 5 Abs. 1 lit f) DSGVO, dass personenbezogene Daten „*in einer Weise verarbeitet werden*“, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.

Anders liegt es hingegen bei Art. 32 DSGVO: Eine ausdrückliche perspektivische Zuweisung zum Handlungsauftrag fehlt zwar, allerdings wird in Abs. 2 auf Beeinträchtigungen der Schutzziele an Daten abgestellt, die bereits „verarbeitet *wurden*“. Aus dieser grammatischen Gestaltung als pas-

165 Art.-29 Datenschutzgruppe, WP 169, 16.02.2010, S. 16.

166 Von einem „eingebauten Datenschutz“ sprechend: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 1.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sives Präteritum wird, wie bereits angedeutet, sichtbar, dass Art. 32 DSGVO perspektivisch von einer bereits bestehenden Verarbeitung ausgeht, im Rahmen derer die Daten z.B. bereits erhoben und gespeichert wurden und somit die zuvor genannte Gestaltung, d.h. insbesondere der Verarbeitungsablauf und -umfang abgeschlossen bzw. festgelegt ist. Der Normauftrag des Art. 32 DSGVO ist es nun diese bestehende Verarbeitung zu sichern.

b. Umsetzung der Verarbeitung durch Systeme und Dienste

Auch die explizite Adressierung von Systemen und Diensten in Art. 32 Abs. 1 lit b) DSGVO stützt diese These, da sich diese als (sozio-)technische Mittel der Verarbeitung logisch von der eigentlichen „Verarbeitung" unterscheiden lassen. Diese Verarbeitung ist nach Art. 4 Nr. 2 DSGVO nur der (mithilfe automatisierter Verfahren) vorgenommene Vorgang, der vom Verantwortlichen abstrakt beschrieben, festgelegt und ausgestaltet werden kann (z.B.: welche Daten werden verarbeitet und wie lange (Umfang), wie läuft diese ab, d.h. welche Abteilungen und ggf. auch Dritte[167] benötigen Zugang und wofür (Zwecke) und inwieweit kann auch mit pseudonymen/anonymen Daten gearbeitet werden). Im Rahmen dieser Ausgestaltung sollen nach Art. 25 Abs. 1 DSGVO insbesondere die Datenschutzgrundsätze wirksam umgesetzt werden.

Dagegen adressiert Art. 32 DSGVO die Datensicherheitsanforderungen in der Phase der praktischen Umsetzung der Verarbeitung, welche unter Zuhilfenahme von informationstechnischen Systemen und Diensten (sowie entsprechendem Bedienpersonal) durchgeführt wird.

c. Rollenansprache

Während Art. 25 DSGVO *nur den Verantwortlichen* adressiert, adressiert Art. 32 DSGVO daneben *auch den Auftragsverarbeiter*. Nach Art. 4 Nr. 7 DSGVO hat allein der Verantwortliche die Entscheidungsgewalt über Zwecke und Mittel der Verarbeitung,[168] d.h. nur er (und nicht der Auftragsverarbeiter Art. 4 Nr. 8, Art. 28 Abs. 3 lit a) DSGVO) bestimmt wie soeben

167 *Arning/Rothkegel*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art 4, Rn. 181.

168 *Klabunde*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 4, Rn. 36.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

beschrieben über Zweck sowie Umfang und Gestaltung (d.h. die „Mittel") der Verarbeitung[169] im Rahmen des Art. 25 Abs. 1 DSGVO.

Dagegen kann und muss die *Sicherheit* der so gestalteten *Verarbeitung sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter* (Art. 32 Abs. 1, Art. 28 Abs. 3 lit b DSGVO) gewährleistet werden. Die insoweit zu treffenden technischen und organisatorischen Maßnahmen betreffen somit nicht die Gestaltung der eigentlichen Verarbeitung selbst, sondern setzen auf der Verarbeitung auf, um diese entsprechend zu sichern.

d. Voluntative Schutzrichtungen

Die bereits dargestellte Unterscheidung zwischen der Gestaltung der Verarbeitung und der Sicherung derselben wirkt sich auch mit Blick auf die Schutzziele und die jeweiligen voluntativen Schutzrichtungen aus, d.h. ob nur vor vorsätzlichen oder auch vor fahrlässigen Ereignissen geschützt werden soll.

i. Vertraulichkeit

Nach dem Wortlaut stellt Art. 25 Abs. 1 i.Vm. Art. 5 Abs. 1 lit f) DSGVO bezüglich des Schutzes der Vertraulichkeit[170] auf eine *unbefugte oder unrechtmäßige Verarbeitung* ab und nicht wie in Art. 32 Abs. 2 DSGVO auf eine *unbefugte Offenlegung* von bzw. den *unbefugten Zugang* zu Daten.

Unbefugt meint dabei die *Tätigkeit eines Dritten* i.S.v. Art 4 Nr. 10 DSGVO, der dem Verantwortlichen nicht zuzurechnen ist.[171] Ein Dritter ist negativ legaldefiniert als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer

- der betroffenen Person,
- dem Verantwortlichen,
- dem Auftragsverarbeiter und

169 *Arning/Rothkegel*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art 4, Rn. 181; EDSA, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 02.09.2020, S. 13, Rn. 33.

170 Siehe hierzu auch EG 39, S. 12 DSGVO.

171 *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 5, Rn. 74.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

– den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten".[172]

Unter den letztgenannten Punkt fallen über das Attribut der Befugnis auch alle Personen, die bei dem Verantwortlichen beschäftigt sind und für die gegenständliche Datenverarbeitung zuständig sind. Dritte sind umgekehrt somit auch die Personen unter unmittelbarer Verantwortung des Verantwortlichen oder Auftragsverarbeiters, die eine *unbefugte Verarbeitung* vornehmen, d.h. wenn sie Daten ohne entsprechende Weisung verarbeiten.[173]

Eine *unbefugte Verarbeitung* im Sinne des Art. 25 Abs. 1 i.Vm. Art. 5 Abs. 1 lit f) DSGVO liegt mithin vor, wenn die Verarbeitung durch Dritte, also entweder durch unzuständige Personen (bzw. Abteilungen) oder auch externe Dienstleister, die Zugriff auf die Verarbeitung haben (z.B. externe IT-Dienstleister), vorgenommen wird. *Unrechtmäßig* hingegen ist die Verarbeitung, die nicht durch einen Dritten, sondern insbesondere durch den Verantwortlichen selbst oder einen Auftragsverarbeiter vorgenommen wird, wenn hierfür keine Rechtsgrundlage existiert.[174] Man könnte durch die damit verbundene Überschreitung bestehender Verarbeitungsrechte auch von einer *überschießenden Verarbeitung* sprechen. Diese unzulässigen Verarbeitungen verletzten insoweit vorsätzlich die Vertraulichkeit der Daten.[175]

Art. 32 Abs. 2 DSGVO hingegen spricht hinsichtlich der Vertraulichkeit nicht von einer „Verarbeitung", sondern von *unbefugter Offenlegung* von bzw. dem *unbefugten Zugang* zu Daten. Dabei wird nicht verkannt, dass der Verarbeitungsbegriff nach Art. 4 Nr. 2 DSGVO die Offenlegung mitumfasst. Gleichwohl ist davon auszugehen, dass der Gesetzgeber hier (bewusst) keine Redundanz geschaffen hat, sondern die unterschiedliche Terminologie einem dahinterstehenden Regelungskonzept folgt: In diesem Kontext kann Verarbeitung im Sinne eines grundlegend geordneten Datenverarbeitungsvorgangs verstanden werden. Dagegen erfasst der Begriff des *unbefug-*

172 Die Listendarstellung wurde aus Gründen der Lesbarkeit durch den Autor ergänzt.

173 Vgl. hierzu exemplarisch die Bußgeldentscheidung des *LfDI BW* zu einem Polizeibeamten, der ohne dienstlichen Bezug die Halterdaten einer Zufallsbekanntschaft aus dem entsprechenden Informationssystem abfragte: LfDI BW, Pressemitteilung vom 18.06.2019, S. 1.

174 *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 5, Rn. 74.

175 Die (berechtigte) Vertraulichkeitserwartung schließt insofern mit ein, dass die preisgegeben Daten nur im Rahmen der jeweiligen Verarbeitung (in die ggf. eingewilligt und über die aufgeklärt wurde) verwendet werden.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ten Zugangs, den sich ein Dritter verschafft, vorsätzliche, *deliktstypische Handlungen*, die z.B. auch den Tatbestand des „Ausspähens von Daten" nach § 202a StGB erfüllen können. Dies beschreibt somit keine „Verarbeitungen", sondern Angriffe sowohl von außen als auch durch (böswillige) Mitarbeitende (Innentäter:innen) des Verantwortlichen.[176] Daneben kann eine *unbefugte Offenlegung* auch fahrlässig geschehen: So kann es durchaus vorkommen, dass personenbezogene Daten aufgrund von IT-Fehlern beim Verantwortlichen versehentlich öffentlich gemacht und damit unbefugten Personen offengelegt werden.

Insgesamt ist festzuhalten, dass Art. 25 Abs. 1 i.Vm. Art. 5 Abs. 1 lit f) DSGVO *unrechtmäßige und unbefugte, d.h. vorsätzliche Vertraulichkeitsverletzungen* durch unzulässige bzw. überschießende Verarbeitungen erfasst und Art. 32 Abs. 2 DSGVO *vorsätzliche* Vertraulichkeitsverletzungen durch Angriffe *unbefugter* Dritten, was demnach sowohl Innen- als auch Außentäter:innen sein können sowie *fahrlässige* Offenlegungen von Daten an unbefugte Dritte.

ii. Verfügbarkeit/Integrität

Auch im Rahmen des Schutzes der Verfügbarkeit[177] und Integrität bestehen entsprechende Unterschiede:

Nach Art. 5 Abs. 1 lit f) DSGVO gilt es *den/die unbeabsichtigte(n) Verlust, Zerstörung oder Schädigung* von Daten zu vermeiden. Dagegen will Art. 32 Abs. 2 DSGVO die Risken minimieren, die aus *Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig* der Daten resultieren. Somit gilt für die Modalitäten der Verfügbarkeits- und Integritätsverletzungen, dass nur Art. 32 Abs. 2 DSGVO neben unbeabsichtigten auch die unrechtmäßigen Verletzungen erfasst.

Unbeabsichtigt (engl. accidental) erfasst alle Verletzungen, die fahrlässig oder zufällig, also gewissermaßen als „Unfall" geschehen. *Unrechtmäßig* hingegen ist wie bereits dargestellt als vorsätzlicher Rechtsbruch zu verstehen; da sich der Begriff hier allerdings nicht auf die „Verarbeitung" bezieht,

176 Vgl. *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 34.

177 Siehe zur zusätzlichen Erfassung der Verfügbarkeit von Art. 5 Abs. 1 lit f) bereits zuvor S. 84, Fn. 159.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

kann eine entsprechende Handlung prinzipiell von jedem und nicht nur von einem „Verarbeiter" vorgenommen werden.[178]

Entsprechend lassen sich die Tatbestandsalternativen im Sinne des Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO wie folgt auslegen: Es soll sichergestellt werden, dass befugte Personen die Daten im Rahmen der Verarbeitung nicht *unbeabsichtigt* (fahrlässig) löschen oder verändern.

Nach *Art. 32 Abs. 2 DSGVO* soll hingegen neben dem Schutz vor *unbeabsichtigten* Ereignissen (zur Abgrenzung im Fazit unter 3.) zusätzlich auch sichergestellt werden, dass die Daten nicht *unrechtmäßig,* mithin *vorsätzlich* beeinträchtigt werden. Dies betrifft zunächst deren vorsätzliche „Vernichtung" etwa durch einen Angriff in Form der Löschung oder der Verschlüsselung durch eine Ransomware. Zweitens soll der vorsätzliche „Verlust" der Daten, d.h. eine Vereitelung des Zugangs zu den noch existenten Daten vermieden werden, z.B. bei Ransomware oder bei Diebstahl von Speichermedien[179], vermieden werden. Beide Alternativen beziehen sich auf die *Verfügbarkeit.*[180] Schließlich soll neben der unbeabsichtigten auch die *unrechtmäßige Datenveränderung,* d.h. auch die böswillige Manipulation der Daten ausgeschlossen werden.

Im Ergebnis erfasst Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO *somit nur fahrlässige Integritäts- und Verfügbarkeitsverletzungen.* Art. 32 DSGVO hingegen erfasst sowohl *fahrlässige als auch vorsätzliche Integritäts- und Verfügbarkeitsverletzungen* durch Angriffe.

---

178 Diese Differenzierung im voluntativen Element (unbeabsichtigt ggü. unbeabsichtigt und unrechtmäßig) wollte der Gesetzgeber möglicherweise auch in den Verletzungsformen ausdrücken, soweit in Art. 5 Abs. 1 lit f) DSGVO neben Verlust von Schädigung (damage) statt wie in Art. 32 Abs. 2 DSGVO Veränderung (alteration) gesprochen wird. Semantisch könnte man hieraus erkennen, dass mit (unbeabsichtigter) Schädigung also gewissermaßen eher noch ein versehentliches Verhalten gemeint ist, wohingegen die (unbeabsichtigte oder unrechtmäßige) Veränderung etwas mehr noch auch ein zielgerichtetes Handeln umfasst: Bei einem versehentlichen Verhalten würde man dem allgemeinen Wortsinn nach wohl weniger von einer „Veränderung", sondern eher (nur) von einer Schädigung sprechen; so dass der Begriff Veränderung insoweit etwas generischer ist. Nach a.A.: *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (406), Fn. 82, hat die Trias „Vernichtung, Verlust, Veränderung" nach Art. 32 Abs. 2, Art. 4 Nr. 12 DSGVO aber dieselbe Bedeutung wie „Zerstörung, Verlust, Schädigung" nach Art. 5 Abs. 1 lit f) DSGVO.

179 In diesem Fall tritt dann zusätzlich zu der Verfügbarkeits- auch eine Vertraulichkeitsverletzung ein, sofern die Daten nicht verschlüsselt waren.

180 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 21; zur Bedeutung der Verfügbarkeit in der Datensicherheit siehe auch: EDSA, Guidelines 9/2022 on personal data breach notification under GDPR, 28.03.2023, S. 8 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

2. Übergreifende Zuordnung in Erwägungsgrund 83

Die bisherigen Feststellungen lassen sich auch durch den Rückgriff auf EG 83 Satz 1 untermauern, in dem beide Aspekte zusammengeführt werden. Hier heißt es:

> „Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen."

Als erstes Indiz drängt sich im Wortlaut zunächst die unterschiedliche Rollenansprache auf: Während Art. 32 DSGVO wie dargestellt den Verantwortlichen *und* den Auftragsverarbeiter, aber Art. 25 DSGVO nur den Verantwortlichen anspricht, werden die beiden Rollen im EG 83 in einem Alternativ-Verhältnis genannt, so dass auch nur einer von beiden erfasst sein kann und damit eine Zuordnung sowohl zu Art. 25 als auch zu Art. 32 DSGVO möglich wird. Diese Zuordnung ergibt sich dann im Detail wie folgt:

Die *Aufrechterhaltung der Sicherheit* weist in Richtung des Art. 32 DSGVO: Dafür spricht der Wortlaut der Überschrift des Art. 32 DSGVO mit „Sicherheit der Verarbeitung"; anders als in Art. 25 Abs. 1 DSGVO, der gerade Datenschutz durch Technikgestaltung (privacy by design) und nicht etwa Sicherheit durch Technikgestaltung (security by design) fordert.[181] Außerdem korrespondiert das Erfordernis der „Aufrechterhaltung" mit Art. 32 Abs. 1 lit b) DSGVO, indem verlangt wird, dass „Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit [Resilienz] der Systeme und Dienste […] *auf Dauer sicherzustellen*" sind.

Die *Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung* weist im Umkehrschluss auf die Gestaltung der Verarbeitung nach Art. 25 Abs. 1 DSGVO hin. Das Merkmal der „Vorbeugung" korrespondiert durch den enthaltenen Präventionsgedanken mit dem in Art. 25 DSGVO ausdrücklich auch fokussierten „Zeitpunkt der Festlegung der Mittel" und bekräftigt damit die gestalterische Prägung des Art. 25 DSGVO, die Daten-

181 Auch wenn dies freilich mittelbar auf die Datensicherheit wirkt, da etwa durch eine Datenverarbeitung mit möglichst wenig Daten (Datenminimierung) und möglichst wenig Personen mit Zugang zu den Daten die dann nach Art. 32 Abs. 1 DSGVO zu sichernde Angriffsfläche verkleinert wird.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

schutzgrundsätze gerade *in* der Verarbeitung *wirksam umzusetzen* bzw. zu implementieren. D.h. die Verarbeitung selbst soll vorbeugend von Anfang an („by Design") so gestaltet werden, dass die Verarbeitung den Anforderungen der DSGVO, insbesondere den Datenschutzgrundsätzen einschließlich Art. 5 Abs. 1 lit f) DSGVO entspricht[182] und eine gegen diese Verarbeitung verstoßende, insbesondere auch überschießende Verarbeitung, verhindert wird.

3. Normaufträge und Fazit

Fraglich ist nun, wie sich nach diesen Feststellungen die Anwendungsbereiche und damit auch die Normaufträge von Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO und dem für diese Untersuchung maßgeblichen Art. 32 DSGVO voneinander abgrenzen lassen.

a. Keine eindeutige Differenzierung nach voluntativem Element und Quelle

Zunächst lässt sich zunächst negativ festhalten, dass sich die Normen nicht eindeutig anhand der Einwirkungen auf Schutzziele mit Blick auf das voluntative Element unterscheiden lassen, sondern dass sich diese zumindest teilweise überschneiden.

182 Vgl. *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 8.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Tabelle 2: Schutzziele in Art. 25 Abs. 1 i.V.m. 5 Abs. 1 lit f) und 32 Abs. 2 DSGVO

	Vertraulichkeit	**Verfügbarkeit/Integrität**
Art. 25 Abs. 1 i.V.m. Art. 5 lit f)	unbefugte oder unrechtmäßige Verarbeitung	Unbeabsichtige(r) Verlust, Zerstörung oder Schädigung
	durch Verantwortlichen oder Dritte (unzuständige Personen, externe Dienstleister)	
Art. 32 Abs. 2	unbefugte Offenlegung unbefugter Zugang	unbeabsichtigte oder unrechtmäßige(r) Vernichtung, Verlust oder Veränderung
	durch Dritte oder, wenn unbeabsichtigt, auch durch Verantwortlichen oder Auftragsverarbeiter	

Sowohl Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) als auch Art. 32 Abs. 2 DSGVO adressieren ausdrücklich sowohl unbefugte bzw. unrechtmäßige (d.h. *vorsätzliche*) als auch unbeabsichtigte, mithin jedenfalls *fahrlässige Ereignisse*. Nach obiger Wortlautauslegung erfasst „unbeabsichtigt" auch zufällige Ereignisse, allerdings erscheint schwer vorstellbar wie *zufälligen Ereignissen* (insbesondere Naturkatastrophen) auf Ebene der Gestaltung der Verarbeitung begegnet werden kann. Der Begriff ist daher für den Bereich des Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) teleologisch zu reduzieren.

Auch bei der Einwirkungsquelle besteht keine stringente Differenzierung: Sowohl Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO als auch Art. 32 DSGVO adressieren interne Ereignisse beim *Verantwortlichen* wie etwa versehentliches Löschen durch Mitarbeitende oder Datenverlust aufgrund von „zufälligen" Hardware-Versagen[183]. Weiterhin werden, wenn auch differenzierend, externe Ereignisse sowohl von Art. 25 Abs. 1 (Verhalten *externer Dienstleister*) als auch von Art. 32 DSGVO (Angriffe von *Dritten,* d.h. wie beschrieben sowohl Innen- als auch Außentäter:innen) adressiert.

Die Abgrenzung ergibt sich aus der besonderen, datenschutzrechtlich geprägten Perspektive mit ihrer eigenen Methodik. Es handelt sich letztlich um eine Abgrenzung anhand von Sphären: Die Verarbeitungssphäre des Verantwortlichen mit allen internen und externen Stellen muss einerseits präventiv und fortlautend im Sinne der Datenschutzgrundsätze nach Art. 25 Abs. 1 DSGVO ausgestaltet sein. Andererseits besteht eine Sphäre

183 *Schultze-Melling*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 32, Rn. 21.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

jenseits dieses verarbeitungsbezogenen Planungshorizonts, in der die so gestaltete Verarbeitung vor „unerwünschten Ereignissen“[184] geschützt werden soll. Hierzu zählen fahrlässige Ereignisse, die sich aber anders als zuvor nicht durch eine Gestaltung der Verarbeitung verhindern lassen als zusätzlich auch zufällige Ereignisse sowie vorsätzlich durch Dritte hervorgerufene Ereignisse. Insgesamt ist somit vor allem nach den jeweiligen Sphären zu unterscheiden, d.h. welche Ereignisse können schon durch die Gestaltung der Verarbeitung vermieden werden und welche erst im Rahmen der Sicherung der Verarbeitung mit ihren Systemen bzw. Diensten.

b. Art. 25 Abs. 1 DSGVO

Nach Art. 25 Abs. 1 DSGVO soll die Verarbeitung im Kontrollbereich des Verantwortlichen zunächst möglichst frühzeitig anhand der Datenschutzgrundsätze (Art. 5 Abs. 1 DSGVO) gestaltet werden.[185]

Hinsichtlich des *Grundsatzes der Integrität und Vertraulichkeit* (und Verfügbarkeit) nach Art. 5 Abs. 1 lit f)[186] soll dabei zunächst sichergestellt werden, dass es nicht zu unbefugten und unrechtmäßige Verarbeitungen (Eingriffe in die „Vertraulichkeit“) kommt.

Eine *unbefugte Verarbeitung* läge beispielsweise in der Verarbeitung personenbezogener Daten durch einen externen IT-Dienstleister zu eigenen Zwecken, etwa um die Nutzung der von ihm implementierten IT-Produkte zu überwachen, ohne dafür einen eigenen Rechtmäßigkeitstatbestand nach Art. 6 DSGVO zu erfüllen oder in einer Verarbeitung durch einen unbefugten Mitarbeitenden.

Unrechtmäßig ist dagegen jede Verarbeitung des Verantwortlichen oder Auftragsverarbeiters, die über den eigentlichen Zweck hinausgeht. Etwa

184 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 59.

185 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 25, Rn. 16, 18.

186 Soll dagegen beispielsweise der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit b) DSGVO) umgesetzt werden, muss die Verarbeitung bei Verfolgung mehrerer Zwecke technisch so ausgestaltet werden, dass für jeden Zweck (z.B. Vertragserfüllung und Werbung) ein separater Einzelprozess vorliegt, so dass diese insbesondere mit ihren Zugriffsrechten unabhängig voneinander beendet werden können. Auch könnten Daten entsprechend gekennzeichnet werden [Tagging]. *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 25, Rn. 16; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 25, Rn. 30.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wenn die Daten von dem Verantwortlichen nur zur Abrechnung eines Dienstens erhoben wurden, dann aber auch zur personalisierten Werbung genutzt werden.

Insoweit muss als technische Maßnahme u.a. durch ein *differenziertes Zugriffsmanagement* sichergestellt werden, dass nur so wenig Personen wie möglich und diese auch nur im notwendigen Umfang an der Verarbeitung beteiligt sind und somit auf die Daten zugreifen können.[187] Außerdem ist ein effektives Kontroll- und Aufsichtssystem (Controlling, organisatorische Maßnahme) erforderlich, dass die erlaubten Verarbeitungsumfänge auch tatsächlich nicht überschritten werden.

Weiterhin sind *eine unbeabsichtigte Zerstörung bzw. Schädigung oder ein unbeabsichtigter Verlust der Daten* (Verfügbarkeit und Integrität) im Rahmen der Verarbeitung zu vermeiden. Gegen ein solches fahrlässiges Verhalten kann wieder durch ein differenziertes Zugriffsmanagement vorgegangen werden, z.B. dass nur bestimmte Personen oder mehrere Personen (Vier-Augen-Prinzip) berechtigt sind, insbesondere besonders sensible Daten zu löschen oder zu verändern.

Vorsätzliche Ereignisse werden hinsichtlich der Verfügbarkeit bzw. Integrität in der Verarbeitungsperspektive des Art. 25 Abs. 1 DSGVO hingegen nicht berücksichtigt. Insofern geht der Schutzzweck des Art. 25 Abs. 1 DSGVO erkennbar davon aus, dass die an der Verarbeitung Beteiligten im wohlverstandenen Eigeninteresse solche destruktiven Eingriffe in die Verarbeitung nicht vornehmen, sondern wie zuvor beschrieben viel mehr vorsätzlich eine zu weitgehende, d.h. *überschießende Verarbeitung* durchführen. Destruktives, vorsätzliches Handeln Dritter fällt insofern unter Art. 32 DSGVO.

c. Art. 32 DSGVO

In einem zweiten Schritt soll die wie zuvor beschrieben ausgestaltete Verarbeitung (insbesondere auch gegenüber Dritten) gesichert werden, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Hierbei sind technische und organisatorische Maßnahmen zu treffen, die ein angesichts der Risiken angemessenes Schutzniveau gewährleisten. In Abgrenzung zu Art. 25 Abs. 1 i.V.m. Art 5 Abs. 1 lit f) DSGVO sind somit die Maßnahmen

187 EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 32.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

auf die Abwehr unerwünschter Ereignisse gerichtet,[188] die *außerhalb des Planungsbereichs des Verantwortlichen liegen* und somit nicht durch die Gestaltung der Verarbeitung (Art. 25 Abs. 1 DSGVO) verhindert werden können.

Ein solches fahrlässiges (*unbeabsichtiges)* Ereignis könnte etwa durch den unsachgemäßen Umgang des Personals mit der Informationstechnik (Hard- und Software) ausgelöst werden[189] (z.B. das Verlieren von Datenträgern, fahrlässige Nichtbefolgung von Richtlinien zur Bedienung oder auch Flüssigkeitsschäden an informationstechnischen Systemen). Fahrlässige Ereignisse können in diesem Bereich auch durch Dritte verursacht werden, etwa wenn die verwendete Hard- und Software Fehler aufweist, die dann zur *Vernichtung* oder *Veränderung* von Daten führen können.[190] Außerdem sind alle *unrechtmäßigen* bzw. *unbefugten*, d.h. vorsätzlichen Angriffe zu berücksichtigen, die entweder von Innen-[191] als insbesondere auch von Außentäter:innen verübt werden können, etwa in Form von Ransomware (*unrechtmäßiger Datenverlust*), Hackerangriffen (*ggf. unrechtmäßige Veränderung*) und Datendiebstahl (*unbefugter Zugang*). Schließlich sind auch zufällige Ereignisse wie etwa höhere Gewalt (Naturkatastrophen) erfasst (z.B. mit der *Folge eines unbeabsichtigten Datenverlusts* durch eine Überschwemmung).[192]

Dabei sollen insbesondere auch die „Systeme und Dienste" mit technischen und organisatorischen Maßnahmen ausgestattet werden, so dass sie eine Datensicherheit gewährleisten, die Einwirkungen unbefugter Dritter auf das System ausschließt als auch dem System ermöglicht, auf interne Störungen wie z.B. Datenverlust oder -veränderung zu reagieren.

---

188 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 59.

189 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 99.

190 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 104.

191 Der Schutz vor Innentäter:innen, die etwa personenbezogene Daten entwenden und veräußern wollen, wird zwar z.T. auch schon dadurch gewährleistet, dass diese beispielsweise als Mitarbeitende einer anderen Abteilung schon aus der Perspektive des Art. 25 i.V.m. Art. 5 Abs. 1 lit f) DSGVO (siehe voranstehendes Kapitel b.) keinen Zugriff auf diese Daten hat. Zusätzlich sind aber ggf. auch Sicherheitsmaßnahmen zu etablieren, dass er sich diesen Zugriff auch nicht durch einen „Innenangriff" verschaffen kann.

192 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 59.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Insgesamt zielt Art. 32 DSGVO somit darauf ab, vorsätzliche, fahrlässige als auch zufällig hervorgerufene, unerwünschte Ereignisse abzuwehren, deren Ursprung intern als auch extern liegen kann und die sich in Abgrenzung zu Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO nicht durch die Gestaltung der Verarbeitung verhindern lassen. Dieser Anwendungsbereich des Art. 32 DSGVO ist somit auch für die weitere Untersuchung der Resilienz maßgeblich.

Zum Abschluss soll das Ergebnis mit den jeweiligen Normadressaten, den unterschiedlichen Perspektiven und den Schutzrichtungen nochmal in folgender Abbildung zusammengefasst werden:

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

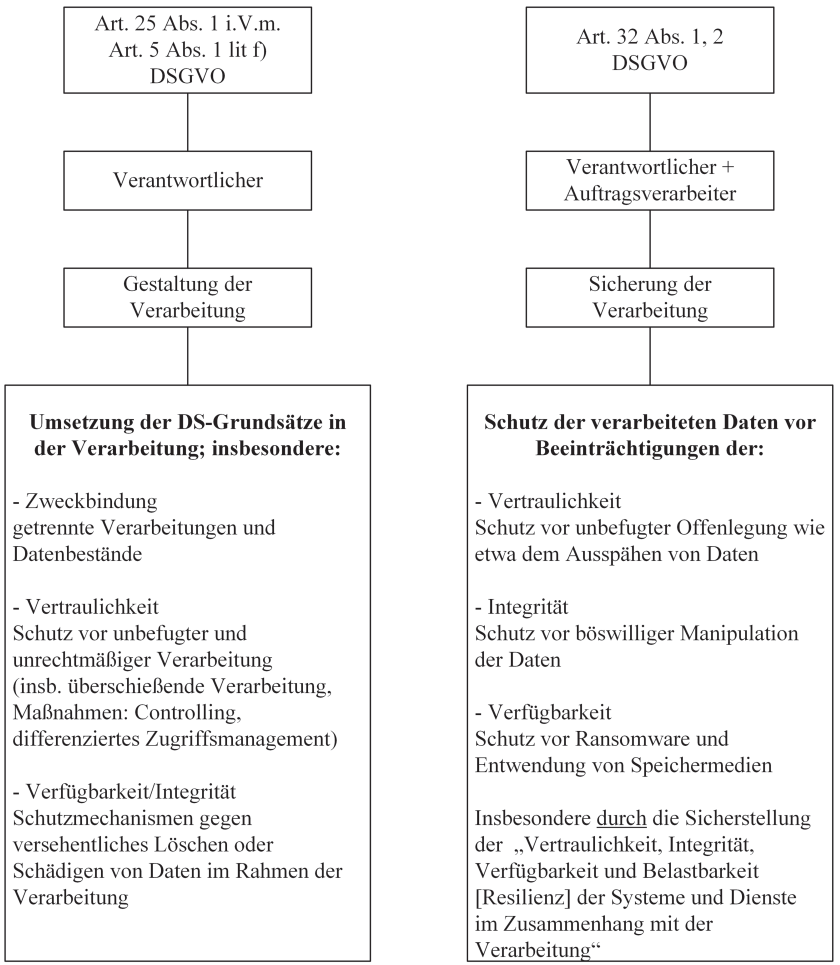

Abbildung 3: Abgrenzung Art. 25/32 DSGVO

B. Schutzgüter

In diesem Kapitel sollen die Schutzgüter der DSGVO ermittelt werden. Zunächst wird hierfür der Begriff des Schutzgutes, seine Bedeutung für das Daten- und IT-Sicherheitsrecht und damit auch für das Merkmal der Resilienz erläutert (I.). Im Anschluss werden spezifischer die Schutzgüter

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

der DSGVO herausgearbeitet (II.) Sodann wird unter III. erläutert, wie diese Schutzgüter in Art. 32 DSGVO eingebunden werden.

I. Terminologie und normative Bedeutung

Der Begriff des Schutzgutes wird nicht einheitlich verwendet; als Kompositum sagt er zumindest aus, dass ein bestimmtes Gut mit einem rechtlichen Schutz versehen wird.[193] Ähnlich wird auch der Begriff des „Rechtsgutes" etwa im Strafrecht definiert als ein „rechtlich geschütztes Interesse"[194] oder ein „rechtlich geschützter abstrakter Wert der Sozialordnung."[195] In dieser Untersuchung werden jene Rechtsgüter als *Schutzgüter* bezeichnet, die gerade durch das Daten- bzw. IT-Sicherheitsrecht geschützt werden sollen. In *andere Rechtsgüter* - insbesondere die berufliche bzw. unternehmerische Freiheit der Normadressaten - wird hingegen eingegriffen, um jene Schutzgüter zu sichern (dazu sogleich).

Zu den Schutzgütern können zunächst insbesondere Grundrechte mit ihren jeweiligen Schutzbereichen gehören.[196] Als Schutzgüter in diesem Sinne verpflichten die Grundrechte in ihrer objektiv-rechtlichen Dimension den Staat, die jeweiligen Grundrechtsträger:innen auch vor den von anderen Privatpersonen ausgehenden Bedrohungen ihrer Grundrechte zu schützen.[197] Die Erfüllung dieser sog. Schutzpflichten stellt zugleich eine Staatsaufgabe dar,[198] welche vom Staat in Gestalt des Gesetzgebers verlangt, diese Schutzpflichten durch entsprechende Gesetze auszugestalten.[199]

193 Siehe etwa *Calliess*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20a, Rn 71.

194 *Liszt*, ZStW 1886, 663 (672 f.).

195 *Jescheck/Weigend*, Lehrbuch des Strafrechts, S. 257 f.; Zur Übersicht mit weiteren Definitionsversuchen: *Engländer*, ZStW 2015, 616 (620).

196 Vgl. *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IX, 413 (436), Rn. 48, der generell den Schutzbereich eines Grundrechts als „Schutzgut" bezeichnet.

197 *Epping/Lenz/Leydecker*, Grundrechte, Rn. 23 [neu]; *Stinner*, Staatliche Schutzpflichten im Rahmen informationstechnischer Systeme, S. 52.

198 *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IV, 3, S. 37, Rn. 70; *Herzog*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IV, 81 (92), Rn. 26.

199 *Bethge*, in: Schmidt-Bleibtreu/Klein/Bethge, Bundesverfassungsgerichtsgesetz, 63. EL 2023, § 90, Rn. 108.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Genauer beschreibt das BVerfG[200] den inhaltlichen Rechtscharakter einer Schutzpflicht mit Blick auf das Grundrecht „Leben und körperliche Unversehrtheit" (Art. 2 Abs. 2 Satz 1 GG) dergestalt, dass die Schutzpflicht dem Staat gebiete „sich schützend und fördernd vor dieses Leben [oder jedes andere Grundrecht] zu stellen, das heißt vor allem, es auch vor rechtswidrigen Eingriffen vonseiten anderer zu bewahren." Entsprechend müsse sich die Rechtsordnung an diesem Gebot ausrichten.

Die Schutzpflicht wirke außerdem umso stärker, „je höher der Rang des in Frage stehenden Rechtsgutes innerhalb der Wertordnung des Grundgesetzes anzusetzen ist."[201] In dem hier vorliegenden Kontext des Daten- bzw. IT-Sicherheitsrechts kommt der Staat dieser Pflicht nach, indem er zur Sicherung der jeweiligen Schutzgüter Dritter (etwa betroffener Personen nach der DSGVO) den eigentlichen Normadressaten Vorgaben zur Gewährleistung der Daten- und IT-Sicherheit auferlegt.

Diese Vorgaben mit mehr oder minder konkreten Handlungspflichten stellen sich indes aus Sicht der Normadressaten, sofern es sich hierbei nicht um öffentlich-rechtliche Einrichtungen handelt, als staatliche Grundrechtseingriffe dar, sei es in ihre allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) oder ggf. auch ihre Berufsfreiheit (Art. 12 GG, Art. 15 GRC)[202] bzw. ihre unternehmerische Freiheit (Art. 16 GRC). Insofern wirken die Grundrechte hier in ihrer subjektiv-rechtlichen Abwehrdimension gegen den Staat („status negativus").[203] Der Grundrechtsträger und Normadressat kann insofern grundsätzlich vom Staat ein Unterlassen[204] dieses Eingriffs verlangen.

Damit der Eingriff gleichwohl gerechtfertigt ist, muss er insbesondere verhältnismäßig sein, d.h. zwischen den konkurrierenden Positionen muss -nach den Grundsätzen praktischer Konkordanz-[205] ein angemessenes Verhältnis hergestellt werden:

Dabei steht der durch die jeweiligen Pflichtennormen vorgegebene Aufwand (hier Art. 32 Abs. 1 DSGVO: Implementierungskosten, i.Ü. auch in

200 *BVerfG*, Urt. v. 25. 2. 1975 – 1 BvF 1 - 6/74, NJW 1975, 573 (575).
201 Wie zuvor.
202 *Poscher/Lassahn*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 133 (149), Rn. 46; *Wischmeyer*, Informationssicherheit, S. 123.
203 *Starck*, in: Mangoldt/Klein/Starck, Grundgesetz, 7. Auflage 2018, Art. 1, Rn. 183; *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IX, 413 (435 ff.), Rn. 47 ff.
204 Wie zuvor.
205 *BVerfG*, Beschluss v. 06.10.2009 – 2 BvR 693/09, NJW 2010, 220 (221 f.), Rn. 24; *BVerfG*, Beschluss v. 24.03.1998 – 1 BvR 131-96, NJW 1998, 2889 (2890); auch mit kritischen Stimmen siehe *Schladebach*, Der Staat 2014, 263 (266, 274 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

§ 30 RegE BSIG (sowie § 19 Abs. 4 TDDDG: „wirtschaftlich zumutbar") für den Adressaten als Eingriff dem hierdurch erreichten Zuwachs bei der Sicherung der Schutzgüter gegenüber. Nachfolgend werden die genannten Aspekte zur Verdeutlichung noch einmal grafisch dargestellt:

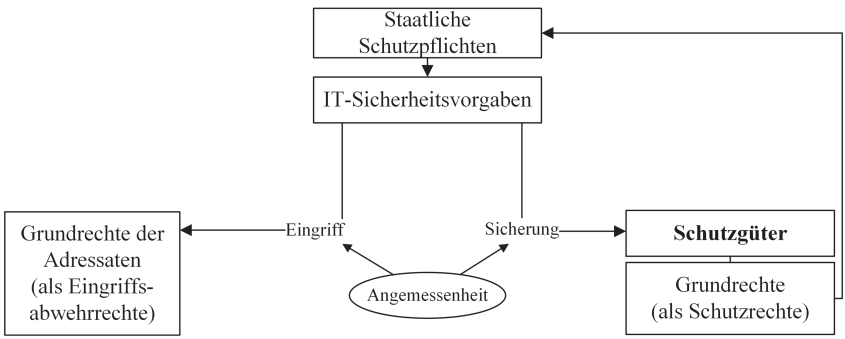

Abbildung 4: Abwägung zwischen Schutzgütern und Grundrechten der Adressaten

Der Gesetzgeber nimmt diese Abwägung zwischen den genannten Positionen dabei nicht unmittelbar und abschließend selbst vor. Vielmehr verfolgen die Pflichtennormen der Daten- und IT-Sicherheit einen sog. risikobasierten Ansatz[206], wonach es zunächst dem Adressaten obliegt, zu ermitteln, welchen Aufwand er betreiben muss, um den Risiken für die Schutzgüter angemessen zu begegnen. Genauer muss er insofern die Risiken bestimmen, d.h. analysieren mit welcher Wahrscheinlichkeit und in welchen Umfang (Folgenschwere) die Schutzgüter betroffen sein können. Anschließend muss er Maßnahmen ergreifen, die Eintrittswahrscheinlichkeit und/oder Folgenschwere angemessen reduzieren. Ob ihm das gelungen ist, ist entsprechend gerichtlich überprüfbar, so dass die Durchsetzung der Vorschriften gesichert ist und die Gesetze, die die o.g. Schutzpflicht ausfüllen insofern auch ihre Wirkung nicht verfehlen.

206 Für Art. 32 DSGVO: *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 22; *BSG*, Urt. v. 20.01.2021 – B 1 KR 15/20 R, BeckRS 2021, 13884, Rn. 79; für § 8a BSIG: *Bussche/Schelinski*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 7.1, Rn. 27.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zusammenfassend wird mit dem Begriff des Schutzgutes in dieser Untersuchung

> *jenes rechtlich zu schützende Interesse bezeichnet, zu dessen Zweck der Gesetzgeber den Normadressaten Pflichten zur Gewährleistung einer angemessenen Daten- oder IT-Sicherheit auferlegt.*

Es zeigt sich, dass Daten- und IT-Sicherheitsnormen nicht im luftleeren Raum stehen, sondern eingebettet sind in einen spezifischen Ausgleich von grundrechtlichen und anderen Positionen mit Verfassungsrang in den jeweils bereichsspezifischen Normen. Dabei ist das Schutzgut von besonderer Bedeutung, da sich hieran zeigt wofür, also zum Schutz welchen Gutes Daten- oder IT-Sicherheit gewährleistet werden soll. Dieser Hintergrund ist entscheidend um den Inhalt der Resilienz als spezifische Anforderung der Datensicherheit (und ggf. auch später der IT-Sicherheit) in ihrer Funktion und Reichweite begründen zu können.

Neben dem hier skizzierten Unterfall, dass die Schutzgüter Ausprägungen von Grundrechten mit entsprechenden staatlichen Schutzpflichten darstellen, können auch andere rechtliche Interessen Schutzgüter sein. Dieser Frage wird ausführlich im Kapitel zu den Schutzgütern im IT-Sicherheitsrecht nachgegangen, in dem insbesondere auch öffentliche Interessen als sog. *Gemeinschaftsrechtsgüter* von Bedeutung sind, etwa im Rahmen der Dienstleistungen aus dem Bereich der Daseinsvorsorge.[207]

II. Die Schutzgüter der DSGVO

Nach Art. 1 Abs. 2, EG 2 der DSGVO ist Zweck der „Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten" die Wahrung ihrer "Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten", mithin liegen die Schutzgüter der DSGVO[208] in eben diesem soeben beschriebenen Bereich des Individualgüterschutzes.

Im vorliegenden Kontext der Datensicherheit muss sich der Staat aufgrund der bestehenden objektiven Schutzpflichten schützend vor die Betroffenen stellen, so dass auf deren personenbezogene Daten nicht durch Dritte unerlaubt zugegriffen werden kann. Um dies zu erreichen, muss er

207 S. 222 ff.
208 Kritisch hierzu: *Veil*, NVwZ 2018, 686 (690 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

in die Grundrechte derjenigen eingreifen, die diese Daten (rechtmäßig) verarbeiten (Verantwortliche) und sie verpflichten, für eine angemessene Sicherheit der verarbeiteten Daten zu sorgen.

Dies gilt im Übrigen nicht nur für die Datensicherheit, sondern auch für den gesamten Datenschutz nach der DSGVO: Auch hier wird insbesondere in die unternehmerische Freiheit (Art. 16 GRC, EG 4 DSGVO) des Verantwortlichen eingegriffen, indem ihm nur innerhalb festgelegter Regeln gestattet wird, die personenbezogenen Daten z.B. seiner Kund:innen zu verarbeiten, um eben diese in ihren Grundrechten, insbesondere ihrem Datenschutzgrundrecht bzw. Recht auf informationelle Selbstbestimmung zu schützen. Es liegt mithin auch im Datenschutz stets ein Konflikt zwischen widerstreitenden Grundrechtspositionen vor, der durch den Staat in ausgleicher Weise geregelt werden muss.[209]

1. Sachliche Bestimmung der „Grundrechte und Grundfreiheiten"

Im Weiteren sollen diese als „Grundrechte und Grundfreiheiten" bezeichneten Schutzgüter näher untersucht werden. Die Bezeichnung „Rechte und Freiheiten" geht dabei auf Art 52 GRC, von dort wiederum auf die EMRK und die französische Rechtstradition zurück und bezeichnet -ohne qualitativen Unterschied zwischen Rechten und Freiheiten- die Individualgrundrechte.[210]

Inhaltlich umfasst dies nach Art. 2 Abs. 1 und EG 2 DSGVO deutlich mehr als nur das ausdrücklich genannte Datenschutzgrundrecht nach Art. 8 GRC und Art. 16 AEUV. Es kann hieraus geschlossen werden, dass dieses Grundrecht zwar das zentrale -„insbesondere"-, aber jedenfalls nicht

209 *Masing*, NJW 2012, 2305 (2306).

210 *Bieker/M. Hansen/Friedewald*, RDV 2016, 188 (188), *Schwerdtfeger*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage 2019, Art. 52, Rn. 25; *Becker*, in: Schwarze/Becker/Hatje/Schoo, EU-Kommentar, 4. Auflage 2019, Art. 52 GRC, Rn. 2; nach a.A. bezieht sich der Begriff der Grundfreiheiten nicht auf die GRC, sondern auf die Grundfreiheiten der europäischen Union (z.B. Warenverkehrsfreiheit): *Veil*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 24, Rn. 117; dagegen spricht aber systematisch, dass insbesondere die hier relevante Freiheit des Datenverkehrs als Voraussetzung für den europäischen Binnenmarkt, dem auch die anderen Grundfreiheiten in diesem Sinne dienen, gesondert in Art. 1 Abs. 3 DSGVO adressiert wird, siehe hierzu: *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 1, Rn. 41 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

das einzige Grundrecht darstellt, das durch die DSGVO geschützt werden soll. Vielmehr erkennt die DSGVO mit der weiten Formulierung der „Grundrechte und Grundfreiheiten" an, dass auch andere Grundrechte und Grundfreiheiten durch eine Verletzung des Datenschutzgrundrechts beeinträchtigt oder umgekehrt erst durch den Schutz desselben ermöglicht werden können.[211] Damit unterscheidet sich die DSGVO wie schon die DS-RL von dem BDSG a.F., dessen Gesetzeszweck in § 1 Abs. 1 BDSG a.F. sich auf den Schutz des allgemeinen Persönlichkeitsrechts sowie daraus insbesondere dem Recht auf informationelle Selbstbestimmung beschränkte.[212]

Andere in Betracht kommende Grundrechte sind insbesondere der Schutz des Privat- und Familienlebens, der Wohnung sowie der Kommunikation gemäß Art. 7 GRC,[213] die Gedanken-, Gewissens- und Religionsfreiheit und die Meinungs- (Art. 10 Abs. 1, 11 Abs. 1 GRC, Art. 4 Abs. 1, 5 Abs. 1 S. 1 Alt. 1 GG)[214] sowie die Informationsfreiheit (Art. 11 GRC, Art. 5 Abs. 1 S. 1 Alt. 2 GG).[215] Daneben ist auch das Diskriminierungsverbot geschützt, was insbesondere in dem Schutz besonderer Kategorien personenbezogener Daten in Art. 9 DSGVO zum Ausdruck kommt, die zumindest teilweise zugleich dem Diskriminierungsverbot unterliegende Merkmale nach Art. 21 Abs. 1 GRC darstellen.[216] Im Ergebnis beschreibt das Datenschutzrecht mit der Adressierung der genannten Schutzgüter „individuellen und unmittelbaren Grundrechtsschutz".[217] Im Rahmen der risikobezogenen Normen werden die Schutzgüter in der DSGVO geringfügig modifiziert, indem der Terminus abstrahierend auf „Rechte und Freiheiten natürlicher Personen"

211 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 1, Rn. 13 f.; *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 1, Rn. 36, 40; nach *Buchner* kann durch einen Datenschutzverstoß in Form der Offenlegung personenbezogener Daten etwa das Recht auf Nichtdiskriminierung verletzt werden; umgekehrt ermöglicht wirksamer Datenschutz erst eine freie Meinungsbildung und -äußerung; zu letzterem auch *Tinnefeld*, ZD 2015, 22 (25).

212 Vgl. § 1 Abs. 1 BDSG a.F., siehe ausführlicher: *Plath*, in: Plath, BDSG Kommentar 2013, § 1, Rn 8 f.

213 *Zerdick*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 1, Rn. 7.

214 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 1, Rn. 13.

215 *Ernst*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 1, Rn. 11.

216 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 1, Rn. 14.

217 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (399), Rn. 21.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ausgedehnt wird, was nach dem Wortlaut auch einfachgesetzliche Rechtspositionen einschließen könnte.[218]

2. Kreis der geschützten „natürliche Personen"

Fraglich ist weiterhin die Reichweite des Begriffs „natürliche Personen" und damit der Kreis der geschützten Grundrechtsträger. Hier ist bemerkenswert, dass auch Art. 32, EG 75 diesen in Art. 1 Abs. 2 DSGVO niedergelegten Terminus verwenden und nicht etwa den der „betroffenen Person", wie er in Art. 4 Nr. 1 DSGVO legaldefiniert wird. Es stellt sich daher die Frage, ob nur die Risiken für die jeweils von den Informationen betroffene Person oder für jede natürliche Person erfasst werden, die ggf. auch nur mittelbar von der Datenverarbeitung betroffen ist.

Der Wortlaut des Art. 32 DSGVO gibt hierauf zunächst keine klare Antwort. Blickt man in EG 75 DSGVO in den ersten Halbsatz, so spricht zunächst viel für eine weite Auslegung, denn dort heißt es die Risken für Rechte und Freiheiten natürlicher Person können aus einer „Verarbeitung personenbezogener Daten" und nicht etwa „Verarbeitung ihrer/der sie betreffenden personenbezogenen Daten" hervorgehen. Dieses Ergebnis wird durch die weiteren Ausführungen in EG 75 gestützt, in denen es als *weitere Schadenskategorie* heißt, dass „die betroffenen Personen" um ihre Rechte und Freiheiten gebracht werden. Dies spricht dafür, dass der Gesetzgeber sich der unterschiedlichen Bedeutung der so bezeichneten Personengruppen durchaus bewusst war und die erfassten Schutzgüter auch in personaler Hinsicht weit ausgestaltet hat.

Damit sind auch mittelbare Auswirkungen auf Dritte erfasst.[219] Denkbar sind z.B. Auswirkungen in engen sozialen Beziehungen wie Familie und Freundeskreise, in denen etwa die unzulässige Veröffentlichung von per-

218 *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 24, Rn. 31; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 27.

219 Vgl. *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 29; häufig wird in der Kommentarliteratur hingegen ohne Erläuterung nur auf betroffene Personen abgestellt, so etwa: *Hladjk*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 32, Rn. 4; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 27; teilweise wird auch EG 76 ins Feld geführt (*Kipker*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 24 DSGVO, Rn. 19) der tatsächlich von den Risiken für betroffene Personen spricht. Allerdings bleibt es dann zumindest begründungsbedürftig, warum dieser EG den eindeutigen Wortlaut in Art. 24, 25 und 32 DSGVO überlagern sollte.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sönlichen Informationen des einen auch die freie Persönlichkeitsentfaltung oder andere Grundrechte des oder der anderen beeinträchtigt.

III. Bestimmung in Art. 32 DSGVO

Nach der amtlichen Überschrift verpflichtet Art. 32 DSGVO den Verantwortlichen zwar wie schon Art. 17 der DS-RL dazu, die *„Sicherheit der Verarbeitung"* zu gewährleisten. Dies wird in Absatz 1 näher konkretisiert, nach dem ein „dem Risiko angemessenes Schutzniveau" zu gewährleisten ist. Dieses Risiko bezieht sich wie auch aus EG 75 ersichtlich auf die *Rechte und Freiheiten natürlicher Personen* und wird dort auch mit verschiedenen Schadens- und Risikokategorien näher umschrieben. Das Risiko muss dabei gerade aus „einer Verarbeitung personenbezogener Daten" hervorgehen.

Fraglich ist insoweit, ob nun nur die „Sicherheit der Verarbeitung" gewährleistet werden muss oder aber ob die „Rechte und Freiheiten natürlicher Personen" unmittelbar geschützt werden müssen.

Nach dem Wortlaut des Art. 32 Abs. 1 kann zunächst abgeleitet werden, dass die „Sicherheit der Verarbeitung" zwar den Handlungsauftrag umschreibt, nicht aber das eigentliche Schutzgut darstellt. Die Schutzgüter bestehen demnach in den „Rechten und Freiheiten natürlicher Personen" bei der Verarbeitung, denn der Kernzweck der Norm ist es, das Risiko für ebendiese zu reduzieren. Dies umfasst wie beschrieben sowohl deren Grundrechte als auch deren einfach-rechtliche Rechtsposition, die durch eine fehlende Datensicherheit beeinträchtigt werden können.

Auf der anderen Seite spricht die Überschrift dafür, dass aus Sicht des Verarbeiters die „sichere Verarbeitung" an sich und nicht unmittelbar die Unversehrtheit der Schutzgüter gewährleistet werden muss. Dafür streitet auch, dass das Risiko für die Rechte und Freiheiten natürlicher Personen im Rahmen der enumerativen Aufzählung nur ein Belang unter mehreren darstellt.

In Gegenüberstellung dieser Alternativen fällt auf, dass die erste Alternative zu einer originären Schutzverantwortung für die Rechte und Freiheiten natürlicher Personen führt, während die zweite Alternative mit dem beschränkten Blick auf die Sicherheit der Verarbeitung nur einer mittelbaren Verantwortung entspricht. Angesichts dessen, dass das Datenschutzrecht aber gemäß Art. 1 Abs. 2 DSGVO ausdrücklich auch die Grundrechte und insbesondere das Recht auf Schutz personenbezogener Daten schützen

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

will, spricht mehr dafür es hier nicht bei einer mittelbaren Verantwortung zu belassen, sondern den Verantwortlichen (und den Auftragsverarbeiter) unmittelbar zu verpflichten, die Grundrechte und einfachrechtlichen Positionen der natürlichen Personen risikoadäquat schützen.[220]

C. Auslegung der Resilienz

Im nun folgenden Abschnitt soll die Bedeutung der Resilienz von Systemen und Diensten zur Gewährleistung der Datensicherheit und damit zur Sicherung der zuvor beschriebenen Schutzgüter durch Auslegung ermittelt werden. Die Einführung der Resilienz (en: resilience) als *explizite Anforderung in der Datensicherheit* neben den bisherigen Schutzzielen (Verfügbarkeit, Vertraulichkeit, Integrität) stellt dabei ein Novum in der europäischen Gesetzgebung dar. Dementsprechend zeigt sich die inhaltliche Rezeption in der fachrechtlichen Literatur bislang sehr divers und mitunter eher oberflächlich ausgeprägt.

Nachdem zunächst einige Vorbegriffe des Art. 32 Abs. 1 lit b) DSGVO ausgelegt und erläutert werden (I.) folgt die eigentliche Auslegung des Resilienzbegriffs nach den vier juristischen Methoden der Auslegung.[221] Zunächst wird der *Wortlaut* Resilienz untersucht (II.). Als nächstes wird im Rahmen *der systematischen Auslegung* untersucht, wie sich die Resilienz zu dem Risikobegriff und der Risikomethodik des Art. 32 DSGVO sowie in die Regelungstechnik neben den anderen Schutzzielen positioniert. (III). In einem dritten Schritt wird in der *historischen und teleologischen Auslegung* untersucht, wie sich die Datensicherheitsvorgaben entwickelt haben und welche neuen Realweltphänomene aufgetreten sind, auf die der Gesetzgeber ggf. auch mit der Einführung der Resilienz reagieren wollte (IV.).

I. Vorbegriffe

Der zentrale Punkt der Auslegung im Rahmen dieser Untersuchung ist nur der Rechtsbegriff der Resilienz selbst. Somit sind, bevor zur Wortlautauslegung ebendieses Begriffs geschritten werden kann, zunächst noch einige Feststellungen zum übrigen Rechtssatz (Art. 32 Abs. 1 lit b) DSGVO) zu

220 So auch: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 28 ff.; *Bieker*, DuD 2018, 27 (27).

221 *Savigny*, System des heutigen Römischen Rechts, Band 1, S. 213 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

treffen. Blendet man zunächst die bisherigen Schutzziele aus (zu diesen ausführlich in der systematischen Auslegung unter II.2.) und nimmt den Normauftrag des 1. Hs. auf, lautet der entsprechende Auszug des Rechtssatzes:

> „diese *Maßnahmen [zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus]* schließen gegebenenfalls unter anderem Folgendes ein: […] b) die Fähigkeit, die *Belastbarkeit [Resilienz]* der *Systeme und Dienste* im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;"

Um die nachfolgende Auslegung des schillernden Begriffs Resilienz zumindest grob einzugrenzen, ist deshalb zunächst zu klären, was unter den Begriffen „Maßnahmen", „Systeme" und „Dienste" zu verstehen ist, auf die die Resilienz hier bezogen wird. Darüber hinaus dienen diese Maßnahmen der Gewährleistung der „Sicherheit der Verarbeitung", so dass dieser Begriff zuerst beschrieben werden soll.

1. Datensicherheit / Sicherheit der Verarbeitung

Die Sicherheit der Verarbeitung ergibt sich als Erfordernis zunächst aus der Überschrift des Art. 32 DSGVO. Auch soll durch die Maßnahmen ein „*dem Risiko angemessenes Schutzniveau*" erreicht werden. In anderen Sprachfassungen[222] wird hier jedoch einheitlich von „Sicherheit" und „Sicherheitsniveau" gesprochen, so dass auch der deutsche Begriff des Schutzniveaus in diesem Sinne ausgelegt werden sollte. Normzweck unter der Überschrift „Sicherheit der Verarbeitung" ist es mithin ein „dem Risiko angemessenes Sicherheitsniveau" zu gewährleisten.[223]

Die Sicherheit der Verarbeitung kann bejaht werden, wenn sie die Sicherheit der personenbezogenen Daten (*Datensicherheit*) gewährleistet,[224] was sich insbesondere auch systematisch aus den Meldepflichten (Art. 33

222 Englisch: „Security of Processing/level of security"; Französisch: „Sécurité du traitement/niveau de sécurité"; spanisch „Seguridad del tratamiento/nivel de seguridad"; italienisch: „Sicurezza del trattamento, livello di sicurezza;"; zur Auslegung bei unterschiedlichen Sprachfassungen sogleich: S. 121 f.

223 Ebenso: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 30.

224 *Seufert*, ZD 2023, 256 (257); *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 1b; als "Daten- und Systemsicherheit", *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 1.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Abs. 1, 34 Abs. 1 DSGVO: „Verletzung des Schutzes personenbezogener Daten") ergibt. Die Datensicherheit lässt sich aus Art. 32 Abs. 2 DSGVO und im Umkehrschluss aus Art. 4 Nr. 12 DSGVO zunächst definieren als die Verfügbarkeit, Vertraulichkeit und Integrität personenbezogener Daten.[225] Dies stellt das Herzstück der Datensicherheit dar, an dem sich am Ende auch stets der „Verletzungserfolg" realisiert.[226]

Aber auch die Anforderungen an die Systeme und Dienste, namentlich die Resilienz sind wichtige Bestandteile einer umfassenden Datensicherheit.[227] Sie wirken zunächst im Vorfeld zum Schutz bestehender personenbezogener Daten, da eine Beeinträchtigung der Sicherheit der Systeme und Dienste häufig eine Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) zur Folge haben kann.[228] Außerdem wirken sie auch dahingehend ergänzend, dass durch die Verarbeitung kein manipuliertes Personenwissen (und damit wiederrum personenbezogenen Daten) erzeugt wird. Datensicherheit kann somit umfassend definiert werden als:

> *die angemessene Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sowie der Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz der für die Verarbeitung genutzten Systeme und Dienste.*

Zur Schutzrichtung wurde bereits erläutert, dass Art. 32 DSGVO auf alle unerwünschten Ereignisse abzielt, d.h. vorsätzliche, fahrlässige und zufällige Ereignisse, die sowohl von internen als auch von externen Quellen ausgelöst werden können.[229]

2. Maßnahmen

Die Sicherheit der Verarbeitung wird durch die Vornahme von Maßnahmen erreicht. Als Maßnahmen werden alle Handlungen definiert, die ge-

225 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (403), Rn. 30.
226 Wie zuvor.
227 So mit Blick auf die „Sicherung der Hard- und Software" auch schon *Gola/Klug/Körffer*, in: Gola/Schomerus, Bundesdatenschutzgesetz [a.F.], 12. Auflage 2015, § 9, Rn. 1.
228 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (403), Rn. 30.
229 Soweit sie in Abgrenzung zu Art 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO nicht bereits durch die Gestaltung der Verarbeitung verhindert werden können, siehe oben, S. 98 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

eignet sind auf den entsprechenden Schutzzweck, im Kontext des Art. 32 DSGVO, mithin die „Gewährleistung eines risikoangemessenen Schutzniveaus", hinzuwirken.[230] Dabei unterscheidet der Gesetzeswortlaut zwischen technischen und organisatorischen Maßnahmen.

Die *technischen Maßnahmen* zeichnen sich dadurch aus, dass sie unmittelbar in bzw. an der verwendeten Technik, also der verwendeten Hard- und Software,[231] implementiert werden: Hierzu gehören neben informationstechnischen Maßnahmen wie der Verschlüsselung und der Verwendung sicherer Passwörter auch bauliche Maßnahmen, die den Zutritt Unbefugter z.B. zu Serverräumen ausschließen.[232]

Organisatorische Maßnahmen betreffen hingegen die Prozesse außerhalb der Technik und setzen somit insbesondere am Personal an.[233] Beispiele für organisatorische Maßnahmen sind etwa das Vier-Augen-Prinzip, Mitarbeiterschulungen und Protokollierungsvorgaben.

Da viele organisatorische Maßnahmen wie etwa das Vier-Augen-Prinzip eine technische Entsprechung haben müssen, also das etwa eine Aktion erst von den jeweiligen zwei Benutzer-Accounts freigegeben werden muss, wird die Möglichkeit einer klaren Unterscheidung zwischen technischen und organisatorischen Maßnahmen mitunter bezweifelt.[234] Rechtlich besteht insoweit auch keine Notwendigkeit zur Unterscheidung;[235] für den Normanwender kann jedenfalls festgehalten werden, dass sich der Handlungsauftrag nicht nur auf technische Maßnahmen beschränkt, sondern durch organisatorische Maßnahmen auch das Personal mit in den Blick genommen werden muss.

---

230 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 20a.

231 *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 37; *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn 24.

232 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 21; nur informationstechnische Maßnahmen nennend: *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn. 24; *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (552).

233 *Freund*, in: Schuster/Grützmacher, IT-Recht 2020, Art. 32 DSGVO, Rn. 16.

234 *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn. 24 f.; *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 24, Rn. 17; *Kipker*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 24 DSGVO, Rn. 16.

235 Wie zuvor.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Systeme

Im nachfolgenden Abschnitt soll der Begriff der „Systeme" im Kontext des Art. 32 DSGVO beleuchtet werden. Nach der sogleich folgenden Darstellung der konsensfähigen Erfassung informationstechnischer Systeme wird auf zwei weitere Fragestellungen eingegangen: Zum einen ob Art. 32 DSGVO an dieser Stelle auch die jeweils enthaltenen Daten in den Systembegriff mit einschließt (a.) und zum anderen ob auch die jeweiligen Personen, die mit dem informationstechnischen System interagieren, im Sinne eines soziotechnischen Verständnisses von dem Systembegriff erfasst werden müssen (b.).

In der Literatur zu Art. 32 DSGVO wird zunächst ein technisches Systemverständnis zugrunde gelegt. Der Begriff des Systems sei insofern weit auszulegen und umfasse somit die Computersysteme wie Server, Arbeitsplatzcomputer sowie die verwendete Netzwerktechnik jeweils sowohl mit ihren *Hard- als auch ihren Softwarekomponenten*.[236] Somit wird deutlich, dass sich der Begriff des Systems in Art. 32 Abs. 1 lit b) DSGVO jedenfalls auf die verwendete Informationstechnik[237] bezieht.[238]

In der Rechtsinformatik definiert *Steinmüller* ein System sehr abstrakt als eine Menge von Elementen und den Relationen zwischen ihnen.[239] Diese Grunddefinition lässt sich dahingehend für die Datensicherheit konkretisieren und erweitern, dass ein System mit seinen Komponenten (Elementen) und deren Relationen so konzipiert ist, dass es einen spezifischen

236 *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 51; *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 43; *Piltz*, in: Gola/Heckmann, DSGVO, 3. Auflage 2022, Art. 32, Rn. 30; *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn 22.

237 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 43 „praktisch jede Form der Informationstechnik". Daneben sind auch Systeme zur „papiergebundenen Verarbeitung" erfasst: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 57.

238 Es sei an dieser Stelle darauf hingewiesen, dass die Begriffe Systeme und Komponenten skalierbar sind. So kann etwa ein Netzwerk von mehreren Computern auch als ein „System" definiert werden, in dem dann diese Computer wiederrum „Komponenten" bilden. Gerade um eine Technologieoffenheit des Rechts sicherzustellen, erscheint es auch sinnvoll eine Entwicklung der Begriffe in diesem Sinne zuzulassen. Teilweise wird auch von einem „System von Systemen" gesprochen, wobei letztere dann auch als Subsysteme bezeichnet werden können: *Steinmüller et al.,* JA-Sonderheft 6: ADV und Recht, 1976, S. 10.

239 *Steinmüller et al.,* JA-Sonderheft 6: ADV und Recht, 1976, S. 9.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Dienst erbringt (dazu sogleich).[240] Außerdem lässt sich ein System durch sog. *Systemgrenzen* beschreiben, die das System von der Umwelt abgrenzen und insbesondere für die Bestimmung der Reichweite der Sicherheitsgewähr eine entscheidende Rolle spielen.[241] Zur Verdeutlichung nachfolgende Grafik:[242]

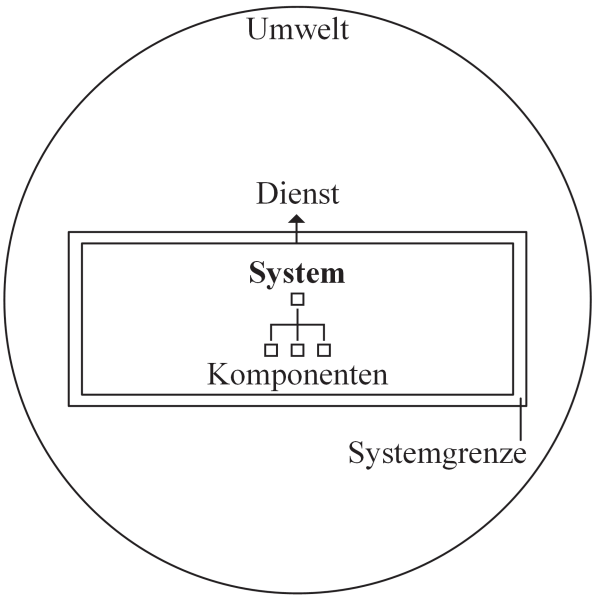

Abbildung 5: IT-System

a. Erfassung personenbezogener Daten

Als Komponenten eines Systems kommen wie o.g. insbesondere die verwendete Hard- und Software in Betracht. Fraglich ist hingegen, ob der Begriff des Systems als weitere Komponente auch die in dem System enthaltenen personenbezogenen Daten umfasst.

240 So in der technischen Literatur auch: *B. Randell/P. Lee/Treleaven*, ACM CSUR 1978, 123 (125).

241 *Aebi*, Praxishandbuch Sicherer IT-Betrieb, S. 5; *Steinmüller et al.,* JA-Sonderheft 6: ADV und Recht, 1976, S. 10.

242 Siehe zu den entsprechenden Definitionen auch *Avizienis et al.*, IEEE TDSC 2004, 11 (11 f.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Entscheidend ist diese Frage insbesondere für die Auslegung von Art. 32 Abs. 1 lit b) DSGVO. Werden die personenbezogenen Daten als Systembestandteil definiert, sind die dort genannten Schutzziele auch hier auf die personenbezogenen Daten zu beziehen.

Dies wird teilweise mit der Begründung angenommen, dass insbesondere das Schutzziel der Vertraulichkeit nicht auf die Systeme mit ihrem Hardware-Design oder ihrem Software-Code zu beziehen sei, sondern nur die Vertraulichkeit der Daten selbst garantiert werden solle.[243]

Dagegen sprechen jedoch eine Reihe von Gründen: Zuvörderst ist hier der *eindeutige Wortlaut* zu nennen, mit dem die Schutzziele in Art. 32 Abs. 1 lit b) DSGVO auf Systeme und Dienste bezogen werden. Dagegen werden die Schutzziele an anderer Stelle, nämlich in Art. 32 Abs. 1 lit a) und c), Abs. 2 DSGVO explizit oder zumindest sinngemäß auf personenbezogene Daten bezogen.[244] Da somit *alle Schutzziele bereits an anderer Stelle in Art. 32 auf personenbezogene Daten* bezogen werden, entsteht durch die Nichtfassung der personenbezogenen Daten unter den Systembegriff auch keine Schutzlücke. Drittens verkennt die Gegenansicht, dass die explizite Adressierung der Sicherheit von Systemen und Diensten teleologisch wie bereits beschrieben *einen Vorfeldschutz bzw. eine Ergänzung* beschreibt, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Wortlaut und auch Telos sprechen insofern an dieser Stelle für eine spezifische Adressierung der Systeme ohne die darin enthaltenen personenbezogenen Daten.

Es spricht somit insgesamt viel dafür, dass der Gesetzgeber bei der Bezugnahme der Schutzziele auf die Schutzobjekte der Systeme und Dienste anstelle der Daten absichtsvoll handelte und ein eigenständiges Schutzerfordernis normiert hat.[245] Im Ergebnis fallen die personenbezogenen Daten somit nicht unter den Systembegriff des Art. 32 Abs. 1 lit b) DSGVO.

---

243 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 38.

244 Vgl. *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 23, Fn. 73.

245 Andernfalls würden sich Art. 32 Abs. 1 lit b einerseits sowie Art. 32 Abs. 1 lit c, Abs. 2 in ihrem Schutzgehalt überschneiden. In diesem Sinne die Schutzziele eigenständig für Systeme und Dienste auslegend auch: *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 22 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

b. Soziotechnisches Systemverständnis

Klärungsbedürftig ist weiterhin, ob auch die *Personen, die die informationstechnischen Systeme bedienen*, also etwa die Mitarbeitenden des Verantwortlichen im Sinne eines soziotechnischen Systemverständnisses in den Systembegriff einzubeziehen sind; womit sich in der Folge auch die Resilienz auf ein soziotechnisches System beziehen würde.

Für ein soziotechnisches Systemverständnis spricht zunächst, dass die informationstechnischen Systeme ohne die bedienenden natürlichen Personen regelmäßig unvollständig betrachtet werden. Die Mitarbeitenden sind oft eng in die Verarbeitung eingebunden,[246] indem sie etwa einen Verarbeitungsvorgang auslösen, gestalten oder beenden. Sie geben neue Informationen als Daten in das System ein, legen fest ob und wie diese verarbeitet werden sollen und nutzen die entsprechenden Ergebnisse.[247] Dies greift Art. 32 Abs. 4 DSGVO auch auf, indem er den Verantwortlichen verpflichtet sicherzustellen, dass seine Mitarbeitenden die personenbezogenen Daten nur auf seine Weisung hin verarbeiten.

Aufgrund dieser zentralen Stellung sind die Mitarbeitenden oft auch für die Gewährleistung der Sicherheit der Verarbeitung ein wesentlicher Bestandteil. Damit sie die insoweit an sie gestellten Anforderungen erfüllen können, sind insbesondere organisatorische Maßnahmen wie Schulungen im Umgang mit den Sicherheitsmaßnahmen (Nutzbarkeit), verbindliche Regelungen (Policies) und entsprechende auf Akzeptanz ausgerichtete Sensibilisierungen und Aufklärungsmaßnahmen erforderlich.[248] Außerdem müssen die Mitarbeitenden auch bei der Gestaltung der technischen Maßnahmen berücksichtigt werden, da nur eine hohe Nutzbarkeit der Maßnahmen wie etwa bei Authentifizierungsmechanismen einen tatsächlichen Sicherheitsgewinn verspricht. Die o.g. organisatorischen Maßnahmen lassen sich somit auch nicht isoliert von den technischen Maßnahmen betrachten, da sie nur gemeinsam gedacht eine entsprechende Schutzwirkung entfalten können.

246 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 37.

247 So auch bereits *Steinmüller:* Menschen sind als „Bedienungspersonal, Datenlieferanten und Benutzer" Teile (Elemente) eines Informationssystems, *Steinmüller*, Leviathan 1975, 508 (521).

248 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 37; *Eckert*, IT-Sicherheit, S. 3 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Spezifisch im Telos der Datensicherheit ist das Ziel eines umfassenden Schutzes der Daten und der daraus ableitbaren persönlichen Informationen hervorzuheben. Hierfür sind auch die Mitarbeitenden und die zugehörigen organisatorische Maßnahmen essenziell. So hilft es für diesen Schutz wenig, wenn die personenbezogenen Daten zwar von dem informationstechnischen System verschlüsselt werden, die Mitarbeitenden mit dem zugehörigen Schlüssel aber nicht sorgsam umgehen oder die persönlichen Informationen in nicht-technischer Weise, etwa mündlich, offenlegen.

Insgesamt sprechen somit einige Argumente dafür, von einem soziotechnischen Systemverständnis auszugehen und die Mitarbeitenden entsprechend mit einzubeziehen.[249]

Allerdings sprechen systematische Gründe gegen ein solches soziotechnisches Systemverständnis. Zunächst ist hier zu beachten, dass die technischen Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität auf das System bezogen werden. Insbesondere die Sicherstellung der Integrität und der Vertraulichkeit der Mitarbeitenden zu verlangen, erscheint nicht sachgerecht. Bei den Schutzzielen handelt es sich um in der Informationstechnik tradierte, technische Eigenschaften.[250] Eine Übertragung auf die soziale Ebene der Mitarbeitenden erscheint daher unpassend. Auch lässt sich argumentieren, dass die Einbeziehung der Mitarbeitenden in das Datensicherheitskonzept des Art. 32 Abs. 1 DSGVO zumindest nicht als Automatismus erfordert, dass diese auch unter den Begriff des Systems subsumiert werden, sondern bereits über das Erfordernis der Vornahme „organisatorischer Maßnahmen" abgedeckt ist.

Insgesamt kann die Frage, ob der Systembegriff in der DSGVO technisch oder soziotechnisch zu verstehen ist, an dieser Stelle noch nicht abschließend beantwortet werden. Für die Resilienz als umfassendes Prinzip könnte ein soziotechnisches Verständnis geboten sein, während die klassischen Schutzziele nur auf ein technisches System angewendet werden können. Mangels einer eindeutigen, abstrakten Festlegung müssen somit beide Aspekte im Verlauf der Untersuchung noch näher beleuchtet werden.[251]

---

249 Für ein Informationssystem in der Informationssicherheit ebenso: *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (547).

250 *Samonas/Coss*, JISSec, Vol. 10 (2014), Heft 3, 21 (23 ff.); hierzu später ausführlich ab S. 187 ff.

251 Siehe im Ergebnis S. 201.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. Dienste

Als weiteres Schutzobjekt neben den Systemen nennt Art. 32 Abs. 1 lit b) DSGVO die Dienste. Fraglich ist, wie der Begriff des Dienstes im Kontext der „Sicherheit der Verarbeitung" auszulegen ist. Im IT-Recht kann der Dienst technisch, ökonomisch als auch rechtlich verstanden werden.

a. Ökonomische Betrachtung

Zunächst kommt dem Dienstbegriff in einer *ökonomischen Betrachtung* Bedeutung zu: So beschreibt der Dienst der Informationsgesellschaft (Art. 4 Nr. 25 DSGVO mit Verweis auf Art. 1 Nr. 1 lit b) RL 2015/1535) „eine Dienstleistung der Informationsgesellschaft, d.h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung." Charakterisierend für den Dienstbegriff ist somit insbesondere das regelmäßig entgeltliche Leistungsangebot an einen Dritten.

Die Anwendung der ökonomischen Betrachtung auf den Dienst in Art. 32 Abs. 1 lit b) DSGVO ist indes zweifelhaft. Die Datensicherheitsvorgaben des Art. 32 DSGVO dienen anders als die Vorgaben des IT-Sicherheitsrechts nicht der gesicherten Erbringung einer ökonomisch relevanten Dienstleistung wie etwa der Bereitstellung einer Online-Suchmaschine oder eines Online-Marktplatzes. Vielmehr liegen wie zuvor beschrieben die Schutzgüter in den Rechten und Freiheiten natürlicher Personen, welche durch die Verarbeitung personenbezogener Daten gefährdet sein können.

b. Rechtliche Betrachtung

Bei einer *rechtlichen Betrachtung* hat der Dienst eine Gruppierungs- und Verantwortungszuweisungsfunktion, etwa im IT-Sicherheitsrecht, indem an den Dienst anknüpfend der Anbieter desselben alle hierfür notwendigen Systeme in seinen Anwendungsbereich einzubeziehen hat.[252]

In der DSGVO erscheint die rechtliche Betrachtungsweise dagegen nicht angezeigt, da die Verantwortung durch die Entscheidungsbefugnis über die Verarbeitung personenbezogener Daten begründet wird (Art. 4 Nr. 7

252 So etwa in Art. 21 Abs. 1 NIS2-RL und § 165 Abs. 1 TKG.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

DSGVO) und nicht durch die Erbringung eines spezifischen Dienstes wie etwa den zuvor genannten.

c. Technische Betrachtung

Schließlich lässt sich bei einer *technischen Betrachtung* festhalten, dass Dienste von Systemen bereitgestellt bzw. erbracht werden.[253] In dem Dienst drückt sich das Verhalten des Systems nach außen, mithin an seine Umwelt aus; er wird wie bereits beschrieben[254] über eine Schnittstelle an der jeweiligen Systemgrenze an eine(n) oder mehrere Nutzer:innen erbracht.[255] Der Dienst stellt somit die spezifische Funktionalität eines Systems dar.

Im Kontext der Verarbeitung personenbezogener Daten kann der Dienst als die spezifizierte Funktionalität des Systems insbesondere auf die Verarbeitungsergebnisse personenbezogener Daten bezogen werden.[256] Somit kann hierunter vor allem das Generieren von *Personenwissen* aus personenbezogenen Einzelinformationen nach dem bereits dargestellten DIW-Modell gefasst werden. Praktisch schließt dies insbesondere die Bewertung persönlicher Aspekte im Rahmen des Profilings mit ein (Art. 4 Nr. 4 DSGVO). Insofern erscheint für den Dienstbegriff der DSGVO die technische Betrachtung am geeignetsten.

Zu beachten ist dabei auch, dass der Dienstbegriff durch den jeweiligen Zweck der Verarbeitung determiniert wird, d.h. ein Dienst darf nur darin bestehen, was vom jeweiligen Zweck (Art. 5 Abs. 1 lit. b) DSGVO) erfasst ist. Liegt der Zweck z.B. in der Reichweitenmessung eines Webangebots, muss sich der zugehörige technische Dienst des jeweiligen Systems auch in dieser Funktionalität erschöpfen.

---

253 *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 43.

254 Siehe oben, S. 115.

255 *Avizienis et al.*, IEEE TDSC 2004, 11 (11 ff.), Nutzer:in muss demnach auch nicht zwingend eine natürliche Person, sondern kann auch ein anderes System sein.

256 Außerdem kann ein technischer Dienst (ohne im hier dargestellten Sinn an der Verarbeitung mitzuwirken) die Zugriffs- (für den Auskunftsanspruch, Art. 15 DSGVO), Änderungs- und Löschungsfunktionen (Art. 16, 17 DSGVO) an den personenbezogenen Daten bereitstellen, die dem Betroffenen zur Wahrnehmung seiner Rechte zustehen; Vgl. *Kramer/Meints*, in: Auernhammer, DSGVO BDSG, 7. Auflage 2020, Art. 32, Rn. 43; *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (214).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Diese technische Unterscheidung zwischen dem System an sich und der von ihm bereitgestellten, spezifizierten Funktionalität (Dienst) ist, wie im weiteren Verlauf gezeigt werden wird, für die Resilienz von nicht zu unterschätzender Bedeutung. Ob die Unterscheidung sich hingegen auch auf die Schutzziele dergestalt auswirkt, dass sich diese mit Blick auf Systeme oder Dienste sinnvoll voneinander abgrenzen lassen, ist zweifelhaft. Einzelheiten dazu werden ebenfalls an späterer Stelle erläutert, wenn die Schutzziele der Resilienz systematisch gegenübergestellt werden.

II. Auslegung nach dem Wortlaut

Nach Bestimmung der soeben dargestellten Vorbegriffe folgt nun die Auslegung des Begriffs der Resilienz. Ausgangspunkt einer jeden Auslegung ist zunächst der Wortlaut des Gesetzes.[257] Dieser Umstand ist zu trennen von der Auslegungsmethodik „nach dem Wortlaut" (auch grammatische Auslegung)[258], die den allgemeinen oder auch den spezifischen Sprachgebrauch der adressierten Fachdomäne ermittelt.[259] Im ersten Schritt (1) soll daher unmittelbar auf den deutschen Wortlaut „Belastbarkeit" eingegangen und diese Begrifflichkeit mit den anderen Sprachfassungen verglichen werden. Im zweiten Abschnitt dieses Kapitels wird sodann das allgemeine sowie das domänenspezifische Verständnis der „Resilienz" untersucht. Daran schließen sich die Synthese der domänenspezifischen Verständnisse (3.) und das Fazit für die Wortlautauslegung (4.) an.

1. „Belastbarkeit" oder Resilienz

Im europäischen Recht kommt den unterschiedlichen Sprachfassungen im Rahmen der Wortlautauslegung eine hohe Bedeutung zu.[260] Nach dem EuGH sind „die *verschiedenen sprachlichen Fassungen gleichermaßen verbindlich* […]; die Auslegung einer gemeinschaftsrechtlichen Vorschrift erfordert somit einen Vergleich ihrer sprachlichen Fassungen."[261]

257 *Herdegen*, Europarecht, S. 226, Rn. 92; *EuGH*, Urt. v. 17.04.2018 – C-414/16, NZA 2018, 569 (570), Rn. 44. *Honsell*, ZfPW 2016, 106 (120).
258 *Honsell*, ZfPW 2016, 106 (120 f.).
259 *Bydlinski*, Grundzüge der juristischen Methodenlehre, S. 27.
260 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (293 f.), Rn. 14.
261 *EuGH*, Urt. v. 06.10.1982 – Rs 283/81, NJW 1983, 1257 (1258).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Wie bereits angedeutet ist in der deutschen Fassung der DSGVO von „Resilienz" zunächst keine Rede. Vielmehr findet sich hier das Merkmal der „Belastbarkeit". Belastbarkeit ist nach dem *Duden* die Fähigkeit, eine Materialbeanspruchung auszuhalten, also z.B. die Belastbarkeit eines Drahtseils, aber auch körperliche und seelische Inanspruchnahme auszuhalten oder zu verkraften.[262]

In der Literatur wird zumeist die Auffassung vertreten, dass der deutsche Begriff „Belastbarkeit" verkürzt sei und daher sachgerechter und näher am englischen Original von Resilienz gesprochen werden sollte.[263] Da ein pauschaler Vorrang insbesondere der englischen Sprachfassung („resilience") im europäischen Recht aber nicht besteht, gilt es nun auch die anderen Sprachfassungen zu vergleichen.

Allerdings wird auch in der französischen („la résilience"), der italienischen („la resilienza") und der spanischen („la resiliencia") Sprachfassung von „Resilienz" gesprochen. Dies spricht bei einer vergleichenden Betrachtung dafür, auch im Deutschen eher dem lateinischen Wortstamm „resilire" (übersetzt als: zurückspringen, abprallen)[264] folgend von Resilienz als von „Belastbarkeit" zu sprechen. Im Übrigen ist die Übersetzung von „resilience" mit „Belastbarkeit" in die deutsche Rechtssprache nicht durchgängig. In EG 13 der NIS-RL wurde „resilience" dagegen mit „Robustheit" übersetzt, auch im Spanischen findet mit „la resistencia" eine abweichende Übersetzung statt. Im Französischen sowie im Italienischen stimmt die Übersetzung hingegen mit der DSGVO überein. In dem EU Cyber-Security-Act wird neben „Security" auch "Resilience" von (elektronischen) Geräten gefordert; in der deutschen Fassung wird es hier mit „Abwehrfähigkeit" übersetzt, während in den französischen, italienischen und spanischen Fassungen erneut o.g. Pendants der „Resilienz" verwendet werden.[265]

Auch aus der Sicht insbesondere der deutschen Rechtsanwender wäre eine einheitliche Übersetzung dringend geboten, um sowohl auf nationaler wie auch auf europäischer Ebene Missverständnissen und Fehlinterpre-

262 *Duden*, https://www.duden.de/rechtschreibung/Belastbarkeit, zuletzt abgerufen am 20.03.2024.

263 *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (442), Fn. 1; *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 42; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39; wohl auch: DSK, Standard-Datenschutzmodell, Teil B1.19, S. 22.

264 *Langenscheidt Wörterbuch*, https://de.langenscheidt.com/latein-deutsch/resilire, zuletzt abgerufen am 20.03.2024.

265 EU Cybersecurity-Act, VO 2019/991, EG. 2, Satz 2, EG. 5 sowie Art. 1 Abs. 1; in letztgenanntem Fall: "Fähigkeit zur Abwehr gegen Cyberangriffe"

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tationen vorzubeugen. In der nachfolgenden Tabelle wird eine Auswahl von Übersetzungen von *„resilience"* aus EU-Dokumenten (Gesetzen sowie Kommissionsmitteilungen) aus der Sicherheit in der Informationstechnik aufgezeigt, um die Problematik zu verdeutlichen:

Tabelle 3: Übersetzungen von Resilienz im Daten- und IT-Sicherheitsrecht

Übersetzung	**Quelle**
Stabilität	Mitteilung der Kommission zum Schutz kritischer Informationsinfrastrukturen (Titel);[266] Entwurf DORA[267]
Robustheit	Mitteilung der Kommission zum Schutz kritischer Informationsinfrastrukturen (Text)[268]; EG 13 NIS-RL (s.o.)
Abwehrfähigkeit	EU Cybersecurity-Act[269]
Widerstandsfähigkeit	EU Cybersicherheitsstrategie 2013[270]
Resilienz	Mitteilung der Kommission zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit […][271]
Belastbarkeit	Art. 32 DSGVO (s.o.)

Diese Bandbreite an Übersetzungen ist kritisch zu bewerten. Zwar ist es nicht per se schädlich, dass ein Begriff in unterschiedlichen Gesetzen unterschiedlich übersetzt wird, da selbst identische Begriffe in unterschiedlichen Gesetzen nicht stets dieselbe Bedeutung haben müssen (sog. „Relativität der Rechtsbegriffe").[272] Da alle diese Gesetze aber zum Daten- und IT-Sicherheitsrecht i.w.S. gehören, legt der zuvor dargestellte Befund eher eine unsystematische, quasi willkürliche Übersetzungsweise nahe.

Für die Auslegung der deutschen Fassungen der Gesetze aus dem Bereich der IT-Sicherheit sollte daher sowohl aus vergleichender Betrachtung mit den anderen Sprachfassungen als auch angesichts der uneinheitlichen

266 EU KOM 2009 149 endgültig.
267 EU COM 2020 595 final, 24.9.2020; in der verabschiedeten Gesetzesfassung (EU-VO 2022/2554) wurde aber erfreulicherweise der Begriff „Resilienz" in der deutschen Fassung verwendet.
268 EU KOM 2009 149 endgültig, u.a. S. 2 f.
269 Siehe Fn. 265.
270 EU KOM, 2013/01 final, S. 5; ebenso: Strategie für eine sichere Informationsgesellschaft, EU KOM 2006/251 final, S. 7.
271 EU KOM, 2016/410 final, S. 3; aber auch häufig wieder als „Abwehrfähigkeit" übersetzt.
272 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (296 f.), Rn. 20.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Übersetzung in die deutschsprachigen, europäischen Rechtsvorgaben zur IT-Sicherheit der Begriff „Resilienz" als vorzugswürdig angesehen werden. Dies ermöglicht ein einheitliches Verständnis und vermeidet insbesondere mit Blick auf die „Belastbarkeit" und andere „behelfsmäßige Übersetzungen"[273] eine unsachgemäße, semantische Reduktion des Begriffs. Insbesondere die Übersetzung „Belastbarkeit" legt v.a. das reduzierte Verständnis einer „besseren Verfügbarkeit"[274] nahe und kann somit gerade nicht die Inhalte der weitergehenden „Resilienz" vollständig erfassen (dazu in den folgenden Abschnitten ausführlich).

2. Allgemeine Wortbedeutung und domänenspezifische Verwendung

Allerdings ist diese Diversität der Übersetzungen auf europäischer Ebene auch nicht völlig unerklärlich. Als Ausgangspunkt für die Wortlautauslegung ist zunächst auf den gewöhnlichen Sprachgebrauch abzustellen.[275] Ein solcher gewöhnliche Sprachgebrauch im Sinne eines allgemeinen, disziplinübergreifenden Verständnisses des Begriffs ist indes für die Resilienz nur schwerlich auszumachen.

Bezüglich des lateinischen Ursprungs des Begriffs „resilire" ist festzuhalten, dass dieser zunächst mit „zurückspringen" oder „abprallen" übersetzt werden kann.[276] Darauf folgte aber eine sehr bewegte Etymologie des Begriffs, die von „springenden" Fröschen im antiken Rom, über den Rückzug der Königin in England bis hin zu den Anforderungen an Stahlträger im Zeitalter der Industrialisierung reicht.[277] Und auch heute finden sich in den Lexika zumeist nur domänenspezifische Definitionen: So beschreibt der *Brockhaus* die Resilienz mit Blick auf die Psychologie und zwar als „die psychische Widerstandsfähigkeit von Menschen, die es ermöglicht,

273 *Scharte*, Resilience Engineering, S. 37.

274 Derart verkürzend: *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 32, Rn. 32; *Voskamp/D. Klein*, in: Kipker, Cybersecurity, S. 279, Rn. 19b; *Karg*, in: Lang/Löhr, IT-Sicherheit, 99 (111).

275 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (295), Rn. 17; *EuGH*, Urt. v. 05.07.2012 – C-49/11, EuZW 2012, 638 (639), Rn. 32; *EuGH*, Urt. v. 10.03.2005 – C-336/03, NJW 2005, 3055 (3055), Rn. 21.

276 *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754); *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (442); en: bounce back: *Alexander*, NHESS 2013, 2707 (2708); *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9.

277 *Alexander*, NHESS 2013, 2707 (2708 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

selbst widrigste Lebenssituationen und hohe Belastungen ohne nachhaltige psychische Schäden zu bewältigen."[278] Das englische Oxford Lexikon nennt dagegen zwei Definitionen aus anderen Domänen: (1) „The capacity to recover quickly from difficulties; toughness, e.g. the often remarkable resilience of so many British institutions" sowie (2) „The ability of a substance or object to spring back into shape; elasticity., e.g. nylon is excellent in wearability, abrasion resistance and resilience". Während die erste Definition auf die Resilienz soziotechnischer Systeme wie (staatlicher) Institutionen abstellt, entstammt die zweite Definition offensichtlich aus der Materialwissenschaft. Zusammen mit der Psychologie-Definition aus dem *Brockhaus* lassen sich mithin allein in den beiden wohl bekanntesten, englischen und deutschen Lexika drei Definitionen aus unterschiedlichen Fachdomänen finden. Zugleich lässt sich aus diesen Definitionen allerdings eine erste Gemeinsamkeit extrahieren: In allen Fällen wird eine Entität mit einer Einwirkung konfrontiert und die Resilienz bezieht sich insoweit auf die Reaktion bzw. die Reaktionsfähigkeit dieser Entität.

Da sich aber ein darüber hinaus konkretisierender, gewöhnlicher Sprachgebrauch nicht fixieren lässt, ist nun in einem zweiten Schritt der spezifische Sprachgebrauch in ausgewählten Fachdisziplinen zu untersuchen.[279] Für eine intensivierte Analyse werden zunächst die Psychologie (a.), die Ökologie-, Klima- und Umweltforschung (b.) sowie aus der Technikdomäne die Material- und Ingenieurswissenschaft (c.i.), die Informationstechnik (c.ii.) und die kritischen Infrastrukturen (c.iii.) betrachtet. Weiterhin wird das Verständnis gesellschaftlicher Resilienz insbesondere angesichts von Katastrophen untersucht (d.).

Mit diesen Vorkenntnissen wird dann schließlich noch das dem Datensicherheitsrecht nahestehende IT-Sicherheitsrecht untersucht (e.). Dieses enthält zwar noch keine spezifisch IT-Sicherheitsrechtliche Definition, aber zumindest allgemeinere Definitionen sowie verschiedene weitere Anhaltspunkte. Neben deutschen und europäischen Regelungen werden auch solche aus der Schweiz und den USA berücksichtigt.

278 Daneben wird auch „digitale Resilienz" genannt, die aber sehr reduziert nur als „Fähigkeit, Herausforderungen der digitalen Welt zu bewältigen" definiert wird; *Brockhaus,* https://brockhaus.de/ecs/enzy/article/resilienz-psychologie, und https://brockhaus.de/ecs/enzy/article/digitale-resilienz, zuletzt abgerufen am 20.03.2024.

279 Siehe für eine erste Übersicht an Definitionen: Meridan Institute, Definitions of Community Resilience: An Analysis.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Die in den jeweiligen Fachdisziplinen gefundenen Ergebnisse werden im Anschluss an diesen Abschnitt (2.) für die Auslegung der Resilienz als Rechtsbegriff im Datensicherheitsrecht synthetisiert (3.).

a. Psychologie

Der Begriff hat hier bereits eine längere Tradition.[280] Erste Ursprünge finden sich in der Stressforschung, in der *Hans Selye*[281] das allgemeine Anpassungs-Syndrom (ASP) als eine „selbstständige, unspezifische Reaktion des Körpers auf jede Art von Schädigung" beschrieb und dabei in drei Phasen unterteilte: Eine Alarmreaktion als eine Art allgemeine Mobilmachung des Körpers, z.B. durch die Ausschüttung von Stresshormonen. In der sich anschließenden Widerstandsphase versucht der Körper sich mittels einer Gegenreaktion anzupassen, die Stresshormone abzubauen und wieder einen zumindest temporär stabilen Zustand zu erreichen. Nimmt die Belastung aber nicht ab, fällt der Körper danach in eine Erschöpfungsphase, da die Anpassungsenergie während der Widerstandsphase verbraucht wird. Zum besseren Verständnis umschreibt er die Phasen anhand des einfachen Beispiels des Hell-/Dunkel-Sehvermögens wie folgt: Tritt eine Person aus dem Dunkel in eine helle Umgebung, wird sie zunächst geblendet (Alarmreaktion). Daraufhin folgt die Anpassung an die neuen Lichtverhältnisse (Widerstandsphase), wodurch die Person ihre Umgebung wiedererkennen kann. Ist das Licht aber zu hell, etwa weil die Person in die Sonne blickt, erschöpft sich die Sehfähigkeit (Erschöpfungsphase).[282]

Während und nach dem zweiten Weltkrieg richtete sich der Blick spezifischer auf den Bereich der Psychologie, d.h. konkret auf die Frage des menschlichen Umgangs mit widrigen Ereignissen. Der Holocaust-Überlebende und spätere Professor für Neurologie und Psychiatrie an der Universität Wien *Viktor Frankl* stellte mit seinem Konzept der „*Trotzmacht des Geistes*" v.a. auf die innere Einstellung im Sinne einer *positiven Zukunftsorientierung* ab, die insbesondere einen über das Ertragen bzw. das Über-

280 Vgl. zu der nachfolgend dargestellten Entwicklung statt vieler: *Hoffmann*, Organisationale Resilienz, S. 49.

281 *Selye*, Stress beherrscht unser Leben, S. 38, 44 f., 82 ff., 146 ff.; vgl. *Nerdinger/Blickle/Schaper*, Arbeits- und Organisationspsychologie, S. 528 f. mit einer Zusammenfassung.

282 *Selye*, a.a.O., S. 84 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

winden des eigenen Leids hinausgehenden, konkreten Sinn des Lebens voraussetze, der die Frage nach dem „Warum" des Überlebens/Leidens beantwortet.[283]

Daneben nahm auch die Entwicklungspsychologie einen zunehmend großen Raum ein. Impetus der Forschung war hier die Frage, ob, inwieweit und aus welchen Gründen kindliche Entwicklungen angesichts von Konfrontationen mit widrigen Ereignissen unterschiedlich (erfolgreich) verlaufen. Hierzu fand ab den 1950er Jahren auf der Insel Kauai (Hawaii) eine groß angelegte und viel zitierte Studie der Entwicklungspsychologin *Emmy Werner* statt, die mit ihrem Team der University of California knapp 700 Jungen und Mädchen beobachtete, die im Jahr 1955 auf besagter Insel geboren wurden.[284] Im Ergebnis wurde dabei festgestellt, dass von den 201 Kindern, die unter besonders schwierigen Bedingungen -wie etwa psychisch kranke oder alkoholsüchtige Eltern- aufwuchsen, 72 Kinder im Rahmen der 40 Jahre andauernden Beobachtung keine besonderen Auffälligkeiten aufwiesen. Sie erwiesen sich mithin als resilient gegenüber den widrigen Bedingungen, denen sie ausgesetzt waren. Im Rahmen weiterer Untersuchungen konnte dies u.a. darauf zurückgeführt werden, dass diese Kinder mindestens eine besonders enge Bezugsperson hatten und eine solche *soziale Bindung* folglich einen Resilienzfaktor darstellt.[285] Später wurde eine solche enge, soziale Bindung auch als Resilienzfaktor zur Prävention von Jugendgewalt nachgewiesen.[286]

Es folgten weitere Studien im Kinder- und Jugendbereich wie z.B. die in den 1990er Jahren durchgeführte „Bielefelder Invulnerabilitätsstudie", die sich mit Jugendlichen aus schwierigen Verhältnissen beschäftigte. Hierbei konnte auch eine *emotionale Ausgeglichenheit bzw. Robustheit* als Resilienzfaktor identifiziert werden; umgekehrt erwiesen sich Impulsivität und eine geringe Frusttoleranz als schädlich.[287]

Heute kann die Resilienz in der Psychologie[288] ergebnisorientiert definiert werden als „die Fähigkeit einer Person […], erfolgreich mit belasten-

283 *Frankl/Batthyány*, Wer ein Warum zu leben hat, S. 102 f., 117 f., 143., 212 ff.
284 Vgl. *Berndt*, Resilienz, S. 65 f.
285 *Berndt*, Resilienz, S. 67 f.
286 *Lösel/Farrington*, AJPM, Vol. 43 (2012), 8-23.
287 *Berndt*, Resilienz, S. 70.
288 Als Synonyme werden mitunter auch die Begriffe „Stressresistenz, psychische Robustheit oder psychische Elastizität" verwendet, *Wustmann*, Resilienz, S. 18.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

den Lebensumständen und negativen Folgen von Stress umzugehen."[289] Bei belastenden oder widrigen Lebensumständen, fachsprachlich auch „Stressor" genannt, kann insbesondere zwischen chronischen Zuständen und singulären traumatischen Ereignissen unterschieden werden.[290]

Dabei sollte der Begriff „Fähigkeit" nicht dahingehend missverstanden werden, dass es sich um ein einer Person etwa genetisch oder aufgrund ihrer Erziehung statisch anhaftendes Attribut handelt. Vielmehr stellt die Resilienz einen „dynamischen Anpassungsprozess" i.S. einer „Auseinandersetzung mit dem Stressor" dar,[291] der bzw. die je nach Grad der Resilienz unterschiedlich erfolgreich verlaufen kann. Der Prozess umfasst chronologisch sowohl die Anpassung während als auch die Regeneration nach entsprechenden widrigen Lebensereignissen.[292] Aus der inhärenten Notwendigkeit der individuellen Anpassung an den jeweiligen Stressor folgt außerdem, dass die Resilienz einer Person über ihre Lebenszeit und angesichts der Konfrontation mit unterschiedlichen Stressoren variabel ist.[293]

Im Sinne eines präventiven Konzepts wird dabei davon ausgegangen, dass die Resilienz einer Person von verschiedenen, z.T. auch miteinander verschränkten Einzelaspekten („Resilienzfaktoren")[294] abhängig ist, deren bisherige Aufzählung in diesem Abschnitt auch lediglich als exemplarisch anzusehen ist.[295] Weiterhin ist zu beachten, dass diese Faktoren nicht einfach summarisch addiert werden können, sondern oft „miteinander assoziiert sind und interagieren".[296] Neben diesen Resilienzfaktoren wird außerdem erforscht, inwieweit die bisherige Erfahrung von widrigen Lebensereignissen ihrerseits die Resilienz für die Zukunft erhöht, mithin

289 *Wustmann*, Resilienz, S. 18 m.w.N.; *Fröhlich-Gildhoff/Rönnau-Böse*, Resilienz, S. 9; *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754 f.).

290 Forschungsergebnisse beziehen sich häufiger auf die letztgenannte Gruppe, *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754).

291 *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754); *Rutter*, Development and psychopathology 2012, 335 (335).

292 *Helmreich/A. Kunzler/Lieb*, Im OP 2016, 270 (271).

293 *Wustmann*, Psychotherapie Forum, Vol. 17 (2009), Heft 2, 71 (73).

294 Als weitere Resilienzfaktoren werden u.a. der sozioökonomische Status (extern) sowie die kognitive Fähigkeiten und die (Epi-)Genetik des Betroffenen (intern) genannt *Kunzler et al.*, Nervenarzt 2018, 747 (747 f.); *R. Kalisch/Müller/Tüscher*, Behavioral and Brain Sciences 2015, AS-Nr. e128 (nur online); *Wright/Masten/Narayan*, in: Goldstein/Brooks, Handbook of Resilience in Children, 15 (17, 20 f.).

295 Siehe zu weiteren Resilienzfaktoren (dort: „Prädiktoren): *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (755 ff).

296 *Kunzler et al.*, Nervenarzt 2018, 747 (748).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

einen „abhärtenden Effekt“[297] hat. Dies betrifft v.a. die Erholungsphase mit der Frage, welche Begleitumstände nach einem widrigen Lebensereignis vorliegen müssen, damit aus einem solchen ein Gewinn an Resilienz und nicht im schlimmsten Fall sogar eine stärkere Anfälligkeit für künftige, widrige Lebensereignisse erwächst.[298]

Exemplarisch sei hier abschließend auf die Arbeit des *Leibniz-Instituts für Resilienzforschung* in Mainz verwiesen, das seit 2014 die neurowissenschaftlichen und psychologischen Mechanismen der Resilienz erforscht und darauf aufbauend auch versucht, resilienzfördernde Interventionen wie etwa psychologische Trainingsmethoden zu entwickeln.[299]

b. Ökologie, Umwelt- und Klimaforschung

Auch in der Ökologie ist der Resilienzbegriff schon länger gebräuchlich. Er wurde hier v.a. durch *Holling* geprägt, der Resilienz definierte als die Beständigkeit von Beziehungen innerhalb eines Ökosystems sowie als Maß für die Fähigkeit eines solchen, die Veränderung von Zustands- oder Antriebsvariablen aufzunehmen und weiterhin zu bestehen.[300] Damit legte sein Ansatz erstmals ein systembezogenes Verständnis von Resilienz zugrunde.[301]

Entscheidend für *Hollings* Verständnis von Resilienz ist v.a. der Gegenbegriff der Stabilität. Ein resilientes System zeichnet sich demnach durch seine Möglichkeit zu starken Schwankungen aus, etwa Insektenpopulationen, die zwar bei einer äußeren Veränderung sehr stark dezimiert werden, sich aber danach auch sehr schnell wieder erholen.[302] Demgegenüber stehen nicht resiliente Populationen, die zwar an sich eine sehr stabile Größe aufweisen, bei einer Veränderung aber ggf. schneller aussterben können.[303]

---

297 „Steeling or Strengthening Effect“, *Rutter*, Development and psychopathology 2012, 335 (335).

298 *Rutter*, Development and psychopathology 2012, 335 (337 ff).

299 Siehe Webseite der Institution: https://lir-mainz.de/strategie, zuletzt abgerufen am 30.08.2024; *Helmreich/A. Kunzler/Lieb*, Im OP 2016, 270 (271).

300 *S. Kaufmann/Blum*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 235 (238); *Holling*, Annual Review of Ecology and Systematics 1973, 1 (17).

301 *Alsubaie/Alutaibi/Martí*, in: Rome/Theocharidou/Wolthusen, Critical Information Infrastructures Security, 43 (44).

302 *Holling*, Annual Review of Ecology and Systematics 1973, 1 (17 f.).

303 Wie zuvor.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Neben dieser quantitativen Resilienz können ökologische Systeme außerdem auch in qualitativer Hinsicht verschiedene komplexere Zustände einnehmen, z.B. Flachwasserseen, die „in Abhängigkeit von Variablen wie Nährstoffgehalt, Seegröße und Temperatur – zwischen einem Klarwasserzustand und einem eutrophierten, trüben Zustand wechseln" können.[304]

Zusammenfassend als maßgeblich festzuhalten ist daher, dass in der Ökologie ein resilientes System durch die Fähigkeit zur Einnahme unterschiedlicher quantitativer und qualitativer Zustände zwar nicht in einem Sinne stabil ist, dass es einen Gleichgewichtszustand kontinuierlich beibehält, aber sich gleichwohl bzw. gerade deshalb als besonders überlebensfähig und mithin resilient auszeichnet.[305] Auch ist es ökologischen Systemen möglich, sich dauerhaft anzupassen[306] und nicht mehr in einen bereits bekannten Zustand zurückzukehren. Hierin wird der wesentliche Unterschied zwischen technischer und ökologischer Resilienz gesehen, da technische Resilienz in der Regel (nur) darauf zielt in einen ursprünglich vorgesehenen „Normal-Betriebszustand" zurückzukehren.[307]

Eine etwas andere Dimension entwickelt der ökologische Resilienzbegriff, soweit der Mensch als Teil des ökologischen Systems berücksichtigt wird. So untersucht etwa das *Stockholm Resilience Centre*[308] die Resilienz mit Blick darauf, dass die Menschen und die Natur auf der Erde ein einheitliches sozio-ökologisches System bilden. Dieses soll resilient sein, d.h. in die Lage versetzt werden mit Veränderungen umzugehen und sich fortwährend weiterzuentwickeln. Maßgeblich soll dies durch die Gestaltung der Beziehung zwischen Menschen (untereinander) sowie zwischen Menschen und Natur erreicht werden. Zur Erreichung von Resilienz werden dabei sieben Prinzipen genannt,[309] von denen zumindest die ersten fünf für die vorliegende Auslegung relevant erscheinen:

---

304 *Brand/Hoheisel/Kirchhoff*, in: Bayerische Akademie für Naturschutz und Landschaftsplege (ANL), Landschaftsökologie. Grundlagen, Methoden, Anwendungen, 78 (80) m.w.N.

305 *Holling*, Annual Review of Ecology and Systematics 1973, 1 (17 f.); siehe aber auch kritisch zur Frage der Allgemeingültigkeit dieses Konzepts: Fn. 304.

306 Ähnlich auch: *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (266).

307 *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (265 f.); *Zampieri*, Ecosphere, Vol. 12 (2021), Heft 2, S. 1.

308 https://www.stockholmresilience.org/research/research-news/2015-02-19-what-is-resilience.html, zuletzt abgerufen am 30.08.2024.

309 *R. Biggs et al.*, ARER 2012, 421 (425 ff.); hier nicht mit aufgenommen wurden die „breite Beteiligung anderer Personen" sowie „polyzentrale Regierungssysteme".

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Diversität bzw. Redundanz:
   Nur ‚diverse' Systeme mit *vielen (unterschiedlichen) Komponenten* wie etwa Tierarten besitzen die Fähigkeit der Kompensation von ausfallenden Komponenten. Umgekehrt bedeutet dies auch, dass nicht redundante Komponenten besonders geschützt werden sollten.
2. Verbundenheit
   Kann in positiver Hinsicht die Regeneration beschleunigen, in negativer Hinsicht aber auch zur schnelleren Ausbreitungen von Störungen führen (Domino-Effekt).
3. Langsame Variablen und Rückkopplungen
   Gewisse Variablen wie etwa *Sättigungsfaktoren* in Flüssigkeiten (Gewässern) oder Gasen (Atmosphäre) werden lange ‚absorbiert', ohne dass es zu einer qualitativen Auswirkung kommt; ab gewissen Sättigungswerten werden aber *Kipppunkte* erreicht, die nur schwer kontrollier- oder umkehrbare Folgen haben, da es ab diesem Moment zu weiteren Rückkopplungen kommt.
4. CAS-Ansatz
   Der komplexe adaptive Systemansatz (CAS) bedeutet, dass innerhalb eines sozio-ökologischen Systems mehrere Zusammenhänge auf verschiedenen Ebenen gleichzeitig auftreten. Damit gehen eine *gewisse Unvorhersehbarkeit* und Unsicherheit einher, die akzeptiert werden müssen. Weiterhin muss dabei stets eine Vielzahl von Perspektiven berücksichtigt werden.
5. Aktives Lernen
   Sozio-ökologische Systeme befinden sich in einem Zustand der ständigen, dynamischen Entwicklung. Daher besteht die Notwendigkeit, das *vorhandene, aber stets unvollständige und unsichere Wissen zu ergänzen* und ggf. auch zu revidieren.

Neben den bislang dargestellten positiven Resilienzaspekten werden im Klimaschutz auch wie soeben in Ziff. 3 angedeutet die *Grenzen der Resilienz* aufgezeigt, d.h. Kipppunkte bestimmter Parameter wie z.B. der CO_2-Konzentration, bei deren Erreichen nichtlineare, abrupte Umweltveränderungen auftreten, die das Leben auf der Erde für die Menschheit deutlich erschweren würden.[310] Insgesamt wird nach diesem sozio-ökologischen Resilienzverständnis somit anders als bei einer rein ökologischen Betrachtung und ähnlich der technischen Resilienz (dazu sogleich) ein erhaltenswerter

310 *Rockström et al.*, E&S, Vol. 14 (2009), Heft 2, S. 1 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zustand umschrieben, der sich in diesem Fall durch den Fortbestand der für den Menschen notwendigen Lebensgrundlagen auszeichnet.

c. Technische Resilienz

Im nachfolgenden wird das technische Verständnis von Resilienz behandelt. Da sich dieses Verständnis wesensmäßig von den Fragen der Psychologie oder der Ökologie unterscheidet, wird es in diesem Absatz als „dritte Strömung" zusammengefasst. Aufgrund der Nähe zur hier gegenständlichen, ebenfalls im Kern technischen „Sicherheit der Verarbeitung" fand hier eine besonders umfangreiche Erhebung statt. Sie wird weiter unterteilt in die Unterbereiche Material- und Ingenieurswissenschaft (i.), Informationstechnik (ii.) und den Schutz kritischer Infrastrukturen (iii.).

i. Material- und Ingenieurswissenschaft

In der Materialwissenschaft wird die Resilienz wie schon in der obigen Definition des Oxford-Lexikons aufgezeigt als Elastizität von Materialien wie z.B. Nylon verstanden. Wissenschaftlich formuliert beschreibt Resilienz demnach „die Fähigkeit eines Materials, sich durch Energieeinwirkung elastisch zu verformen. Das Maß für Resilienz ist hier die maximale Energie, die das Material pro Volumeneinheit aufnehmen kann, ohne sich permanent (also plastisch bzw. spröde) zu verformen"[311], d.h. unbeschadet zu bleiben.[312]

In der Ingenieurswissenschaft lässt sich die Resilienz komplexer Systeme implementieren bzw. erhöhen, indem man bereits bei der Entwicklung des Systems den möglichen Ausfall von einzelnen Systemkomponenten wie etwa Lüftern, Ventilen oder Rohren berücksichtigt und entsprechende Techniken etabliert, die eine minimale Funktionsfähigkeit des Systems trotz des Ausfalls beliebiger Komponenten garantieren und die Möglichkeit bietet, die Funktionalität im Nachhinein vollständig wiederherzustellen.[313]

311 *Scharte/K. Thoma*, in: Wink, Multidisziplinäre Perspektiven der Resilienzforschung, 82-98, S. 83.

312 *Fooken*, in: Wink, Multidisziplinäre Perspektiven der Resilienzforschung, 13 (24 f.); vgl. auch: *Sheridan*, Hum Factors 2008, 418 (423).

313 *Altherr et al.*, AMM, Vol. 885 (2018), 240 (242).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ii. Informationstechnik

In der Informationstechnik ist der Diskurs zur Resilienz gemessen an der Bedeutung des Begriffs in anderen Domänen bislang noch eher klein.[314] Überwiegend wird Resilienz hier als die Fähigkeit eines Informationssystems gesehen, Veränderungen in seiner externen Umgebung zu bewältigen.[315] Diese recht allgemeine Definition soll im Weiteren geschärft und dabei die unterschiedlichen Konnotationen der Resilienz in den Bereichen Verlässlichkeit (1) und IT-Sicherheit (2) berücksichtigt werden. Diese großen Bereiche gegenüberstellend und zusätzlich die Bereiche Netzwerktechnik und Software-Entwicklung berücksichtigend wird unter (3) ein abschließendes Fazit für den Bereich der Informationstechnik gebildet.

(1) Verlässlichkeit

In der Forschung der Verlässlichkeit von informationstechnischen Systemen meint *Verlässlichkeit* (en: Dependability)[316] selbst zunächst die Fähigkeit eines Systems einen berechtigt vertrauenswürdigen Dienst anzubieten; ein berechtigt vertrauenswürdiger Dienst liegt wiederrum dann vor, wenn Ausfälle desselben nicht über ein akzeptables Maß an Häufigkeit und Schwere hinaus gehen.[317]

Die Resilienz wurde hier von *Avizienis/Laprie* als ein Synonym für Fehlertoleranz (en: Fault Tolerance) verstanden.[318] Dem Konzept der Fehlertoleranz liegt eine im Englischen sprachlich ausdifferenzierte Fehlerkette zugrunde, die nachfolgend illustriert wird.[319]

---

314 *Heeks/Ospina*, ISJ (Information Systems Journal) 2019, 70 (71 ff.)

315 Wie zuvor.

316 Ebenso übersetzend und kritisch zur Übersetzung als „Zuverlässigkeit": *Pfitzmann*, DuD 1993, 539 (540).

317 Das Erfordernis der Vertrauenswürdigkeit ergibt sich aus der Abhängigkeit von einem System, d.h. aufgrund der Abhängigkeit von einem System bzw. einem Dienst muss auf dessen Verlässlichkeit vertraut werden (können); *Avizienis et al.*, IEEE TDSC 2004, 11 (13, 22)

318 *Avizienis et al.*, IEEE TDSC 2004, 11 (14, 27).

319 *Avizienis et al.*, IEEE TDSC 2004, 11 (15 ff.); *B. Randell/P. Lee/Treleaven*, ACM CSUR 1978, 123 (125 f.); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (8 f.); in der Netzwerktechnik auch: *Sterbenz et al.*, Computer Networks 2010, 1245 (1246).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

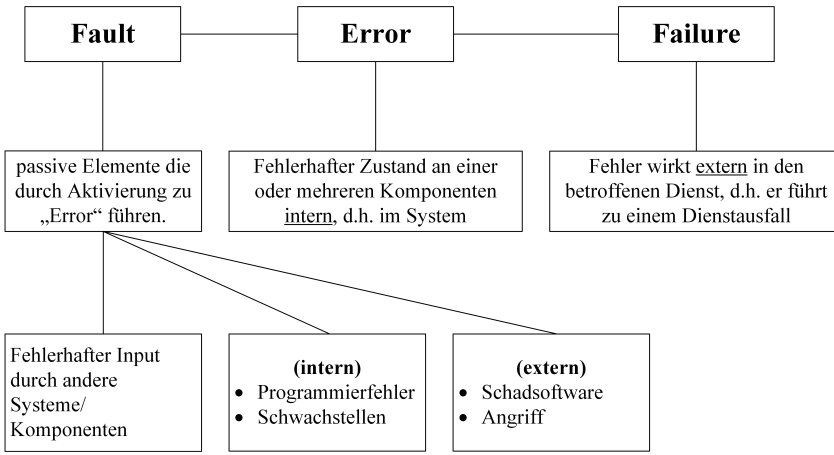

Abbildung 6: Fehlerkette in der Verlässlichkeit

Die Fehlertoleranz wird definiert als das Vermeiden eines Dienstausfalls (en: Service Failure) angesichts von Fehlern (en: Faults).[320] Ein Dienstausfall liegt vor, wenn der tatsächlich erbrachte Dienst von dem korrekten Dienst abweicht, d.h. die entsprechende Systemfunktion nicht erfüllt wird.[321]

Sie umfasst hierfür zunächst die Erkennung des fehlerhaften Zustands (en: Error detection) sowie die anschließende Wiederherstellung (en: Recovery).[322] Letztere bezieht sich sowohl auf die Beseitigung des fehlerhaften Zustands (en: Error Handling) als auch auf die Beseitigung bzw. das dauerhafte Verhindern der Reaktivierung der diesen Zustand auslösenden Elemente (Fault Handling).[323] Entsprechend o.g. Definition soll somit durch die Fehlertoleranz das Versagen des Dienstes und im Ergebnis eine Beeinträchtigung der Verlässlichkeit vermieden werden.[324]

320 *Avizienis et al.*, IEEE TDSC 2004, 11 (14).
321 Dies schließt sowohl die vollständig als auch teilweise fehlende, zeitliche Verfügbarkeit des Dienstes als auch die die inhaltlich fehlerhafte Diensterbringung ein: *Avizienis et al.*, IEEE TDSC 2004, 11 (13, 18 f.).
322 *Avizienis et al.*, IEEE TDSC 2004, 11 (24 ff.).
323 Wie zuvor.
324 *Avizienis et al.*, IEEE TDSC 2004, 11 (14).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

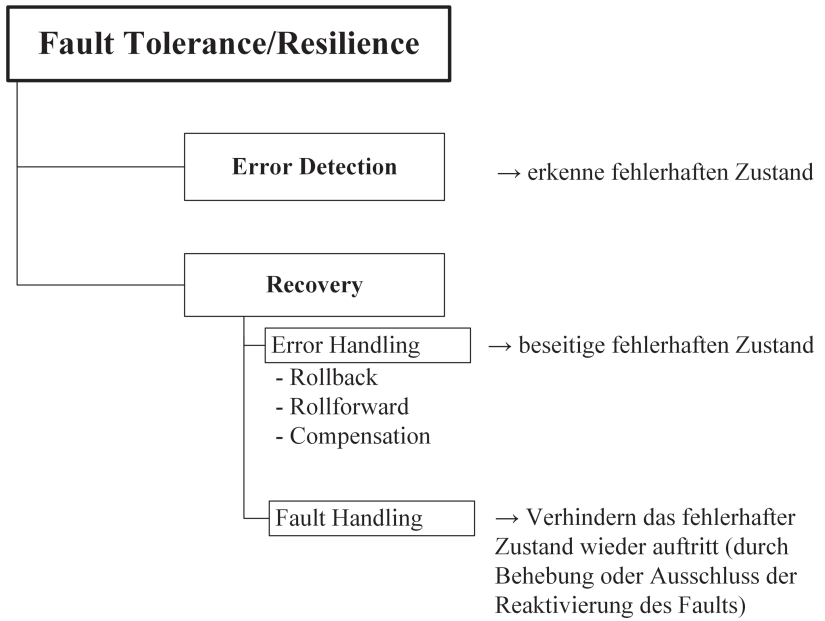

Abbildung 7: Fault Tolerance/Resilience

In dieser Methodik ist besonders das reaktive Element der Resilienz erkennbar: Falls ein fehlerhafter Zustand eingetreten ist, soll dieser erkannt und sodann beseitigt werden. An Beseitigungsmethoden[325] steht zunächst der sog. Rollback zur Verfügung, d.h. das System wird in einen vorherigen, fehlerfreien Zustand zurückversetzt. Beim Rollforward hingegen wird ein neuer, fehlerfreier Zustand hergestellt. Schließlich besteht die Möglichkeit der Kompensation, d.h. der fehlerhafte Zustand wird durch den Einsatz von Redundanzen gewissermaßen „maskiert", so dass er sich nicht mehr als Dienstausfall auswirkt.

Später wurde Resilienz von *Laprie* mit Blick auf die Verlässlichkeit umfassender definiert als „die Beständigkeit von Verlässlichkeit bei Veränderungen.[326] Damit bezieht sich die Resilienz nicht nur auf die Fehlertoleranz,

325 *Avizienis et al.*, IEEE TDSC 2004, 11 (25).

326 En: "Resilience is defined as the persistence of dependability when facing changes"; *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9. *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (13).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

sondern auch auf die Fehlerprävention, die (nicht akute) Fehlerentfernung und die Fehlervorhersage.[327] Diese Verschiebung des Fokus‘ auf Veränderungen war und ist demnach geboten, da die modernen großen und vernetzten Informationsinfrastrukturen als ubiquitäre Systeme ständig mit Veränderungen, insbesondere hinsichtlich der Bedrohungslage, konfrontiert sind. Um Resilienz zu gewährleisten, müssen sich Systeme somit insbesondere an diese Veränderungen anpassen können (en: evolvability);[328] die Veränderungen lassen sich dabei in funktionale und strukturelle Veränderungen unterteilen. Funktionale Veränderungen meinen in diesem Kontext veränderte Anforderungen der Nutzer:innen an das System.[329] Dagegen beziehen sich strukturelle Veränderungen auf die eingesetzte Technologie und die Umwelt, z.B. ein Fehler in einer Komponente oder auch eine veränderte Bedrohungslage durch Angreifer:innen.[330] Diese Veränderungen, gegen die das informationstechnische System resilient sein soll, können dabei insbesondere auch unvorhergesehen auftreten.[331]

Neben den zuvor dargestellten Anpassungen im Rahmen der *Fault Tolerance* einschließlich der Wiederherstellung haben andere Forschende auch weitere Resilienzaspekte entwickelt, etwa die maßvolle Degradation, d.h. dass ein Dienstlevel reduziert wird, ohne einen kompletten Ausfall zuzulassen (z.B. ein geringerer Funktionsumfang).[332] Soweit die entsprechenden Anpassungen von den informationstechnischen Systemen autonom erfolgen, wird auch von „selbst-adaptiven Systemen“ gesprochen.[333] Als

327 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9; ausführlich zu diesen Begriffen: *Avizienis et al.*, IEEE TDSC 2004, 11 (24 ff.)

328 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9.

329 Z.b. gestiegene Lastanforderungen: *Laprie*, in: Fourth IEEE International Symposium on Network Computing and Applications, Resilience for the Scalability of Dependability, 5 (5); *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (15); zum holistischen Verständnis von „Funktion“ (d.h. nicht nur wie hier Nutzeranforderungen, sondern auch Sicherheitsanforderungen) in dieser Untersuchung: S. 202.

330 Wie zuvor.

331 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9; *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (11); *Cámara et al.*, Computing 2013, 689 (689).

332 *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (16).

333 *Cámara et al.*, Computing 2013, 689 (690).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

weitere Aspekte der Resilienz neben den skizzierten Kernelementen werden auch genannt:[334] Erstens die Bewertbarkeit in Bezug auf die Effektivität der Resilienz. Zweitens die Nutzbarkeit von Resilienztechniken sowohl für Administrator:innen als auch mit Blick auf die Anforderungen der Nutzer:innen. Und schließlich die Diversität des Systems, um sog. Single Points of Failure (SPOF) zu vermeiden, d.h. dass ein singuläres Ereignis alle (redundant vorgehaltenen) Komponenten gleichermaßen betrifft.

(2) IT-Sicherheit

Ob und inwieweit die o.g. Verlässlichkeit auch die IT-Sicherheit bereits mit einschließt, ist zweifelhaft. IT-Sicherheit lässt sich als der Schutz eines informationstechnischen Systems vor unautorisierten Eingriffen verstehen.[335] Dabei sind die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen[336] und Informationstechnik[337] angesichts solcher Eingriffe zu wahren.

Auch bei *Avizienis/Laprie et al.* wurde die IT-Sicherheit im Rahmen der Verlässlichkeit nicht von Anfang an berücksichtigt, sondern erst zu einem späteren Zeitpunkt einbezogen[338] und auch die Fehlertoleranz bzw. Resilienz wie oben dargestellt hierauf erstreckt.[339] Diese Integration der IT-Sicherheit in die Verlässlichkeit wird teilweise insbesondere mit Blick auf die sehr unterschiedlichen Terminologien kritisch gesehen.[340]

334 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9.

335 Vgl. *Eckert*, IT-Sicherheit, S. 6; *Avizienis/Laprie/Randell,* Fundamental Concepts of Dependability, 2001, S. 3; *L. Fischer/Lehnhoff*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 316 (318).

336 DIN, ISO/IEC 27000:2017, S. 12, Ziff. 2.33 (Definition: Informationssicherheit); BSI, IT-Grundschutz-Kompendium, 2023, Glossar, S. 3.

337 *Solms/van Niekerk*, Computers & Security, Vol. 38 (2013), 97 (98); *Whitman/Mattord*, Principles of Information Security, S. 8.

338 Folglich wurden in der sehr weiten Definition des Fehlers (fault) sowohl intern als auch extern ausgelöste sowie fahrlässige ebenso wie absichtlich, böswillig ausgelöste Fehler umfasst; *Avizienis et al.*, IEEE TDSC 2004, 11 (15); Ähnlich zur Resilienz als Eigenschaft sowohl für Verlässlichkeit als auch IT-Sicherheit: *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (8).

339 Wohl zustimmend, da auch auf „Angriffe" abstellend: *W. J. Zhang/Lin*, Enterprise Information Systems, Vol. 4 (2010), Heft 2, 99 (102).

340 Mit einem alternativen Vorschlag zur Integration: *Jonsson/Olovsson*, in: Pham/Hamza, Proceedings of the IASTED International Conference on Reliability, Quality Control and Risk Assessment, 93 (93 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Jedenfalls hat die IT-Sicherheit auch eine eigene historische Entwicklung hinter sich, die sich zumeist auch unabhängig von der Verlässlichkeit vollzog.[341] Auch hier wurde die Resilienz als wichtiges Merkmal erkannt und definiert. Dabei wird sie mitunter auch ausdrücklich neben den klassischen Schutzzielen genannt.[342] Für die Bestimmung der Resilienz ist demnach im Ausgangspunkt anzuerkennen, dass *Bedrohungssituationen unvermeidbar sind*, ständig wiederkehren und es dabei auch zumindest zu partiellen Fehlfunktionen der Verteidigung kommen wird. Dies ist insbesondere auf eine starke Ungewissheit bezüglich der drohenden Ereignisse zurückzuführen, da sich die Angriffsformen schnell weiterentwickeln.[343] Im Falle eines solchen unvorhergesehenen, durchbrechenden Angriffs müsse es das Ziel sein, „Ressourcen und [auszuführende] Operationen zu priorisieren, besonders wichtige Schlüsselwerte und Systeme vor den Angriffen zu beschützen und am Ende einen normalen operativen Zustand wiederherstellen zu können".[344] Dazu gehört *auch die soziotechnische Komponente*, also die Mitarbeitenden, einzubeziehen.[345]

Zur Resilienz in der IT-Sicherheit gehören laut *Singer/Friedman* im Ergebnis drei Elemente:[346] Das erste Element ist die Fähigkeit [durch flexible Anpassung] die beabsichtigte Leistungsfähigkeit auch unter verschlechterten Bedingungen (Ereignis) erbringen zu können.[347] Dazu muss indes auch (vorgelagert) die Erkennung dieses Ereignisses gehören, da andernfalls eine Anpassung nicht möglich ist. Zweitens muss schnellstmöglich die schon angesprochene Wiederherstellung stattfinden. Und drittens muss aus den Ereignissen gelernt werden, um in Zukunft besser mit Angriffen umgehen zu können.

341 *Avizienis et al.*, IEEE TDSC 2004, 11 (22); grundlegend zur Information Security: *Saltzer/Schroeder*, Proc. IEEE 1975, 1278 (1278 ff.).
342 *Singer/Friedman*, Cybersecurity and cyberwar, S. 36.
343 *Collier et al.*, Computer 2014, 70 (70); *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2).
344 *Singer/Friedman*, Cybersecurity and cyberwar, S. 35.
345 *Collier et al.*, Computer 2014, 70 (75); *Singer/Friedman*, Cybersecurity and cyberwar, S. 171.
346 *Singer/Friedman*, Cybersecurity and cyberwar, S. 170 f.; ähnlich auch: "ability of the system to prepare, absorb, recover and adapt to adverse effects": *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (12).
347 Vgl. *Alt*, Die Sachverständigen 2020, 169 (170).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

(3) Weitere Teilbereiche und Fazit

Ob Resilienz im Kontext der spezifischen IT-Sicherheit begrifflich anders verstanden werden muss als im klassischen Bereich der Verlässlichkeit, ist zweifelhaft. Methodisch zeigen sich zumindest starke Überschneidungen wie die Erkennung des fehlerhaften Zustands sowie die anschließende Behebung bzw. Abwehr desselben. Danach soll in beiden Fällen aus dem Ereignis „gelernt" werden, indem die auslösenden Elemente dauerhaft deaktiviert bzw. die entsprechenden Angriffspfade geschlossen werden.

Auf sachlicher Ebene können sich indes Unterschiede ergeben, insbesondere bei der Betrachtung von typischerweise in der Verlässlichkeit adressierten, fahrlässig oder zufällig ausgelösten Ereignissen einerseits und andererseits die für die IT-Sicherheit prägenden, absichtlich agierenden Akteure, was zu unterschiedlichen Ausgestaltungsanforderungen führen kann:[348] Soweit es z.B. bei zufälligen Fehlern wie etwa Hardware-Defekten oder Naturkatastrophen zu Ausfällen kommen kann, reicht zur Herstellung der Resilienz im Sinne der Verlässlichkeit unter Umständen bereits eine bloße Redundanz der jeweiligen Komponenten oder Systeme. Ein(e) Angreifer:in, welche(r) diese Struktur kennt, könnte dann aber mit nur einer Schadsoftware die identischen, redundanten Systeme und Komponenten ausschalten und so diese Backup-Sicherung leicht überwinden.[349] Somit sind für die Resilienz in der IT-Sicherheit zumindest eine heterogene Redundanz[350] (Diversität) oder sogar gänzlich andere Resilienzmechanismen erforderlich. Für die abstrakte begriffliche Bestimmung der Resilienz im vorliegenden Kontext erscheinen aber sowohl das Verständnis der IT-Sicherheit als auch der Verlässlichkeit zumindest als Ausgangsbasis nutzbar.

Neben den bereits genannten großen Strömungen der Verlässlichkeit und der IT-Sicherheit sind noch zwei konkretere Teilbereiche zu nennen, die bezüglich der Resilienz im Bereich der Informationstechnik Hinweise geben können:

Zum einen die Netzwerktechnik[351], in der Resilienz v.a. die Fähigkeit betrifft mit stark schwankenden Lasten umgehen zu können. Eine hohe Last-

348 *Singer/Friedman*, Cybersecurity and cyberwar, S. 171.

349 *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (13); *Singer/Friedman*, Cybersecurity and cyberwar, S. 170.

350 *L. Fischer/Lehnhoff*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 316 (337).

351 Vgl. *L. Xie et al.*, in: Hutchison/Denazis/Lefevre/Minden, Active and Programmable Networks, 83 (83 f.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

phase kann einerseits durch sog. flash crowd events, also einem plötzlichen Anstieg legitimen Datenverkehrs (en: Traffic) entstehen,[352] z.B. eine hohe Last auf den Servern, die VoIP-Dienste anbieten, infolge der Ausgangsbeschränkungen im Rahmen der Corona-Krise. Andererseits kann eine solche Lastphase auch böswillig durch sog. DDoS-Angriffe ausgelöst werden, bei denen ein Botnetz unerwünschten Traffic in Form von „sinnlosen" Anfragen durchführt, mit dem expliziten Ziel die Server und Netzwerke zu überlasten.[353] Mitunter sind ausgeklügelte DDoS-Angriffe aber gar nicht ohne Weiteres von legitimem Datenverkehr zu unterscheiden.[354] Folglich muss „Resilienz" hier sowohl auf angriffsbedingte als auch auf an sich legitime Lastspitzen eine Antwort bieten. Gleiches gilt generell bei lokalen Ausfällen von Knotenpunkten in einem Netzwerk, bei denen es ebenfalls nicht darauf ankommt, ob dies durch einen Angriff oder einen Fehler geschieht.[355] Ein resilientes Netzwerk bietet und erhält trotz solcher Einwirkungen zumindest noch ein „akzeptables Dienstniveau".[356]

In der Softwareentwicklung kann man auch von „Resilient Software Development" sprechen, wobei Software-Resilienz ganz ähnlich, wenn auch detaillierter definiert wird als „die Fähigkeit, das Ausmaß und/oder die Dauer von Störungsereignissen zu reduzieren. Die Effektivität einer resilienten Anwendungs- oder Infrastruktursoftware hängt von ihrer Fähigkeit ab, ein potenziell störendes Ereignis zu erkennen, zu absorbieren, sich anzupassen und/oder sich schnell davon zu erholen."[357]

Insgesamt bleibt festzuhalten, dass die Resilienz in der Informationstechnik die Reaktion auf verschiedene Ereignisse wie Angriffe, fehlerhafte Systemzustände, Lastspitzen in Netzwerken oder Programmstörungen beschreibt. Dabei soll das in Rede stehende Ereignis zunächst in einer akuten

352 Vgl. *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (13).

353 *R. Grimm/Waidner*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 33 (44, 49), Rn. 44, 73 ff.; *LG Düsseldorf*, Urt. v. 22.03.2011 – 3 KLs 1/11, MMR 2011, 624 (624), mit Anmerkung *Bär*, S. 625 f.

354 Vgl. *Eckert*, IT-Sicherheit, S. 12.

355 *Bishop et al.*, in: Proceedings of the 2011 workshop on New security paradigms workshop (NSPW), Resilience is more than availability, 95 (95).

356 *L. Xie et al.*, in: Hutchison/Denazis/Lefevre/Minden, Active and Programmable Networks, 83 (84). *Sterbenz et al.*, Computer Networks 2010, 1245 (1246).

357 Englisches Original: "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient application or infrastructure software depends on its ability to anticipate, absorb, adapt do and/or recover rapidly from a potentially disruptive event." In: *Merkow/Raghavan*, Secure and resilient software, S. 1 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Phase erkannt und bewältigt werden, um eine Beeinträchtigung des jeweiligen Dienstes möglichst zu verhindern oder andernfalls die Funktionsfähigkeit des Dienstes schnellstmöglich wiederherzustellen. Außerdem soll eine Reaktivierung der Elemente, die das Ereignis ausgelöst haben für die Zukunft möglichst ausgeschlossen werden.

Ungeachtet dessen, dass sich fahrlässige und zufällige Ereignisse, wie sie tradiert von der Verlässlichkeit erfasst werden, einerseits und vorsätzliche Sicherheits-Ereignisse andererseits, oft ohnehin nicht unterscheiden lassen (wie etwa in der Netzwerktechnik), so ist eine Differenzierung auf definitorischer Ebene der Resilienz jedenfalls auch nicht erforderlich. Allein auf der Maßnahmenseite können sich insoweit Unterschiede ergeben.

iii. Kritische Infrastrukturen

Einen weiteren Referenzbereich für die technische Resilienz bilden die kritischen Infrastrukturen. Kritische Infrastrukturen sind „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."[358] Im RegE BSIG wird nun in § 2 Nr. 22 stattdessen der Begriff „kritische Anlagen" verwendet.[359] Erfasst werden u.a. Einrichtungen aus den Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation.

In der bereits untersuchten Informationstechnik steht die Resilienz von IT-Systemen im Fokus. Der Resilienzbegriff geht im Bereich kritischer Infrastrukturen notwendigerweise noch darüber hinaus, da etwa bei Energieerzeugungsanlagen eingebettete IT-Systeme (Embedded Systems) vorliegen, die mit den übrigen Bestandteilen ein *cyber-physisches sowie ein soziotechnisches Gesamtsystem* bilden.[360] Kernziel der Resilienz ist hier, dass die von der kritischen Infrastruktur erbrachte Dienstleistung nicht unterbrochen wird.

358 BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009, S. 3.

359 *Kipker/Dittrich*, MMR 2023, 481 (481 f.).

360 Vgl. *Alsubaie/Alutaibi/Martí*, in: Rome/Theocharidou/Wolthusen, Critical Information Infrastructures Security, 43 (50); *Gazos*, in: Polarisierte Welten: Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie, Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen, S. 1, 3.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Dieses Ziel ist weiter gefasst als das Verständnis der Informationstechnik, soweit diese nur auf die Funktionalität der IT-Systeme abstellt. Durch die Einbettung sind die IT-Systeme nicht mehr isoliert, sondern im Kontext des Gesamtsystems zu betrachten, etwa bei der Frage wie ein IT-System bei Ausfall einer physischen Komponente reagiert. Umgekehrt kann ein defekter Steuerungsdienst in einem Kraftwerk den Generator schädigen und so einen Abbruch der Stromerzeugung herbeiführen. Auch die soziale Komponente (mithin das Personal) ist bei kritischen Infrastrukturen ergänzend zu berücksichtigen, hier jedoch nicht nur bezüglich der Informationstechnik, sondern bezüglich des ganzen cyber-physischen Systems.

In der wissenschaftlichen Literatur[361] lässt sich zwar keine feststehende Definition, aber zumindest ein grober Konsens dahingehend feststellen, dass unter Resilienz die Fähigkeit eines Systems verstanden werden kann, „internen/externen Belastungen standzuhalten und sich von ihnen zu erholen."[362] Das Ziel der Resilienz liegt somit in der Gewährleistung einer möglichst kontinuierlichen bzw. schnell wiederherstellbaren Funktionalität[363] dieses Gesamtsystems angesichts solcher Belastungen.

d. Gesellschaftliche Resilienz / Katastrophenschutz

Die gesellschaftliche oder auch „soziale Resilienz"[364] ist vor allem mit Blick auf zwei Kategorien von Ereignissen bedeutsam: Einerseits schleichende, längerfristige Ereignisse bzw. Veränderungen wie z.B. der Klimawandel und andererseits abrupte Störereignisse in Gestalt von Katastrophen.[365]

Aufgrund der höheren Vergleichbarkeit mit Daten- und IT-Sicherheitsvorfällen wird nachfolgend nur auf letzteres eingegangen. Unter Katastrophenschutz werden somit im hiesigen Kontext alle Maßnahmen verstanden, die (ggf. schon vorher vorbereitet) auf den Eintritt einer Katastro-

361 Eine exemplarische Übersicht findet sich bei: *Alsubaie/Alutaibi/Martí*, in: Rome/Theocharidou/Wolthusen, Critical Information Infrastructures Security, 43 (45).

362 *Y. Fang/Zio*, in: Gritzalis/Theocharidou/Stergiopoulos, Critical Infrastructure Security and Resilience, 97 (98 f.) m.w.N.

363 Ebd.

364 Definiert als „Widerständigkeit sozialer Gemeinschaften": *Bonß*, in: Endreß/Maurer, Resilienz im Sozialen, 15 (26).

365 Wie zuvor; Vgl. OECD, Concepts and dilemmas of State building in fragile situations, 2009, S. 17.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

phe[366] reagieren und versuchen diese zu bewältigen. Insofern ist er dem (technischen) IT-Sicherheitsrecht ereignis-chronologisch nachgelagert, etwa wenn die Katastrophe in Form eines großflächigen Stromausfalls infolge des Versagens ein oder mehrerer kritischer Energieerzeugungsanlagen vorliegt.[367]

Da Katastrophen trotz aller Bemühungen nicht immer vorherhergesehen und damit auch nicht durch „planende Vorausschau" verhindert werden können,[368] kommt der Resilienz mit ihren Aspekten der Anpassung während der Katastrophe bzw. der Regeneration nach einer solchen eine besondere Bedeutung zu.[369] Dementsprechend lässt sich als Kerngedanke hier „die Möglichkeit, mit negativen Folgen von Ereignissen durch unterschiedlichste Strategien fertigzuwerden"[370] identifizieren. Dass der Resilienz in diesem Sinne heute große Bedeutung zukommt ist auch Ausdruck einer Verlagerung, mit der der Fokus sich nicht mehr nur auf die präventive Reduktion der Verletzlichkeit (auch Resistenz genannt)[371] beschränkt, sondern insbesondere auch darauf bezogen wird, eine starke Resilienz im Katastrophenfall zu gewährleisten.[372]

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) definiert Resilienz noch recht abstrakt als „Fähigkeit eines Systems, Ereignissen zu widerstehen bzw. sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder möglichst schnell wieder zu erlangen".[373] Das *USA National Research Council* ist in seiner Definition hingegen deutlich detaillierter: „Die Fähigkeit, widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen." Auch das *United Nations Office for Disaster Risk Reduction (UNDRR)* verfolgt einen solch umfassenden Ansatz, indem es Resilienz definiert als die „Fähigkeit eines Systems, einer Gemeinschaft oder Gesellschaft, die Gefahren ausgesetzt ist, den

366 BBK, Online-Glossar des BBK, 2024, Definition Katastrophe.
367 Dies gilt umgekehrt aber nicht für Katastrophen, die etwa durch Naturereignisse ausgelöst werden.
368 *Würtenberger*, in: Baumeister, Staat, Verwaltung und Rechtsschutz, 561 (564).
369 Vgl. *Bonß*, in: Endreß/Maurer, Resilienz im Sozialen, 15 (19f.); ähnlich auch: *Häfele/Renn/Erdmann*, in: Häfele, Energiesysteme im Übergang, 375 (408).
370 *Krüger/Max*, Resilienz im Katastrophenfall, S. 31.
371 *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (263 ff.).
372 *Korff*, in: Lewinski, Resilienz des Rechts, 23 (23).
373 BBK, Online-Glossar des BBK, 2024, Definition Resilienz.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Auswirkungen einer Gefahr rechtzeitig und effizient zu widerstehen, sie zu absorbieren, sie aufzunehmen, sich an sie anzupassen, sie zu transformieren und sich von ihnen zu erholen, auch durch die Erhaltung und Wiederherstellung ihrer wesentlichen Grundstrukturen und -funktionen durch Risikomanagement."[374]

Spezifischer auf die Fragen sozialer Aspekte bei Katastrophen lässt sich auch die soziale Resilienz in drei inzwischen bereits vertraut erscheinende Aspekte unterteilen:[375] Als erstes die Fähigkeit der Gesellschaft eine Katastrophe durch Anpassung einzudämmen und sie durch flexible Reaktion zu ertragen. Zweitens sich von einem durch die Katastrophe ausgelösten Tiefpunkt der Funktionalität der Gesellschaft wieder zu erholen. Und schließlich aus der Katastrophe und den Konsequenzen in konstruktiver Weise zu lernen um künftig (noch) resilienter zu werden.[376] Als wesentliche (positive) Resilienzfaktoren werden insoweit ein starkes Zusammengehörigkeitsgefühl der Gesellschaft, eine gemeinsame Weltanschauung, vertrauensgetragene Führung sowie ziviles Engagement und aktive Öffentlichkeitsbeteiligung genannt.[377]

Zunehmend verbreitet sind auch sehr übergreifende Ansätze, eine Nation bzw. eine Gesellschaft als Gesamtsystem möglichst resilient zu gestalten, indem sie (präventiv) so gestaltet wird, dass menschliche, ökonomische und ökologische Schäden durch widrige Ereignisse bestmöglich vermieden werden können.[378]

374 UNDRR (vormals: UNISDR), https://www.undrr.org/terminology/resilience, zuletzt abgerufen am 12.04.2024.

375 *Elran*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 291 (294 f.).

376 Siehe hierzu auch *Berkes*, Nat Hazards, Vol. 41 (2007), 283 (287).

377 *Elran*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 291 (295 f.).

378 *Cutter et al.*, Environment: Science and Policy for Sustainable Development 2013, 25; ähnlich auch: Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022, 08.12.2017, S. 516, Kap. 6.2; vgl. auch: OECD, Concepts and dilemmas of State building in fragile situations, 2009, S. 17 f, wobei der resiliente Staat hier als positiver Gegenpol zum fragilen Staat angesehen und sich vor allem durch einen funktionierenden Gesellschaftsvertrag (en: social contract) zwischen Staat und Gesellschaft auszeichnet. Letzteres wird insbesondere dann angenommen, wenn der Staat in der Lage ist die gesellschaftlichen Erwartungen an ihn zu erfüllen.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

e. IT-Sicherheitsrecht

Im Nachfolgenden soll auf Anforderungen aus dem IT-Sicherheitsrecht i.w.S. eingegangen werden. Dabei wird zunächst eine allgemeine Einführung mit der Verwendung des Resilienzbegriffs nicht nur in europäischen Gesetzen, sondern insbesondere auch bereits zuvor in Politikansätzen und Strategien der EU-Kommission gegeben (i.). Anschließend wird konkret auf die (sofern vorhandenen) Definitionen der Resilienz im (RegE) BSIG und der NIS(2)-RL, dem RefE KRITIS-DachG, dem IT-Sicherheitsgesetz für Banken: DORA[379] und dem die Agentur der EU für Cybersicherhit (ENISA) einrichtenden CSA[380] eingegangen (ii-v). Schließlich folgt noch ein internationaler Blick auf die Definitionen in (IT-)Sicherheitsstrategien aus der Schweiz und den USA (vi.-vii.).

i. Einführung

Der Begriff der Resilienz ist zumindest im europäischen Kontext der IT-Sicherheit an sich nicht unbekannt. Bereits seit 2007 wird der Begriff „Resilienz" von der EU-Kommission in diesem Kontext regelmäßig verwendet.[381] Die Tätigkeit der EU-Kommission in dem Bereich der europäischen IT-Sicherheit lässt sich schon auf das Jahr 2001 zurückführen,[382] in der die Europäische Kommission einen Vorschlag für einen europäischen Politikansatz im Bereich der Sicherheit der Netz- und Informationssysteme einbrachte.[383] Das Ziel der „Erhöhung der Sicherheit und der Widerstandsfähigkeit" (en: resilience) wurde dann 2006 mit der Strategie für eine sichere Informationsgesellschaft noch wenig prominent eingeführt.[384] Die darauf folgende, stärkere Positionierung des Resilienzbegriffs wird u.a. auf die Cyber-Angriffe in Estland 2007 zurückgeführt, die gewissermaßen zu einem Weckruf in der EU geführt haben.[385] Denn an diesem jenseits der finanziellen Schä-

379 EU-VO 2022/2554, Digital Operational Resilience Act.
380 EU-VO 2019/881, Cyber Security Act, Cybersecurity Act.
381 *Dewar*, The European Union and Cybersecurity, S. 173.
382 *Dewar/Dunn Cavelty*, in: Schünemann/Kneuer, E-Government und Netzpolitik im europäischen Vergleich, 281 (283).
383 EU-Kommission, KOM (2001) 298 endgültig, 06.06.2001.
384 EU-Kommission, KOM(2006) 251 endgültig, 31.05.2006, S. 7; s. auch Entschließung d. europäischen Rates, EU-ABl. 2007 C 68/3.
385 *Dewar*, The European Union and Cybersecurity, S. 166 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

den[386] an sich nicht sehr folgenschweren Angriff zeigte sich exemplarisch die immer stärker werdende Abhängigkeit von Netz- und Informationssystemen und zwar sowohl mit Blick darauf, dass die Auswirkungen eines Ausfalls mit der wachsenden Zahl der digitalisierten Lebensbereiche immer größer werden, als auch, dass aufgrund der technischen Interdependenz entsprechende Ausfälle in einzelnen Mitgliedsstaaten potenziell kaskadenartige Ausfälle in ganz Europa auslösen können.[387]

Zum Schutz des europäischen Binnenmarktes[388] sollten die entsprechenden Infrastrukturen in Anbetracht solcher Ereignisse daher möglichst resilient ausgestaltet sein. Ausdrücklich definiert wird „Resilienz" in diesem Zusammenhang jedoch nicht. Zumindest Anhaltspunkte liefert die Cybersecurity-Strategie 2013, die der „Cyber Resilience" einen eigenen Abschnitt widmet:[389] Demnach kann diese insbesondere dazu dienen, „grenzübergreifende Risiken und Bedrohungen einzudämmen und in Notfällen auf koordinierte Weise zu reagieren." Besonders hervorgehoben werden mit Blick auf Sicherheitsvorfälle koordinierte Prozesse zur „Prävention, Erkennung, Folgenminderung und Reaktion", einschließlich der Ermöglichung eines europaweiten Informationsaustauschs. Auch der private Sektor selbst sollte seine Resilienz gegenüber Cyberangriffen stärken. In diesem Zusammenhang wird die „Reaktion auf Sicherheitsvorfälle, die Ermittlung der Ursachen und die Durchführung [retrospektiver] cyberforensischer Untersuchungen" genannt. Im Kontext der Cyberverteidigungspolitik wird die Resilienz von Kommunikations- und Informationssystemen in diesem Dokument außerdem mit der „Erkennung komplexer Cyberbedrohungen, der Reaktion darauf und der Wiederherstellung danach" assoziiert.[390]

An diesem Punkt lässt sich bereits festhalten, dass Resilienz Bewältigungsmethoden für Sicherheitsvorfälle umschreibt: Hierzu können insbesondere deren möglichst frühzeitige Erkennung, die Reaktion während des Vorfalls sowie die Minimierung der Folgen bzw. die Wiederherstellung

386 *M. Schmidt*, Cyberkrieg gegen Estland macht Westen ratlos, Tagesspiegel vom 30.05.2007 in: Tagesspiegel, 30.05.2007.

387 *Dewar*, The European Union and Cybersecurity, S. 172.

388 Für den Bereich der nationalen Sicherheit, zu der man diese Frage sicherlich auch zählen könnte, fehlte der EU die Kompetenz; der EU-Cybersicherheit liegt daher ein sozio-ökonomisches Verständnis mit Fokus auf den Schutz der europäischen Wirtschaft zugrunde. s. *Dewar*, The European Union and Cybersecurity, S. 175 ff.

389 EU-Kommission, JOIN(2013) 1 final, 07.02.2013, Kap. 2.1, S. 5 ff; in der deutschen Fassung: „Widerstandsfähigkeit".

390 EU-Kommission, JOIN(2013) 1 final, 07.02.2013, Kap. 2.3, S. 13; in der deutschen Fassung: „Robustheit".

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

gezählt werden. Ein hoher Stellenwert wird dabei auch organisatorischen Aspekten wie der Zusammenarbeit der beteiligten Akteure zur Vermeidung der Ausbreitung von Sicherheitsvorfällen eingeräumt, so dass der Begriff auf das soziotechnische Gesamtsystem abzielt und nicht auf (einzelne) IT-Systeme beschränkt bleibt.

ii. RegE BSIG und NIS2-RL

Im deutschen IT-Sicherheitsrecht, insbesondere in § 30 RegE BSIG (wie auch dem damit umgesetzten Art. 21 NIS2-RL) ist das Erfordernis der Resilienz noch nicht eingeführt. Gleiches gilt für die Sicherheitsdefinitionen nach § 2 Nr. 36 RegE BSIG, Art. 6 Nr. 1 NIS2-RL.

Allerdings finden sich einige Erwähnungen der Resilienz: So findet sich z.B. in § 51 RegE BSIG die aus Art. 28 der NIS2-RL übernommene Vorgabe: „Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, sind Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister verpflichtet, genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu sammeln und zu pflegen."

Daneben findet sich v.a. in der NIS2-RL noch eine Vielzahl weiterer Erwähnungen, allerdings ohne ein definiertes Begriffsverständnis zu ermöglichen: So würde etwa die Schwachstellendatenbank der ENISA die Resilienz erhöhen (EG 63), die Resilienz der Lieferkette von IKT-Diensten, -Systemen und -Produkten müsse sichergestellt werden (EG 91) und Meldungen über Vorfälle müssten hinreichend detailliert sein, damit andere Einrichtungen daraus wichtige Lehren ziehen und ihre Resilienz erhöhen könnten (EG 101).[391]

Diese inhaltlich wenig detaillierte Verwendung des Resilienzbegriffs in der NIS2-RL überrascht insoweit besonders, da laut EG 2 derselben seit Inkrafttreten der NIS-RL „erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden."

391 Weitere Erwähnungen finden sich in EG 2, 5, 55, 85, 100, 109 sowie Art. 7 Abs. 2 lit i) NIS2-RL. Auch in der NIS-RL wurde die Resilienz bereits in EG 13 und Art. 9 Abs. 3 genannt; im BSIG hingegen bislang nicht.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

iii. RefE KRITIS-DachG

Weiterhin ist der Referentenentwurf des KRITIS-DachG, mit dem die europäische RL 2022/2557 über die „Resilienz kritischer Einrichtungen" (RKE-RL) umgesetzt werden soll, zu berücksichtigen. Dieses Gesetz soll zwar nicht der Gewährleistung der IT-Sicherheit, sondern der physischen Sicherheit dienen – dabei aber gleichwohl zu den Regelungen der IT-Sicherheit eine „größtmögliche Kohärenz" erreichen,[392] so dass sich dieses Gesetz hier als weiterer Ansatzpunkt auch für die Auslegung der Resilienz in der Datensicherheit anbietet.

Nach § 2 Nr. 5 RefE KRITIS-DachG umfasst Resilienz „die Fähigkeit eines Betreibers kritischer Anlagen, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen;" Ein Vorfall ist nach § 2 Nr. 9 RefE KRITIS-DachG „ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich stört oder stören könnte."

In § 10 Abs. 1 RefE KRITIS-DachG werden die einzelnen Resilienzmaßnahmen genannt, wobei die Elemente nach § 2 Nr. 5 konkretisiert und ergänzt werden. Darüber hinaus enthält Anhang 1 praktische Resilienzmaßnahmen und nennt unter anderem Notfallvorsorge, Maßnahmen des Objektschutzes (Zäune, Sperren), Zugangskontrollen i.V.m. Personaleinteilungen nach Kritikalität der wahrgenommenen Funktion und entsprechenden Zugangsrechten sowie Sensibilisierungen des Personals.

Im Ergebnis soll Resilienz demnach Störungen der kritischen Dienstleistung (etwa der Wasserversorgung) mit Blick auf die Sicherheit der Anlagen (jenseits der IT-Sicherheit) möglichst ausschließen. Dabei wird laut Entwurfsbegründung mit der Pflichtennorm des § 10 RefE KRITIS-DachG ein „risikobasierter All-Gefahren-Ansatz beim Ergreifen von Maßnahmen zur Stärkung der Resilienz verfolgt."[393]

392 BMI, Referentenentwurf zum KRITIS-DachG, 21.12.2023, S. 1 f.
393 BMI, Referentenentwurf zum KRITIS-DachG, 21.12.2023, S. 60 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

iv. Digital Operational Resilience Act (DORA)

Im Finanzsektor besteht innerhalb des IT-Sicherheitsrechts der Digital Operational Resilience Acts (DORA) als lex specials gegenüber dem RegE BSIG bzw. der NIS2-RL.[394]

Im DORA ist „digitale operationale Resilienz" in Art. 3 Nr. 1 definiert als „die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es […] das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, zu unterstützen."

Festzuhalten ist zunächst, dass Resilienz auch hier als (aktive) Fähigkeit verstanden wird. Inhaltlich werden hierunter alle IKT-bezogenen Fähigkeiten zur Gewährleistung der Sicherheit der Netzwerk- und Informationssysteme erfasst. Damit ermöglicht diese Definition allerdings keine inhaltliche Konturierung der Resilienz; vielmehr wird insofern eher ein Gleichlauf mit dem IT-Sicherheitsbegriff in dem Sinne geschaffen, dass alle Maßnahmen (insbesondere auch das IKT-Risikomanagement, Art. 5 Abs. 1 DORA) auf eine Erhöhung der Resilienz und auf die Gewährleistung von IT-Sicherheit einzahlen, so dass kein eigenständiger Anwendungsbereich für die Resilienz verbleibt. Allerdings werden in den Art. 10 (Erkennung) Art. 11 (Reaktion und Wiederherstellung) und Art. 13 (Lernprozess und Weiterentwicklung) auch spezifische, dem Resilienzkonzept zuordnungsfähige Aspekte beschrieben.

v. Cybersecurity-Act (CSA)

Eine weitere wesentliche Entwicklung der Resilienz findet sich im Cyber-Security-Act (CSA), der ebenfalls zum IT-Sicherheitsrecht gezählt werden kann.[395] In EG 2 wird festgestellt, dass insbesondere im Bereich IoT „die Sicherheit und Abwehrfähigkeit [eng.: security and resilience] dieser Geräte

394 Siehe EG 28 NIS2-RL.

395 Diese europäische Verordnung (2019/881) regelt die Befugnisse der Agentur der Europäischen Union für Cybersicherheit (ENISA). Zu deren Aufgaben gehört es nach EG 24, 25 insbesondere die Umsetzung der NIS-RL zu unterstützen.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

schon bei der Konzeption [bislang] nicht ausreichend berücksichtigt wurden". Mithin wird Resilienz hier nun auch von der Makroebene komplexer Netz- und Informationssysteme auf einzelne IoT-Geräte herunterskaliert. Ungeachtet dessen wird der Resilienzbegriff aber auch hier auf höherer Ebene verwendet, etwa in Bezug auf einzelne Mitgliedsstaaten oder die europäische Union; auf dieser Makroebene sollen die Mitgliedsstaaten demnach insbesondere einen strukturierten Informationsaustausch über Cybersicherheitsrisiken und Maßnahmen pflegen, um nationale Kapazitäten und abgestimmte Verfahren aufzubauen und so im Ergebnis die Resilienz insgesamt zu stärken.[396]

vi. Strategie zum Schutz kritischer Infrastrukturen (Schweiz)

Auch in anderen Ländern wird Resilienz bereits im Kontext der Sicherheit einschließlich der IT-Sicherheit kritischer Infrastrukturen als regulatorischer Begriff verwendet: In der Schweiz ist Resilienz als Bestandteil der vom Schweizerischen Bundesrat beschlossenen „Nationale[n] Strategie zum Schutz Kritischer Infrastrukturen" genannt und anders als im europäischen Rechtsrahmen auch schon mit einer feststehenden Definition ausdifferenziert: Demnach seien kritische Infrastrukturen in der Zielvorstellung resilient, wenn „großflächige und schwerwiegende Ausfälle möglichst verhindert und die Funktionsfähigkeit im Ereignisfall möglichst rasch wieder gewährleistet werden kann."[397] Hierfür wird Resilienz definiert als „die Fähigkeit eines Systems, […] intern oder extern verursachten Störungen zu widerstehen (Widerstandsfähigkeit) und die Funktionsfähigkeit möglichst zu erhalten (Anpassungsfähigkeit) respektive möglichst schnell und vollständig wiederzuerlangen (Regenerationsfähigkeit)."[398]

396 EG 39 CSA; siehe zur Skalierbarkeit des Resilienzbegriffs auch: *Björck et al.*, in: New Contributions in Information Systems and Technologies, Cyber Resilience - Fundamentals for a Definition, 311 (312); *Bodeau/Graubart,* Cyber Resiliency Engineering Framework, Sep. 2011, S. 37.

397 Grundlegend: Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022, 08.12.2017, S. 515 f.

398 Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen, 16.06.2023, S. 3; Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022, 08.12.2017, S. 515 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

vii. Strategic Plan 2023-2025 (USA)

In den USA hat sich der Begriff seit mehreren Jahren als prominenter Begriff im Bereich des Schutzes kritischer Infrastrukturen etabliert.[399] So spricht auch die Strategie der Cybersecurity and Infrastructure Security Agency (CISA)[400] für die Jahre 2023-2025 von Risikoreduktion und Resilienzstärkung an Amerikas kritischer Infrastruktur.[401] „Dabei wird Resilienz als die Fähigkeit definiert, sich auf veränderte Bedingungen vorzubereiten und sich an sie anzupassen. Das bedeutet, dass die kritische Infrastruktur in der Lage sein muss, Störungen, vorsätzlichen Angriffen, Unfällen oder natürlich auftretenden Bedrohungen oder Zwischenfällen standzuhalten und sich schnell davon zu erholen. Eine resiliente Infrastruktur muss demnach auch robust, agil und anpassungsfähig sein."[402] Demgegenüber wird Sicherheit (Security) definiert als die „Reduktion von Risiken für kritische Infrastrukturen durch Eindringen, Angriffe oder die Auswirkungen von Naturkatastrophen oder vom Menschen verursachten Katastrophen durch den Einsatz von physischen Mitteln oder defensiven Cyber-Maßnahmen."[403]

Hieran zeigt sich, dass die Gewährleistung von Resilienz von der Risikoreduktion im Rahmen der IT-Sicherheit zu unterscheiden ist. Dieser Differenzierung wird später im Rahmen der systematischen Auslegung noch weiter nachgegangen. Im Übrigen lassen sich auch hier ähnlich der Schweizer KRITIS-Strategie die Elemente des Widerstands, der Anpassung an und der Erholung nach einem Ereignis isolieren.[404]

---

399 Teilweise wird er auch als „Ersatz" für den Begriff des Schutzes kritischer Infrastrukturen verstanden: *Fekete/Grinda/Norf*, in: Wink, Multidisziplinäre Perspektiven der Resilienzforschung, 215 (222).

400 Die CISA ist in den USA eine Bundesbehörde und zugleich Teil des Ministeriums für innere Sicherheit (en: Department of Homeland Security), siehe auch: https://www.dhs.gov/topics/cybersecurity, zuletzt abgerufen: 19.04.2024.

401 CISA, Strategic Plan 2023-2025, Sep. 2022, S. 16 ff.

402 Original (en): "Resilience may be defined as the ability to prepare for and adapt to changing conditions. This means being able to withstand and recover rapidly from disruptions, deliberate attacks, accidents, or naturally-occurring threats or incidents. Resilient infrastructure must also be robust, agile, and adaptable."; CISA, A Guide to Critical Infrastructure Security and Resilience, Nov. 2019, S. 11.

403 Original (en): "Security may be defined as reducing the risk to critical infrastructure from intrusions, attacks, or the effects of natural or man-made disasters, through the application of physical means or defensive cyber measures." CISA, A Guide to Critical Infrastructure Security and Resilience, Nov. 2019, S. 11.

404 Siehe zu diesen Elementen ausführlicher auch schon: NIAC, Critical Infrastructure Resilience, 08.09.2009, S. 12 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

viii. Fazit

Insgesamt bleibt der Begriff Resilienz im europäischen und nationalen IT-Sicherheitsrecht eher unscharf und für die Ermittlung eines präzisen Wortlautverständnisses ungeeignet. Zu häufig wird er als Schlagwort im Rahmen der Gewährleistung von IT-Sicherheit und (Cyber)resilienz verwendet.

In der DORA zeigt sich mit der Definition der „digitalen operationalen Resilienz" eine weitgehende Gleichsetzung von Resilienz und IT-Sicherheit. Gleichzeitig werden aber zumindest auch resilienzspezifische Maßnahmen (Erkennung, Reaktion und Wiederherstellung sowie einen Lernprozess) verlangt. Der CSA fordert in Art. 1 Abs. 1 zwar sowohl „ein hohes Niveau" der Cybersicherheit als auch der Cyber-Resilienz (zit: „Fähigkeit zur Abwehr von Cyberangriffen", eng.: cyber resilience), definiert letztere aber nicht. Mit diesem Schlagwort bestimmt der EU-Gesetzgeber folglich nur ein übergreifendes Ziel, das anzustreben und bei dessen Erreichen gleichsam die Sicherheit gewährleistet sei. In eben diese Richtung weist auch der CRA-E, der eine horizontale Regelung zur IT-Sicherheit von Produkten darstellt, aber trotz der Resilienz im vorgesehenen Gesetzestitel und mehrfacher Nennung im Gesetzestext als auch in den Erwägungsgründen diesen Begriff in keiner Weise inhaltlich nutzbar macht.

Ähnlich verhält es sich auch mit der NIS2-RL, dem RegE BSIG und dem RefE KRITIS-DachG. Letzterer liefert zwar eine Methodendefinition, die erneut auch mögliche Resilienzelemente wie die Reaktion auf Vorfälle oder die Folgenbegrenzung sowie die Erholung von Vorfällen beinhaltet; sie bezieht sich aber im Übrigen v.a. auf ein klassisches, risikobasiertes Vorgehen (§ 10 Abs. 1 S. 2 RefE KRITIS-DachG) und umfasst insbesondere auch typische Sicherheitsaspekte wie etwa den Objektschutz durch Zäune und Sperren. Dadurch schafft diese Definition nicht die nötige Abgrenzung zum bisherigen Sicherheits- oder Schutzbegriff. Stattdessen wird Resilienz hier erneut als konsumierender Oberbegriff -in diesem Fall für die physische Sicherheit- verwendet.

Einen etwas anderen Blickwinkel liefert hingegen die Schweizer KRITIS-Strategie sowie der Strategieplan der US-amerikanischen CISA. Hier wird zum einen eine präzise Definition mit unterschiedlichen Teilaspekten der Resilienz als auch im Strategieplan der CISA sogar eine definitorische Abgrenzung zur IT-Sicherheit geliefert. Diese Aspekte können die Wortlautauslegung somit entscheidend bereichern.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Synthese

Auf Basis der beschriebenen Begriffsverständnisse und den dahinterstehenden Konzepten der Resilienz in den unterschiedlichen Domänen erfolgt nun die Synthese derselben für das Wortlautverständnis der Resilienz als Rechtsbegriff in der Datensicherheit. Insgesamt zeigte sich die Resilienz als Begriff sehr universell und lässt sich auf verschiedenste Objekte (Materialien, Menschen, Ökosysteme, kritische Infrastrukturen) beziehen. Das Nationale Institute of Standards and Technologie (NIST) weist dementsprechend verschiedene Definitionen für Resilienz aus, je nachdem auf welches Objekt sie sich bezieht.[405] Für die Auslegung des Resilienzbegriffs ist folglich zu beachten, dass dieser nach Art. 32 Abs. 1 lit b) DSGVO neben Diensten insbesondere auf Systeme bezogen wird. Insofern liegt es nahe jenen Verständnissen der Resilienz ein gesteigertes Gewicht in der Synthese einzuräumen, die sich ebenfalls auf die Resilienz von Systemen beziehen.

In den Bereichen der IT-Sicherheit, der kritischen Infrastrukturen sowie dem Katastrophenschutz zeigte sich außerdem spezifischer, dass die entsprechenden Verständnisse und Definitionen ein *soziotechnisches System* voraussetzen. Dabei war insbesondere festzuhalten, dass die Resilienz sich hier nicht auf das technische System beschränken darf, sondern die Mitarbeitenden miteinbezogen werden müssen, um etwa nach einem technischen Zwischenfall eine gewisse Ordnung aufrechtzuerhalten, die Schadensausbreitung zu vermindern oder ggf. auch Maßnahmen zur Wiederherstellung einzuleiten.[406] Ihnen kommt insoweit anders als den meisten technischen Systemen die Fähigkeit zu, sich angesichts von überraschenden Vorfällen adaptiv zu verhalten.[407] Auf den Aspekt des soziotechnischen Systemverständnisses der Resilienz wird in der systematischen Auslegung mit Blick auf den Systembegriff in Art. 32 Abs. 1 lit b) DSGVO noch zurückzukommen sein.

Hinsichtlich der Auslegung des Resilienzbegriffs als solchem bildet zunächst gleichwohl der psychologische Resilienzbegriff als die prägende

405 Dort u.a. für Systeme, Organisationen oder Nationen; *Ross et al.,* Developing cyber resilient systems, 2019, S. 71 f.; ähnlich auch: *Björck et al.*, in: New Contributions in Information Systems and Technologies, Cyber Resilience - Fundamentals for a Definition, 311 (312).

406 Vgl. auch: *Gazos*, in: Polarisierte Welten: Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie, Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen, S. 4.

407 Wie zuvor.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Domäne das Fundament für die weitere Bestimmung. Er offeriert ein grundlegendes Verständnis, indem er die erfolgreiche Anpassung an bzw. die Erholung nach widrigen Lebensumständen adressiert. Mit Blick auf die Unabdingbarkeit der Konfrontation mit widrigen Lebensumständen wird der Charakter des Konzepts deutlich, nachdem Gegenstand der Resilienz jedenfalls nicht die Vermeidung bzw. der Ausschluss der schädigenden Ereignisse als solcher sein kann. Vielmehr gilt es nach diesem Verständnis der Resilienz solche unvermeidbaren, „umweltbedingten Risikoerfahrungen" und insbesondere deren „erwartete Folgen" möglichst gut zu bewältigen.[408] Dieses Definitionsmerkmal als *Umgang mit unvermeidbaren, widrigen Ereignissen*[409] ließe sich auch uneingeschränkt auf die deutsche Übersetzung „Belastbarkeit" übertragen, da dieser Begriff impliziert, dass das Auftreten von Belastungen nicht verhindert werden kann und diese somit ausgehalten werden müssen.[410] Weiterhin lässt sich abstrahierend festhalten, dass bestimmte Faktoren die entweder an dem Subjekt (hier dem System) ansetzen oder sich aus dessen Verhältnis zu seiner Umgebung ergeben, die Resilienz als Ergebnis begünstigen oder schwächen. Diese Faktoren könnten in der Datensicherheit durch Maßnahmen beschrieben bzw. ausgefüllt werden. Gleichzeitig sollte wie in der Psychologie davon ausgegangen werden, dass die Resilienz stets nur eine Momentaufnahme ist und nicht als statische Eigenschaft einem Subjekt per se anhaftet.[411] Schließlich dürfte auch die Steigerung der Resilienz durch einen „Abhärtungseffekt" in der Erholungsphase, bei dem aus den bisherigen Ereignissen gelernt wird, für die Datensicherheit ein wesentlicher Baustein sein.

Weiterhin gibt der ökologische Resilienzbegriff entscheidende Impulse für das Verständnis von Resilienz: Zunächst ist die Anpassungsphase in der Ökologie besonders charakteristisch. Hierbei wird auf die Fähigkeit zur Einnahme *qualitativ verschiedener Zustände* abgestellt und weniger auf eine Rückkehr zu einem primären, stabilen Zustand, wie es das technische Verständnis propagiert.[412] Dies lässt sich auf informationstechnische Systeme und Dienste allerdings nur bedingt übertragen, da auch hier zwar ein

408 *Rutter*, Development and psychopathology 2012, 335 (336); *Bröckling,* Resilienz: Über einen Schlüsselbegriff des 21. Jahrhunderts, 2017, S. 8.

409 Vgl. in diesem Sinne im Datenschutzrecht bereits: DSK, Standard-Datenschutzmodell, B.1.19, S. 22; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39.

410 *Bröckling,* Resilienz: Über einen Schlüsselbegriff des 21. Jahrhunderts, 2017, S. 8.

411 *Park et al.*, Risk analysis 2013, 356 (359).

412 Vgl. *Davoudi*, Planning Theory & Practice 2012, 299 (300 f.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

abweichender Zustand z.B. in Form eines Notfallmodus möglich und ggf. sogar sinnvoll erscheint, das mittel- bis langfristige Ziel aber in der Regel die Rückkehr zu einem „Normalzustand" und dem eigentlichen Leistungsprogramm ist.[413] Eine gewissermaßen freie evolutionäre Anpassung ist bei IT-Systemen und Diensten insoweit kaum möglich. Technische Systeme sind anders als ökologische Systeme Ausdruck einer menschlichen Intention und sind somit dahingehend konzipiert einen bestimmten Dienst zu erbringen,[414] wovon sie nicht ohne weiteres transformatorisch abweichen können und sollen.[415] Somit ist insgesamt ein Verständnis der Resilienz anzuwenden, wie es in anthropozentrischen Resilienzverständnissen wie der technischen Resilienz (mit Blick auf den Menschen auch in der Psychologie) und innerhalb der Ökologie allenfalls noch in der Klima(schutz)forschung zugrunde liegt, bei dem nur ein intendierter, stabiler Zustand des Systems bzw. des Dienstes als Maßstab für die Resilienz vorliegt. Eine evolutionäre Anpassung ist bei der Resilienz als Datensicherheitsprinzip nur insoweit möglich, als dass moderne IT-Systeme möglichst autonom aus Ereignissen lernen und sich optimierend anpassen sollen, um künftig besser auf solche vorbereitet zu sein.[416] Aber dieser Prozess bleibt auf die Sicherheit der Systeme und Dienste beschränkt. Dass sich IT davon unabhängig z.B. an geänderte Nutzeranforderungen anpassen soll, ist jedenfalls kein Aspekt der Resilienz im Kontext der Datensicherheit.

Darüber hinaus ist der Aspekt der *quantitativen Resilienz* zu beachten, der in der Ökologie in Form von schwankenden Populationsgrößen auftritt. Dieser Aspekt lässt sich für die Informationstechnik in dem Sinne nutzbar machen, dass ein System in der Lage sein soll bei einem widrigen

413 „You want your computer to bounce back and do what it was designed to do." *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (265 f.). Gleichzeitig weist *Longstaff* aber auch auf die bestehende Tendenz hin, technische Systeme stärker nach ökologischem Vorbild zu gestalten.

414 Vgl. *Park et al.*, Risk analysis 2013, 356 (357), die insoweit ebenfalls attestieren, dass zwischen der Anwendung des Resilienzbegriffs auf ökologische bzw. technische Systeme differenziert werden muss, da nur letztere eine Intentionalität (nach hiesigem Verständnis: die Erbringung eines bestimmten Dienstes) aufweisen.

415 Vgl. *Heeks/Ospina*, ISJ (Information Systems Journal) 2019, 70 (72) mit Verweis auf ihre Literaturrecherche zur Resilienz bei Informationssystemen, nach der die überwiegende Mehrheit der untersuchten Literatur eine Wiederherstellung der Systemleistung (bounce back) anstrebt, eine fortentwickelnde Anpassung (bounce forward) konnte hingegen nur in 3 Literaturquellen gefunden werden.

416 Vgl. mit englischer Bezeichnung „Evolvability", welche als Teil der Resilienz kontinuierliches Lernen und Optimieren beschreibt: *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (11); *Ratasich et al.*, IEEE Access 2019, 13260 (13271).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ereignis zu schwanken, d.h. seine Leistung in Form des Dienstangebots graduell abzusenken, aber nach Möglichkeit ein schlagartiges und vollständiges Ausfallen des Dienstes zu verhindern.

Ebenso ist die Vorstellung von *Grenzen der Resilienz* sowohl aus dem ökologischen als auch dem technischen Verständnis transferfähig: Unabhängig davon ob es nun um das Aussterben eines multistabilen Ökosystems oder die Unmöglichkeit zur Rückkehr eines Ausgangszustands nach dem technischen Verständnis geht: Die abzuleitende Erkenntnis ist, dass das Maß an Belastungen beschrieben werden muss, mit dem ein (hier informationstechnisches) System trotz vorhandener Resilienz möglicherweise nicht mehr umgehen kann.[417] Dies wirft zugleich die noch ungeklärte Frage nach der Messbarkeit von Resilienz[418] auf, die an dieser Stelle aber nicht vertieft werden soll.

In der Informationstechnik begründen *Avizienis/Laprie u.a.* ein methodisch solides Verständnis des Resilienzbegriffs als Fehlertoleranz, d.h. dass aktiv werdende Fehler erkannt und bewältigt werden müssen, so dass sie nicht zu einem (vollständigen) Ausfall der Systemfunktion in Gestalt des Dienstes führen. Die später von *Laprie* vorgenommene Ausdehnung des Resilienzbegriffs u.a. auf die Fehlerprävention ist dagegen geeignet diese methodische Klarheit zu konterkarieren; allerdings setzt diese Ausdehnung mit der Hervorhebung einer sich verändernden Umgebung und den deshalb notwendigen Merkmalen insbesondere der Entwicklungsfähigkeit als auch der Diversität von Systemen auch für die Datensicherheit wichtige Akzente. Mit Blick auf die IT-Sicherheit erscheinen insbesondere die Merkmale der Erkennung eines Ereignisses (hier v.a. eines Angriffs), der Anpassungsfähigkeit an ein solches sowie ggf. der Wiederherstellung nach einem solchen einschließlich eines Lerneffekts zentral auch für das Verständnis in der Datensicherheit. Aus der Netzwerktechnik kann ergänzend abgeleitet werden, dass Resilienz auch bedeutet mit Ereignissen umzugehen, bei denen gar nicht bekannt ist, ob es sich um einen vorsätzlichen Angriff oder ein sonstiges Ereignis handelt (etwa im Falle des Erhalts (vermeintlich) korrumpierter Daten). Darüber hinaus folgt aus der IT-Sicherheit auch die Erkenntnis, dass Resilienz gegen ungewisse Ereignisse wie etwa neue, bislang unbekannte Angriffsformen gerichtet ist.

417 Resilienzmaßnahmen werden im Datensicherheitsrecht insbesondere auch durch das Merkmal der Angemessenheit beschränkt, siehe dazu später: S. 182 f.

418 *Heeks/Ospina*, ISJ (Information Systems Journal) 2019, 70 (72); *Zobel/Khansa*, Decision Sciences 2012, 687 (687 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Das IT-Sicherheitsrecht bietet sich als Pate für das Datensicherheitsrecht insofern an, als dass es dort ebenfalls um die staatlich vorgegebene Gewährleistung von Sicherheit in informationstechnischen Systemen zum Schutz von zumindest auch grundrechtlich geprägten Schutzgütern geht. Allerdings besteht auch hier zumeist noch keine eindeutige Legaldefinition. Als prägend für den Resilienzbegriff kann zumindest identifiziert werden, dass er Bewältigungsmethoden wie die Erkennung, die Reaktion, die Folgenminderung und die Erholung von bzw. auf Ereignisse(n) umschreibt. Dabei sind insbesondere auch die Schweizer Strategie zum Schutz kritischer Infrastrukturen sowie der Strategic Plan der *CISA* hervorzuheben, die recht eindeutig die drei Elemente der (Widerstandsfähigkeit, Anpassungsfähigkeit und Regenerationsfähigkeit) beschreiben und damit ein hohes Maß an Operationalität versprechen. Aus den Definitionen der CISA ist weiterhin zu entnehmen, dass Resilienz anders als „klassische Sicherheitsgewährleistung" nicht (unmittelbar) auf die Reduktion von Risiken gerichtet ist (ausführlich dazu auf S. 169 ff.).

Im Katastrophenschutz verdeutlicht sich schließlich noch einmal die schon in der Psychologie identifizierte Differenzierung zur Resistenz: So geht es bei Resilienz nicht mehr vorrangig darum, widrige Ereignisse zu verhindern (was insbesondere bei Naturkatastrophen oder auch Terroranschlägen naturgemäß nur begrenzt möglich ist), sondern v.a. um die Strategie im Umgang mit einem eingetretenen Ereignis.

Aus vielen der untersuchten Begriffsverständnissen wird außerdem deutlich, dass sich die Resilienz i.d.R. nicht auf die Bewältigung spezifischer Ereignisse richtet, sondern vielmehr den Blick auf das zu schützende Objekt (in der Psychologie eine Person, bei Ökologie und technischer Resilienz ein System) selbst richtet, um dieses in seiner (generellen) Bewältigungsfähigkeit gegenüber unterschiedlichsten und zumeist auch ungewissen, widrigen Ereignissen zu stärken.[419] Dieser Aspekt wird in der systematischen Auslegung bei der Abgrenzung gegenüber den klassischen, spezifischen Schutzzielen (Verfügbarkeit, Vertraulichkeit und Integrität) nochmals vertieft.

419 So mit Blick auf Ökologie, Ingenieurswissenschaft und Psychologie zur Ableitung der Resilienz im Katastrophenschutz: *Krüger/Max*, Resilienz im Katastrophenfall, S. 66.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. Fazit

Ausgehend von der zuvor dargestellten Synthese ergibt sich für die Wortlautauslegung der Resilienz in der Datensicherheit folgendes Fazit und die am Ende dieses Abschnitts dargestellte Arbeitsdefinition für die weitere Auslegung.

Aus der Synthese lassen sich insbesondere drei für die Resilienz konstituierenden Elemente identifizieren: Es wurde gezeigt, dass für die Resilienz die Fähigkeit zur Anpassung an ein (widriges) Ereignis als auch zur Regeneration nach einem solchen entscheidend sind. Beides setzt jedoch, wie auch einige der untersuchten Resilienzansätze zeigten, zunächst voraus, dass das Auftreten eines nicht vorhergesehenen (ungewissen) Ereignisses zunächst einmal von dem System möglichst frühzeitig erkannt wird („*Ereigniserkennung*").[420]

Die „*Anpassungsfähigkeit*" an ein Ereignis verfolgt das Ziel, die Auswirkungen des Ereignisses auf die Datensicherheit (z.B. auch durch manipulierte Dienste) durch adaptive Maßnahmen möglichst gering zu halten.[421] In diesem Zusammenhang ist insbesondere auch die nach dem ökologischen Verständnis wichtige Schwankungsfähigkeit zu sehen, d.h. die Möglichkeit zur graduellen Absenkung anstelle eines Totalausfalls. Die ebenfalls immer wieder genannte *Widerstandsfähigkeit* dürfte sich zumindest zum Teil als Aktives widerstehen (z.B. durch die Aktivierung redundanter Strukturen) als Unterfall bzw. Synonym der Anpassung verstehen lassen.

Schließlich erwies sich die *Fähigkeit zur Erholung* als essenziell. Dies umfasst sowohl die Wiederherstellung des ordnungsgemäßen Zustandes

420 So insbesondere bereits in der Informationstechnik, sowohl Fehler- (Verlässlichkeit) als auch Ereigniserkennung (IT-Sicherheit): Informationstechnik, S. 133 ff. ; als Merkmal der Resilienz auch bei *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 45, *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 61; als Angriffserkennungssysteme: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39; unabhängig von der Resilienz als beispielhafte Maßnahme nach Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f): EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 33.

421 Vgl. *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 42, 45; ähnlich auch: *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 26; mit in vorheriger Fußnote genannten Einschränkungen *EDSA,* wie zuvor.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

(z.B. bei der Diensterbringung) als auch die Analyse und das Lernen aus dem Ereignis,[422] um die Resilienz für die Zukunft zu verbessern.

Insgesamt lässt sich damit als Arbeitsdefinition aus der Wortlautauslegung festhalten, dass Resilienz nach dem Wortlaut *die Fähigkeit eines soziotechnischen Systems beschreibt, ungewisse Ereignisse zu erkennen, sich an diese anzupassen und sich nach einem solchen unter lernender Verbesserung schnellstmöglich zu erholen.*

III. Systematische Auslegung

Im Rahmen der systematischen Auslegung gilt es den Begriff der Resilienz gegenüber dem übrigen Art. 32 DSGVO rechtlich einzuordnen. Nach Art. 32 Abs. 1 DSGVO sind alle Maßnahmen und somit auch jene zur Gewährleistung der Resilienz auf ein „dem Risiko angemessenes Schutzniveau" auszurichten, so dass sich für die systematische Auslegung zunächst die Frage stellt, wie sich die Resilienz mit dem schon angedeuteten Fokus auf ungewisse Ereignisse gegenüber dem Begriff sowie der Methodik des Risikos positioniert (1.). Nach Art. 32 Abs. 1 lit b) DSGVO soll aber nicht nur die Resilienz, sondern auch die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sichergestellt werden. In einem zweiten Schritt ist daher die Resilienz diesen Schutzzielen gegenüberzustellen (2.)

1. Risiko

Der Risikobegriff bezieht sich nach Art. 32 Abs. 1 DSGVO auf die Schutzgüter der „Rechte und Freiheiten natürlicher Personen". Nach einer Einleitung soll der Begriff des Risikos (b.) sowie die Risikomethodik (c.) näher erläutert werden.

a. Einleitung

Das Risiko ist ein essenzieller Abwägungsfaktor bei der Wahl von toM, wozu auch die Resilienzmaßnahmen gehören. Der Normadressat hat insofern eine Entscheidung zu treffen, welche toM er auswählt, um den Norm-

422 Mit den in Fn. 420 genannten Einschränken: *EDSA,* wie zuvor.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

auftrag der Gewährleistung eines risikoangemessenen Schutzniveaus zu erfüllen. Bei dieser Entscheidung ist eine Abwägung zwischen der Risikominderung der zu ergreifenden toM und dem hierfür nötigen Aufwand (Implementierungskosten) vorzunehmen.[423] Aufgrund des zentralen Elements der Entscheidung im Rahmen dieses Normauftrags wird der Normadressat in diesem Abschnitt (1. Risiko) als *Entscheider* bezeichnet.

b. Begriffsdefinition

Eine gesetzliche Definition des Risikos enthält die DSGVO nicht. Allerdings wird der Begriff in der DSGVO in EG 75 zumindest durch die zwei Dimensionen der „Eintrittswahrscheinlichkeit" und „Schadensschwere" konturiert.[424] Auch ergibt sich aus EG 75, dass die Risiken initial stets „aus einer Verarbeitung personenbezogener Daten hervorgehe[n]". Die Eintrittswahrscheinlichkeit bezieht sich im Kontext des Art. 32 DSGVO auf den Eintritt von im Sinne der Datensicherheit unerwünschten Ereignissen und die Schadensschwere auf dessen Folgen.[425]

Für einen Risikoeintritt müssen weitere Umstände, namentlich Angriffe oder sonstige Ereignisse, das Vorhandensein von Sicherheitslücken[426] sowie ggf. das Fehlen bzw. die Unvollständigkeit von Schutzmaßnahmen[427] gegeben sein, die zu einer Beeinträchtigung von Rechten und Freiheiten natürlicher Personen führen. Da der Eintritt dieser Umstände abhängig von der oder den Eintrittswahrscheinlichkeit(en) aber nicht sicher ist, stellt der Risikobegriff stets nur eine beschreibende, antizipierende Annäherung an eine unsichere Zukunft dar.[428]

---

423 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 95, wonach zumindest kein „eklatantes Missverhältnis" bestehen darf.

424 *Bieker/Bremert*, ZD 2020, 7 (8).

425 *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 13; als „Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung" *Grages*, in: Plath, DSGVO, BDSG, TTDSG Kommentar, 4. Auflage 2023, Art. 32, Rn. 4.

426 *Grages*, in: Plath, DSGVO, BDSG, TTDSG Kommentar, 4. Auflage 2023, Art. 32, Rn. 4.

427 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (401 f.), Rn. 26.

428 Vgl. *Scherzberg*, in: Engel/Halfmann/Schulte, Wissen, Nichtwissen, unsicheres Wissen, 113 (136).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Die Datenschutzkonferenz (DSK) definiert das Risiko als

> *„das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.*"[429]

Dies deckt sich zumindest teilweise mit den rechtlichen Vorgaben. Zutreffend ist zunächst, „das Bestehen der Möglichkeit" als Ausdruck der unsicheren Zukunft an den Anfang zu stellen und insoweit mit dem Begriff der *Eintrittswahrscheinlichkeit* zu beschreiben.

Das „Ereignis" selbst sollte indes vom Schaden sprachlich getrennt bleiben. Zutreffend ist zwar, dass Ereignis und Schaden unmittelbar zusammenfallen können, etwa wenn persönliche Daten unbefugt offengelegt wurden. Nichtsdestotrotz sollte zwischen dem technischen Ereignis (also insbesondere, aber nicht ausschließlich dem „Sicherheitsvorfall") und seinen rechtlichen Auswirkungen bzw. Schäden konsequent differenziert werden. Auch ist zu beachten, dass nicht jedes Ereignis auch zu einem Schaden führt, d.h. es ist unzureichend hier nur von einer Eintrittswahrscheinlichkeit auszugehen. Vielmehr besteht eine weitere Eintrittswahrscheinlichkeit (an der ggf. auch mit Maßnahmen angesetzt werden kann), wonach das Ereignis auch einen Schaden nach sich zieht.[430]

Den Komplementärbegriff zum Risiko bildet aus soziologischer Perspektive die „Sicherheit".[431] Nach der Überschrift des Art. 32 DSGVO soll die „Sicherheit der Verarbeitung" gewährleistet werden. Da eine absolute Sicherheit im Sinne einer vollständigen Risikofreiheit per se nicht erreicht, sondern allenfalls eine (soziale) Fiktion darstellen kann,[432] reduziert Art. 32 DSGVO die Gewährleistungsanforderung sachgemäß hin zu einem risikoangemessenen Schutzniveau; d.h. die Risiken müssen um ein angemessenes Maß gemindert werden.[433]

---

429 DSK, Kurzpapier Nr. 18, 26.04.2018, S. 1.

430 Wohl ebenfalls (aber ausschließlich) auf die Eintrittswahrscheinlichkeit des Schadenseintritts abstellend: *Bieker*, DuD 2018, 27 (30 f.); vgl. außerdem: DIN, ISO/IEC 27005:2022 (EN), S. 16.

431 *Luhmann*, Soziologische Aufklärung 5, S. 128.

432 Wie zuvor.

433 Ausführlich dazu sogleich auf S. 167.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Insgesamt sollte Risiko darum definiert werden als

„die Eintrittswahrscheinlichkeit eines Ereignisses sowie eines Schadens an den Rechten und Freiheiten natürlicher Personen und dessen Schwere.“

Diese Definition soll anhand der nachfolgenden Grafik noch einmal illustriert werden:

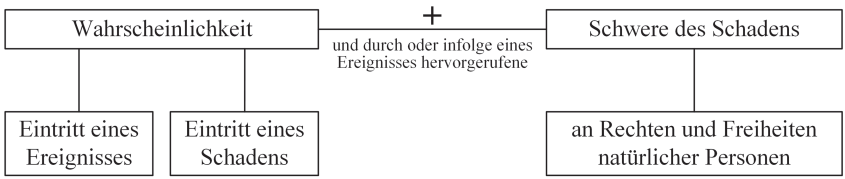

Abbildung 8: Risiko aus Wahrscheinlichkeit und Schadensschwere

Der *Begriff des Ereignisses* sollte dabei möglichst generisch verstanden werden. Er kann zwar die Verletzung des Schutzes personenbezogener Daten i.S.d. Art. 4 Nr. 12 DSGVO darstellen. Auch dieser kann aber noch ein Ereignis vorausgegangen sein, z.B. ein Fehler und damit ein Verfügbarkeitsverlust in einem System. Insofern normiert die DSGVO mit der Verletzung des Schutzes personenbezogener Daten nur einen „datenbezogenen Sicherheitsvorfall“; der system- oder dienstbezogene Sicherheitsvorfall, also eine Verletzung der diesbezüglichen Schutzziele, ist hingegen nicht ausdrücklich benannt. Seine Bedeutung als Ursache für eine Verletzung personenbezogener Daten ergibt sich aber systematisch aus Art. 32 Abs. 1 lit b) DSGVO.[434]

Entsprechend kann die voranstehend beschriebene *Kette von Ereignissen* und dem schlussendlichen Schaden erweitert werden, z.B. Manipulation im System (Wahrscheinlichkeit a) führt mit Wahrscheinlichkeit b) zu einer Veränderung personenbezogener Daten, was mit Wahrscheinlichkeit c) zu bestimmten Schäden an den Rechten und Freiheiten natürlicher Personen (EG 75, z.B. finanzieller Verlust) führt. Somit können Risiken tiefgreifend antizipiert und abgeschätzt werden. In der Praxis werden insbesondere auch für eine granularere Darstellung der Eingriffe in informationstechnische Systeme sog. Angriffsbäume verwendet.[435]

434 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (403), Rn. 30.
435 *Liedtke*, Informationssicherheit, S. 176; *Schneier*, Dr. Dobb's journal, Vol. 24 (1999), Heft 12, 21 (21 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Daraus wird außerdem deutlich, dass sich das Risiko mit dem Eintritt des Ereignisses der Verletzung des Schutzes personenbezogene Daten häufig noch nicht endgültig realisiert hat. Vielmehr führt die extensive Auslegung des Risikobegriffs dazu, dass sich das Risiko erst dann endgültig verwirklicht hat, wenn infolge des Ereignisses auch ein Schaden in seiner finalen Ausprägung an den Rechten und Freiheiten natürlicher Personen eingetreten ist.

c. Methodik

Die Identifikation, die Analyse und die ggf. vorzunehmende Behandlung von Risiken bedarf weiterhin einer bestimmten Methodik, die als „Risikomanagement" bezeichnet wird.[436]

i. Einleitung

In Art. 32 DSGVO ist ein Risikomanagement zunächst nicht explizit vorgeschrieben.[437] Allerdings ist es im Rahmen einer sog. Risikofolgenabschät-

436 *Bieker/Bremert*, ZD 2020, 7 (8); ähnlich auch DSK, Standard-Datenschutzmodell, S. 49; weisen insofern daraufhin, dass der Begriff „Risikomanagement" im Unternehmensbereich an sich eine Methodik meint, um Risiken für ein Unternehmen auf ein aus dessen Sicht annehmbares Maß zu reduzieren, was insbesondere von der jeweiligen Risikoaffinität des Unternehmens abhängt. Der Begriff wird in dieser Untersuchung davon insofern abweichend verwendet, als dass die Methodik nach hiesigem Verständnis stets auf das Ziel einer rechtlich unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes angemessenen Risikoreduktion gerichtet ist. Außerdem ist Risikoobjekt insofern nicht das ggf. als Verantwortlicher operierende Unternehmen, sondern die durch die DSGVO geschützte betroffene Person; vgl. *F. Thoma*, ZD 2013, 578 (578 f.); ähnlich auch *Heinemann*, in: Moos/Arning/Schefzig, Die neue Datenschutz-Grundverordnung, 463 (466 f.), Rn. 10-13.

437 Ob ein solches Risikomanagement insbesondere auch mit Blick auf die erforderliche Risikobeurteilung (siehe hierzu: *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 24 ff.) sowie das Erfordernis der regelmäßigen Überprüfung, Bewertung und Evaluierung nach Art. 32 Abs. 1 lit d) DSGVO trotzdem bei Anwendung des Art. 32 Abs. 1 stets erforderlich ist, kann an dieser Stelle dahingestellt bleiben. Es spricht jedoch aufgrund der genannten Anforderungen einerseits viel dafür; mit Blick auf die Verhältnismäßigkeit gerade bei sehr kleinen Unternehmen oder Selbstständigen sind jedoch andererseits auch Zweifel angezeigt, ob wirklich ein Risikomanagement im hier verstandenen Sinne durchgeführt werden muss (oder ob es ggf. nicht auch hinreichend ist, wenn nur

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zung nach Art. 35 DSGVO auch hinsichtlich der Datensicherheit vorgesehen.[438] Somit findet ein Risikomanagement (auch) hinsichtlich der Datensicherheit jedenfalls dann statt, wenn die Voraussetzungen einer Risikofolgenabschätzung nach Art. 35 DSGVO (voraussichtlich hohes Risiko der Verarbeitung (Art. 35 Abs. 1) oder Erfüllung eines Regelbeispiels nach Art. 35 Abs. 3) gegeben sind. Bei den hier gegenständlichen digitalen Diensten dürfte dies regelmäßig bereits aufgrund des für die Personalisierung vorgenommenen Profilings der Fall sein.[439]

Inhaltlich wird das Risikomanagement wie folgt konturiert: Nach Art 35 Abs. 7 DSGVO sind insbesondere die Verarbeitungsvorgänge zu beschreiben, die daraus resultierenden Risiken zu bewerten und durch entsprechend vorzusehende Abhilfemaßnahmen zu bewältigen. Auch die Erwägungsgründe 77 und 90 DSGVO zeichnen ein solches Risikomanagement vor, in denen u.a. dem europäischen Datenschutzausschuss (EDPB)[440] die Verfassung entsprechender Leitlinien nahegelegt wird. Demnach ist das mit der Verarbeitung verbundene Risiko zunächst zu *ermitteln*, anschließend in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere *abzuschätzen* und schließlich entsprechend *einzudämmen*.

Darüberhinausgehend lässt die DSGVO offen, anhand welcher konkreten methodischen Ausgestaltung das Risikomanagement vorgenommen werden soll. Die dargestellten Ansätze weisen aber bereits Ähnlichkeiten mit dem aus der Informationssicherheit bekannten Informationssicherheitsmanagementsystem (ISMS) nach der ISO/IEC 27000-Familie bzw. dem allgemeinen Risikomanagement nach ISO 31000[441] auf. Spezifisch für das Datenschutzrecht existiert weiterhin eine Norm zur Datenschutzfolgen-

---

generell risikoangemessene Maßnahmen nach dem Stand der Technik getroffen werden, z.B. auf Basis eines Branchenleitfadens zur Datensicherheit).

438 *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 35, Rn. 54; *Syckor/Strufe/Lauber-Rönsberg*, ZD 2019, 390 (392).

439 Die „Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen" wird auch in der Liste der Verarbeitungsvorgänge, für die eine Datenschutzfolgenabschätzung gemäß Art. 35 Abs. 4 DSGVO durchzuführen ist genannt; der „Betrieb von großen sozialen Netzwerken" wird hierzu als typisches Einsatzfeld bezeichnet, DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 17.10.2018, S. 3, Ziff. 9.

440 Zum europäischen Datenschutzausschuss siehe Art. 68 DSGVO. Im Englischen: European Data Protection Board (EDPB), wobei diese Abkürzung auch im Rahmen dieser Untersuchung verwendet wird.

441 Ebenfalls auf eine „Überschneidung" hinweisend: Art.-29 Datenschutzgruppe, WP 248 Rev. 01, 04.10.2017, S. 21.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

abschätzung (ISO/IEC 29134), die auch die Datensicherheit abdeckt[442] und auf die vom EDPB verwiesen wird.[443] Auf nationaler Ebene existiert daneben noch das sog. Standard-Datenschutzmodell der DSK.[444]

Aufgrund der internationalen Ausrichtung, die insbesondere für Anbieter der global angebotenen digitalen Dienste entscheidend sein dürfte und des ausdrücklichen Verweises durch den EDPB wird nachfolgend die Methodik der ISO/IEC 29134 dargestellt, die grundlegenden Bausteine finden sich aber in allen genannten Normen wieder.[445]

Die ISO/IEC 29134 enthält mit Blick auf die Risikobeurteilung insbesondere folgende methodische Schritte, die Ermittlung" und „Abschätzung" von Risiken aus der DSGVO entsprechen:[446]

1. Identifizieren von Datenschutzrisiken (ii.)
2. Analysieren der Datenschutzrisiken (iii.)
3. Bewertung der Datenschutzrisiken (iv.)
4. (Angemessene) Behandlung von Datenschutzrisiken (v.)
5. Iteration (vi.)

ii. Identifizieren von Datenschutzrisiken[447]

Im Rahmen der Identifikation sind insbesondere die technisch möglichen Sicherheitsvorfälle zu umschreiben, d.h. von welchen Risikoquellen die Schutzziele in Bezug auf die personenbezogenen Daten verletzt werden könnten.[448] Dabei sind auch die entsprechenden Szenarien wie Angriffe, eine missbräuchliche Nutzung oder technische sowie umweltbezogene Stö-

442 Hier findet sich die Datensicherheit in Form der Schutzziele der Risikoidentifikation: Verfügbarkeit, Vertraulichkeit, Integrität sowie bei den Maßnahmen u.a. mit dem Zugangsschutz, der Reduktion von Schwachstellen und dem Schutz vor Schadsoftware, DIN, ISO/IEC 29134:2020, S. 27, 34; siehe hierzu auch: *Trautwein/Kurpierz*, PinG 2018, 26 (29).

443 Art.-29 Datenschutzgruppe, WP 248 Rev. 01, 04.10.2017, Anhang 1, S. 27.

444 DSK, Standard-Datenschutzmodell, S. 5 f., das auch ausdrücklich auf die Anforderungen nach Art. 32 DSGVO, also der Datensicherheit Bezug nimmt.

445 Ein ähnlicher methodischer Ansatz auch u.a. auf ISO 29134 aufbauend findet sich bei: *F. Ritter/Reibach/Lee*, ZD 2019, 531 (531 ff.).

446 Zur Anwendung diese Schritte unter der DSGVO wohl ebenso: *Alt*, Die Sachverständigen 2020, 169 (170).

447 DIN, ISO/IEC 29134:2020, S. 26 f.

448 *Bieker*, DuD 2018, 27 (30).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

rungen zu berücksichtigen. Hinsichtlich der möglichen Angriffe kann auch eine Modellierung typischer Angreifer:innen vorzunehmen sein.[449]

iii. Analysieren der Datenschutzrisiken[450]

Bei der darauffolgenden Analyse werden die identifizierten Datenschutzrisiken genauer untersucht. Dies umfasst neben den Kategorien personenbezogener Daten (und damit ihrer Sensibilität sowie den drohenden Schäden bei Datensicherheitsverletzungen) auch die möglichen oder bekannten Schwachstellen sowie die Bedrohungen, die diese Schwachstellen ausnutzen können. Daraus sind die für das Risiko konstituierenden Eintrittswahrscheinlichkeiten (ggf. anhand zuvor beschriebener Kette von Ereignissen) sowie die Folgenschwere zu bestimmen, d.h. ihnen werden bestimmte Werte zugewiesen. Die Analyse kann dabei insbesondere qualitativ (d.h. durch bestimmte, deskriptive Kategorien (hoch, mittel, gering) als auch quantitativ, insbesondere auf Basis von empirischen Daten oder spieltheoretischen Berechnungen erfolgen.[451]

Wie bei der Auswahl von toM ist auch schon bezüglich des Risikomanagements als Verfahren der Grundsatz der Verhältnismäßigkeit zu wahren. Insofern muss der Normauftrag dahingehend restriktiv ausgelegt werden, dass nicht jedes noch so versteckte Risiko identifiziert und analysiert werden muss, sondern nur soweit sich dies im Rahmen eines *„vernünftigen Aufwands"*[452] bewegt.

iv. Bewerten von Datenschutzrisiken[453]

Im Rahmen der Bewertung der Datenschutzrisiken werden diese anhand der analysierten Eintrittswahrscheinlichkeiten und Schadensschwere priorisiert, d.h. es wird festgelegt welche Risiken in welcher Reihenfolge behandelt werden sollen. Dafür wird eine „Datenschutzrisikokarte" erstellt, in der die Risiken mit *Eintrittswahrscheinlichkeit* und *Auswirkungsgrad*

449 *Bieker*, DuD 2018, 27 (30).
450 DIN, ISO/IEC 29134:2020, S. 27 ff.
451 *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (169 f.), Rn 33 f.
452 Zu dem Begriff später noch vertieft: S. 170 ff.
453 DIN, ISO/IEC 29134:2020, S. 29 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

gekennzeichnet werden (sind beide Faktoren als „hoch" zu bewerten, hat die Behandlung eine höhere Priorität als wenn einer oder beide Faktoren als „mittel" oder als „niedrig" zu bewerten sind).[454]

v. (Angemessene) Behandlung von Datenschutzrisiken

Für die Risikobehandlung stehen vier Optionen zur Auswahl: Risikoreduktion,[455] Risikobeibehaltung, Risikovermeidung und Risikoübertragung,[456] wobei Art. 32 DSGVO regelmäßig eine Risikoreduktion oder notfalls eine -vermeidung (keine oder zumindest eine eingeschränkte Verarbeitung personenbezogener Daten) fordern dürfte.[457]

Soweit eine Risikoreduktion erforderlich ist, müssen so lange technische und organisatorische Maßnahmen getroffen werden, bis das verbleibende Restrisiko „akzeptabel" ist[458] bzw. bis nach dem Wortlaut der DSGVO ein „dem Risiko angemessenes Schutzniveau" hergestellt wurde.

Hierfür ist eine Abwägung zwischen dem Aufwand („Implementierungskosten") der Maßnahmen und dem hierdurch erreichten Nutzen in Form der Risikoreduktion (Eintrittswahrscheinlichkeit x Folgenschwere vor/nach Maßnahme) erforderlich.[459] Diese Risikoreduktion kann quantitativ auch

454 Vgl. DIN, ISO/IEC 29134:2020, S. 29 f., S. S. 56 f.; eine solche „Risikokarte" findet sich auch als „Risikomatrix" in: DSK, Kurzpapier Nr. 18, 26.04.2018, S. 5.

455 Zu beachten ist, dass der Begriff Risikoreduktion missverständlich sein kann, da (geeignete) Maßnahmen das Risiko zwar insgesamt reduzieren, aber z.T. auch andere Risiken schaffen oder erhöhen könnten; Vgl. *Bieker*, DuD 2018, 27 (31); so könnte etwa eine Maßnahme zur Erkennung von manipulierten Informationen das Risiko erhöhen, dass aufgrund der Fehlerquote (false-positive) „zutreffende Informationen" aussortiert werden.

456 DIN, ISO/IEC 29134:2020, S. 31.

457 Eine Risikobeibehaltung ist nur möglich, wenn die bereits vorhandenen Maßnahmen ausreichen, etwa wenn die Methodik als Iteration (dazu sogleich) durchgeführt wird. Eine Risikoübertragung etwa durch eine Versicherung (so ausdrücklich in: DIN, ISO/IEC 29134:2020, S. 32) ist hingegen im Sinne der DSGVO keine rechtlich adäquate Option, da der Verantwortliche die Risiken tatsächlich angemessen mindern muss; vgl. zu diesem Rechtsgedanken im KRITIS-Recht: *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn. 20.

458 Vgl. DIN, ISO/IEC 29134:2020, S. 32.

459 Zumeist bleibt die Beschreibung der Abwägungspunkte sehr vage, so z.B. auch das DIN, ISO/IEC 29134:2020, S. 30; sowie das EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, Rn. 24. Im dargestellten Sinne neben *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (168 ff.), Rn. 29 ff.; bereits ähnlich: *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018,

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wiederrum als Differenz der Risikokosten (vor/nach Maßnahme) und somit als Kostenwert ausgedrückt werden.

Die daraus resultierende *Kosten-Nutzen-Abwägung* verhilft auch dem grundrechtlichen Verhältnismäßigkeitsprinzip zur Geltung.[460] Dabei werden die Maßnahmen in der Datensicherheit nach Art. 32 Abs. 1 DSGVO zumeist die Eintrittswahrscheinlichkeit eines Ereignisses (und damit auch eines Schadenseintritts) reduzieren, z.B. durch das Schließen einer Schwachstelle bzw. durch den Aufbau größerer und besserer Sicherheitsmechanismen, die bei einem Angriff überwunden werden müssen.

Im Ergebnis sind die zur Risikoreduktion getroffenen Maßnahmen angemessen und das verbleibende Restrisiko „akzeptabel", wenn die Vornahme weiterer Maßnahmen einen im Vergleich zur damit zu erreichenden Risikoreduktion unverhältnismäßigen Aufwand begründen würde,[461] also insbesondere hohe Kosten aufweisen würde ohne die Eintrittswahrscheinlichkeit signifikant zu senken.

vi. Iteration

Dieser in ISO/IEC 29134 als „Reflektieren von Prozessänderungen" bezeichnete[462] und in Art. 32 Abs. 1 lit d) und Art. 35 Abs. 11 DSGVO niedergelegte Schritt enthält Vorgaben zur Iteration des Risikomanagements. So ist das Risikomanagement zum einen zu aktualisieren, wenn sich die Sachlage hinsichtlich der Datenverarbeitungsprozesse ändert,[463] was als *anlassbezogene Iteration* bezeichnet werden kann. Demgegenüber steht die - in ISO/IEC 29134 vorgesehene, aber gesetzlich nicht vorgeschriebene- *turnusmäßige Iteration*, wonach das Risikomanagement in festen Zeitabständen

---

Art. 32, Rn. 52 ff.; nach a.A. wird nur auf die absolute Höhe der Risiken abgestellt, so wohl *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 95, insofern dürfe kein „eklatantes Missverhältnis" zu den Kosten bestehen. Das Abstellen auf die Risikoreduktion ermöglicht hingegen eine präzisere Anknüpfung an die Maßnahmen, die gerade nach ihrem Nutzen, also ihrer Risikoreduktion ausgewählt und vorgenommen werden müssen.

460 *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (165), Rn. 17; vgl. auch: *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 20.

461 Vgl. auch *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn. 63 wonach Maßnahmen das Risiko auf ein angemessenes Maß reduzieren müssen.

462 DIN, ISO/IEC 29134:2020, S. 39.

463 Wie zuvor.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

überprüft werden soll.[464] Ungeachtet dessen wird zumindest ein „stetig laufendes Verfahren zur Überwachung datenschutzrechtlicher Risiken" vorgegeben.[465]

Mit Blick auf die Datensicherheit müssen dabei nicht nur Prozessänderungen, sondern auch Änderungen in der Datensicherheitslage, d.h. insbesondere das Auftauchen neuer Sicherheitsrisiken, berücksichtigt werden.[466] Steht mithin neues Wissen über Risiken zur Verfügung, etwa durch neu bekannt gewordene Schwachstellen, ist das Risikomanagement diesbezüglich zu aktualisieren und ggf. die Risikobehandlung dementsprechend anzupassen. Insofern wird hier *explizites Wissen* über neue spezifische Risiken (Risikowissen) verfügbar.[467]

d. Gegenüberstellung der Resilienz

Fraglich ist, wie sich die Resilienz in Begriff und Methodik des Risikos nach der DSGVO bzw. der ISO/IEC 29134 einfügt. Dabei wird zunächst herausgearbeitet, dass sich die Resilienz, wie schon in der Wortlautauslegung angedeutet, anders als das Risiko definitorisch mit der Bewältigung von Ungewissheit befasst (i.). In einem weiteren Schritt wird dann das Verhältnis der Resilienz zum Risikomanagement geklärt (ii.).

i. Resilienz als Umgang mit Ungewissheit

Das Risiko befasst sich nach seiner Definition und wie auch in der Methodik gezeigt wurde mit hinreichend bekannten und beschreibbaren Vorgängen (Einwirkungen, die auf Schwachstellen treffen, führen zu Ereignissen, bei denen Schutzziele verletzt werden (Sicherheitsvorfälle), welche ihrerseits Auswirkungen auf Schutzgüter haben können). Risiken beschreiben mithin Vorgänge, die sich im Vorfeld antizipieren bzw. kalkulieren lassen[468]

464 DIN, ISO/IEC 29134:2020, S. 39; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 35, Rn. 73.
465 *Rath/Feuerherdt*, CR 2017, 500 (503); *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 35, Rn. 77.
466 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 35, Rn 73.
467 Zur Abgrenzung des impliziten Wissens siehe: S. 183 f.
468 *Luhmann*, Soziologische Aufklärung 5, S. 129; *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (52).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

und denen daher im Rahmen der Angemessenheit mit spezifischen Gegenmaßnahmen begegnet werden kann.

Nachfolgend soll die Ungewissheit zunächst genauer beschrieben werden. So lassen sich verschiedene Formen von Ungewissheit ausmachen (1) und die Ungewissheit kann sich auf unterschiedliche Aspekte, namentlich die Eintrittswahrscheinlichkeiten und/oder die Schwere von Ereignissen beziehen (2). Unter (3) wird dann dargestellt, ob und inwieweit die Resilienz eine Antwort auf diese Ungewissheit geben kann. Schließlich (4) wird beschrieben, wie sich die Resilienz mit der Adressierung der Ungewissheit zum Risikobegriff in Art. 32 DSGVO verhält, dem dort wie gezeigt eine übergeordnete Rolle (Schutzzweck des Art. 32 DSGVO: Gewährleistung eines dem Risiko angemessenen Schutzniveaus) zukommt.

(1) Ungewissheit als (Un)bekanntheit und (Nicht)-Wissen

Allerdings gibt es insbesondere in der Daten- und IT-Sicherheit Situationen, die nicht hinreichend als Risiken antizipiert werden können und die tradierte Risikomethodik somit an ihre Grenzen bringen.[469] Basierend auf einer Differenzierung in der *Entscheidungstheorie* kann man diesbezüglich in Abgrenzung zu den soeben skizzierten Entscheidungen unter Risiko (Entscheidung unter Unsicherheit)[470] von Entscheidungen unter Ungewissheit sprechen.[471] Die Ungewissheit drückt dabei aus, dass der *Entscheider*

469 *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2); *Collier et al.*, Computer 2014, 70 (70).

470 *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (51 f.).

471 *G. Menges*, Statistische Hefte 1963, 151 (152); *Boeckelmann/Mildner*, SWP-Zeitschriftenschau Sep. 2011, 1 (1 f.); *Gigerenzer*, in: Fleischer, Rationale Entscheidungen unter Unsicherheit, 1 (2 ff.); *Knight*, Risk, Uncertainty and Profit, S. 19 f.; *Nell*, Wahrscheinlichkeitsurteile in juristischen Entscheidungen, S. 127 f.; *Bamberg/Coenenberg/Krapp*, Betriebswirtschaftliche Entscheidungslehre, S. 19; die Verwendung des Terminus „Ungewissheit" in hier vertretener Abgrenzung zur „Unsicherheit/Risiko wird in der Literatur zur Sicherheitsforschung uneinheitlich bewertet. Nicht abschließend zu nennen sind insoweit: *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (46 f.), der Ungewissheit als Unterfall von Unsicherheit definiert oder *Schmid*, in: Pelizäus/Nieder, Das Risiko – Gedanken übers und ins Ungewisse, 31 (55) der von Ungewissheit spricht, wenn nur Wissen über die Eintrittswahrscheinlichkeit fehlt und von Unsicherheit spricht, wenn das Wissen sowohl über Eintrittswahrscheinlichkeit als auch Folgen fehlt; *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (61 ff.) unterscheidet mit grundlegendem Verweis auf *Beck*, Risikogesellschaft, S. 17, 28 f. zwischen alten, bekannten und beherrschbaren Risiken einerseits sowie neuen, teilweise unbekannten und unbeherrschbaren Risi-

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

– also hier der zur Gewährleistung der Datensicherheit verpflichtete Verantwortliche - kein (vollständiges) Bild der Realität hat,[472] also dass kein Wissen vorhanden ist bzw. er keinen Zugang zu vorhandenem Wissen hat.[473] Konkret fehlt ihm hier das Wissen darüber, ob, weshalb und mit welcher Wahrscheinlichkeit es zu einem schädigenden Ereignis kommt und welche Auswirkungen dieses hat.[474] In Abgrenzung zum Risiko liegt Ungewissheit mithin vor, wenn sich die Eintrittswahrscheinlichkeit und/oder die Folgenschwere eines Ereignisses nicht mehr qualitativ oder quantitativ analysieren lassen[475] oder bereits das Ereignis selbst nicht als mögliches Risiko identifiziert werden konnte. Rechtlich maßgeblicher Zeitpunkt für die Frage der Ungewissheit ist dabei der Zeitpunkt der Maßnahmenwahl. Im Weiteren ist außerdem zwischen zwei Formen oder *Ordnungen von Ungewissheit* zu differenzieren:[476]

Als (Un)gewissheit erster Ordnung wird hier das abstrakte Vorhandensein bzw. Nichtvorhandensein von Wissen über den Sachgegenstand, also Ereignisse und Umstände, welche für die Gewährleistung der Datensicherheit von Bedeutung sind, definiert. Diese (Un)gewissheit erster Ordnung wird für diese Untersuchung als *Wissen*[477] *bzw. Nicht-Wissen* bezeichnet.

---

ken andererseits; *Scherzberg*, in: Engel/Halfmann/Schulte, Wissen, Nichtwissen, unsicheres Wissen, 113 (117), bezeichnet Ungewissheit im hier verwendeten Sinn als „unkalkulierbarer Ungewissheit" und Unsicherheit/Risiko als „kalkulierbare Ungewissheit". Jedenfalls zum Teil mag diese Uneinheitlichkeit auch auf unterschiedliche Übersetzungen des englischen Worts „uncertainty" (Unsicherheit/Ungewissheit) zurückzuführen sein, wobei die Übersetzung mit „Ungewissheit" den Kern des mangelnden Wissens besser beschreibt, *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 20.

472 *G. Menges*, ebd.; *Nell,* ebd.; vgl. auch weiter ausdifferenzierend: *W. Walker et al.*, Integrated Assessment 2003, 5 (8 ff.).

473 Vgl. *Wollenschläger*, Wissensgenerierung im Verfahren, S. 33; als „Mangel an Information zur Ausgangslage oder zu zukünftigen Entwicklungen" *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 19.

474 Vgl. *Kolliarakis*, in: Jeschke/Jakobs/Dröge, Exploring Uncertainty, 313 (317); *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (118 f., 122).

475 *Lamker*, Unsicherheit und Komplexität in Planungsprozessen, S. 85.

476 Grundlegend wurde diese Unterscheidung in (un)known (un)knowns vom US-Verteidigungsminister Donald Rumsfeld populär gemacht, DoD, News Briefing - Secretary Rumsfeld and Gen. Myers, 12.02.2002; als Konzept bestand sie allerdings bereits zuvor und wurde u.a. von der NASA verwendet: NASA, Program Management and Procurement Procedures and Practices, 24.06.1981, S. 73 f.

477 Klarstellend sei an dieser Stelle darauf hingewiesen, dass der Begriff des Wissens sich hier auf das Wissen über die Datensicherheitsgewährleistung bezieht, nicht auf

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Im Falle des Nicht-Wissens ist weiter zu differenzieren: Das Wissen ist entweder nicht vorhanden, weil es jeweils zum Zeitpunkt der Entscheidung absolut nicht existiert oder aber die Hebung dieses Wissens ist nicht mehr mit *vernünftigem Aufwand* möglich. Diese Einschränkung des Wissensbegriffs ergibt sich aus dem Kontext des Datensicherheitsrechts, der somit einen relativen und keinen absoluten Wissensbegriff fordert: Denn der Normauftrag muss den Adressaten als Entscheider zum Ausgangspunkt nehmen und dieser kann Wissen nur insoweit innehaben, als dieses objektiv existiert und er dieses auch mit vernünftigem Aufwand erlangen kann. Der vernünftige Aufwand ist insofern Ausdruck des Verhältnismäßigkeitsprinzips und richtet sich nach der Bedeutung der jeweils zu sichernden Schutzgüter.[478]

Die Ungewissheit zweiter Ordnung beschreibt den subjektiven Erkenntniszustand des Entscheiders bzgl. dieses Wissens.[479] Sie beschreibt spezifischer die subjektive Kenntnis des Entscheiders von dem objektiv vorhandenen und mit verhältnismäßigen Aufwand erreichbaren Wissen und wird nachfolgend als *(Un)bekanntheit* bezeichnet. Es adressiert somit insbesondere auch den Fall, dass an sich mit vernünftigem Aufwand zu hebendes Wissen dem Entscheider gleichwohl nicht vorliegt. In welchen praktischen Fällen dies gegeben ist, wird sogleich bei den einzelnen Kategorien erläutert.

Entsprechend dieser Definition lassen sich folgende Kategorien unterscheiden, wobei hier zusätzlich die verbreiteteren englischen Entsprechungen genannt werden:[480]

---

das Wissen über natürliche Personen, welches die personalisierten Dienste verwenden.

478 Der vernünftige Aufwand hat insoweit den gleichen Bezugspunkt wie die abstrakte Angemessenheit (S. 182 f.). Da auf der anderen Seite der Abwägung aber hier nicht der Aufwand für konkrete toM zur Sicherheitsgewähr, sondern die Reichweite des Verfahrens der Risikoidentifikation und -analyse steht erscheint es sinnvoll, hier zwei unterschiedliche Begriffe zu nutzen.

479 Dies wird auch als „epistemologischer Status" bezeichnet: *Daase/Kessler*, Security Dialogue 2007, 411 (413); *Wollenschläger*, Wissensgenerierung im Verfahren, S. 33 spricht insoweit von einem „bewussten oder unbewussten Mangel an Wissen" .

480 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 57 ff; diese sprechen sprachlich nur von „Bekanntheit"; mit von hiesiger Verwendung teilweise abweichender inhaltlicher Ausgestaltung der Kategorien: *Daase/Kessler*, Security Dialogue 2007, 411 (413 ff.); *Boeckelmann/Mildner*, SWP-Zeitschriftenschau Sep. 2011, 1 (2 f.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Known	Knowns	=	bekanntes	Wissen (Risiko)
Known	Unknowns	=	bekanntes	Nicht-Wissen
Unknown	Knowns	=	unbekanntes	Wissen
Unkown	Unknowns	=	unbekanntes	Nicht-Wissen

Zunächst beschreibt die Kategorie des *bekannten Wissens* (Known Knowns) die Risiken und gehört somit mangels Vorliegens eines Wissensdefizits gerade nicht zur Ungewissheit. Das Wissen über Risiken ist durch Empirie oder fundierte Schätzung objektiv vorhanden bzw. erzeugbar und dieses Wissen ist dem Entscheider auch bekannt. Es handelt sich somit zwar immer noch um eine Entscheidung unter Unsicherheit, da der Eintritt des Ereignisses nicht sicher feststeht; der Entscheider verfügt aber vollständig über das Wissen, was er zum Zeitpunkt der Entscheidung (Maßnahmenwahl) haben kann.[481]

Die Kategorie des *bekannten Nicht-Wissens* (Known Unknowns) beschreibt den Zustand, bei welchem der Entscheider Kenntnis davon hat, dass ihm über bestimmte Umstände kein Wissen vorliegt.[482] Dies kann zum einen daran liegen, dass die zum gegenwärtigen Zeitpunkt bestehenden *absoluten Grenzen der wissenschaftlichen Erkenntnisfähigkeit* erreicht sind (exemplarisch bei dem Blackbox-Charakter von KI-Systemen, der zumindest in Ansätzen versucht wird durch sog. erklärbare, künstliche Intelligenz (en: explainable AI) zu durchbrechen[483]).

Zum anderen muss Wissen (über Risiken), wie bereits angerissen, nur im Rahmen des *vernünftigen Aufwands* gehoben werden: Diese Grenze kann etwa bei sehr hoher Komplexität von Systemen[484] erreicht werden, da diese Systeme bei einer antizipierten Betrachtung nur stark vereinfacht modelliert werden können und dabei bestimmte Annahmen getroffen werden müssen, wie etwa dass Wechselwirkungen zwischen den Komponenten nur schwach ausgeprägt sind und das Verhalten der Komponenten

481 Teilweise gleichwohl auch als Entscheidungen unter Ungewissheit bezeichnet: *Schneeweiß*, Entscheidungskriterien bei Risiko, S. 1, 12, 27. Zur begrifflichen Vielfalt bei Unsicherheit/Ungewissheit: siehe Fn. 471.

482 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 59.

483 *Adadi/Berrada*, IEEE Access 2018, 52138 (52138 ff.).

484 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 59; zur Resilienz als Antwort Vgl. *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (12); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

linear ist.[485] Solche komplexen Systeme weisen mitunter sogar Eigenschaften auf, die über die Eigenschaften ihrer Komponenten hinausgehen (sog. Emergenz)[486] und folglich auch nicht alleine durch eine Betrachtung ihrer Komponenten erklärt werden können. Somit ist das Wissen über komplexe Systeme und ihr zukünftiges Verhalten zumeist unvollständig.[487] Unter diese Fallgruppe dürften auch Situationen fallen, in denen (auch) Dienste oder Informationen von Dritten genutzt werden und der Entscheider keinen Einblick in die Funktionsweise sowie die Sicherheit der Systeme des Dritten hat. Diese Systeme liegen mithin außerhalb seiner *Systemgrenzen*,[488] die den Kontrollbereich des Entscheiders umschreiben.

Die nächste Kategorie ist jene des *unbekannten Wissens* (Unknown Knowns). Charakteristisch ist hier, dass das Wissen über bestimmte Umstände an sich verfügbar bzw. mit vernünftigem Aufwand zu heben wäre. Das Wissen ist dem Adressaten aber jedenfalls unbekannt, d.h. es wurde subjektiv nicht erhoben bzw. zur Kenntnis genommen. Theoretisch ist dieses Defizit somit vermeidbar[489] und wird z.T. mit dem Schlagwort „Ignoranz" umschrieben.[490]

In Erscheinung treten kann diese Kategorie insbesondere bei Fehlern bzw. Schwachstellen in Systemen. Es ist nicht anzunehmen, dass jede Software bereits herstellerseitig fehlerfrei zur Verfügung gestellt wird.[491] Ebenso wenig kann davon ausgegangen werden, dass der Verwender einer solchen Software wie etwa der Verantwortliche all diese Fehler einschließlich insbesondere der Schwachstellen finden und beheben kann; außerdem ist insoweit zu berücksichtigen, dass durch die Behebung mitunter auch unbemerkt andere, neue Fehler in das System eingefügt werden können.[492] Verschuldenstechnisch kann hier ein fahrlässiges Verhalten vorliegen, da

485 *Park et al.*, Risk analysis 2013, 356 (362); *Beckerman*, Systems Engineering 2000, 96 (97).

486 *Hiermaier/Scharte/Fischer*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 155 (156); *Holland*, Complexity, S. 49 ff.

487 *Park et al.*, Risk analysis 2013, 356 (362); *Funtowicz/Ravetz*, Futures 1994, 568 (578); *Berkes*, Nat Hazards, Vol. 41 (2007), 283 (284 f.); *W. Walker et al.*, Integrated Assessment 2003, 5 (9 f.).

488 Dazu bereits S. 114 f.

489 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 61.

490 *Daase/Kessler*, Security Dialogue 2007, 411 (414 f.); *Boeckelmann/Mildner*, SWP-Zeitschriftenschau Sep. 2011, 1 (3).

491 FZI, Wirksame Sicherheitsmaßnahmen für IoT-Produkte, 25.01.2021, S. 10.

492 *Avizienis et al.*, IEEE TDSC 2004, 11 (29).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

entweder vorhandenes Wissen oder zumindest mit vernünftigem Aufwand erzeugbares Wissen nicht genutzt wurde.[493] Allerdings liegt dieses Verschulden nicht zwangsläufig beim Verantwortlichen, z.B. wenn er eine fehlerhafte (Soft- oder Hardware-) Komponente einkauft, den Fehler in derselben aber selbst nicht erkennen konnte.

Schließlich verbleibt sog. *unbekanntes Nicht-Wissen* (*Unknown Unknowns),* d.h. drohende Ereignisse, die unvorhersehbar und unerwartet auftreten.[494] Entscheidend ist insoweit insbesondere in Abgrenzung zu dem bekannten Nicht-Wissen*,* dass dem Entscheider nun auch nicht bekannt ist, dass ihm das Wissen über Ereignisse fehlt. Es handelt sich mithin um Ereignisse, von denen er „nicht einmal träumt",[495] d.h. die als solche gänzlich außerhalb seines Erkenntnishorizonts liegen. Sie werden teilweise auch als *Black Swans* bezeichnet; was genauer Ereignisse beschreibt, die aufgrund ihrer (erst im Nachgang feststellbaren und dies ggf. auch rückblickend mit vernünftigem Aufwand) sehr geringen Eintrittswahrscheinlichkeit auch objektiv nicht antizipiert wurden, die aber hohe Schäden zur Folge hatten.[496] Hierunter können etwa global wirkende Sicherheitslücken wie *Heartbleed*[497] in der zur Transportverschlüsselung im Internet weit verbreiteten Software OpenSSL oder *Meltdown*[498] als Hardware-Sicherheitslücke in Mikroprozessoren gefasst werden. Aus Sicht eines Entscheiders außerhalb der mit den jeweiligen IT-Produkten befassten Organisationen[499] handelt es sich hierbei um Nicht-Wissen, da er das Wissen hierüber nicht mit vernünftigem Aufwand hätte erlangen können. Es traf diese Entscheider auch völlig unerwartet (Unbekanntheit), da sie nicht mit einer solch

493 Ist eine Sicherheitslücke hingegen so versteckt (weil sie etwa nur bei beim gleichzeitigen Zusammentreffen vieler Programmzustände eintritt), dass sie mit vernünftigem Aufwand nicht gefunden werden konnte, liegt ein Fall des *bekannten oder unbekannten Nicht-Wissens* vor.

494 *Sharkov*, in: Multari/Singhal/Manz, Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense - SafeConfig'16, 3 (4).

495 *Daase/Kessler*, Security Dialogue 2007, 411 (413).

496 Vgl. *Kolliarakis*, in: Jeschke/Jakobs/Dröge, Exploring Uncertainty, 313 (320); *Hiermaier/Scharte/Fischer*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 155 (156); *Taleb*, Der Schwarze Schwan, S. 1 f.

497 *Ghafoor et al.*, in: 17th IEEE International Multi Topic Conference 2014, Analysis of OpenSSL Heartbleed vulnerability for embedded systems, 314 (314 ff).

498 *Lipp et al.*, CACM, Vol. 63 (2020), Heft 6, 46 (46 ff.).

499 Aus deren Sicht mag es sich hingegen um *unbekanntes Wissen* gehandelt haben, da die Sicherheitslücken möglicherweise auch mit vernünftigem Aufwand hätten festgestellt werden können; wird dies verneint, wäre es auch aus deren Sicht ein Fall *unbekannten Nicht-Wissens.*

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

schweren und übergreifenden Sicherheitslücke in einer global eingesetzten (open-source) Komponente rechneten.[500]

Alle drei Kategorien die sich mit Unbekanntheit und/oder Nicht-Wissen befassen, sind dem Oberbegriff des „Entscheidens unter Ungewissheit" (en: unknown) zuzuordnen, da in jedem Falle ein Mangel im Erkenntniszustand vorliegt. Im Ergebnis ergibt sich somit folgende Matrix:[501]

Tabelle 4: Kategorien von Ungewissheit

	Wissen	Nicht-Wissen
bekannt	**Bekanntes Wissen** ***Entscheiden unter*** Risiko ***(Unsicherheit)*** Dem Entscheider ist vorhandenes Wissen bekannt.	**bekanntes Nicht-Wissen** ***Entscheiden unter Ungewissheit*** Dem Entscheider ist das Nicht-Wissen bekannt.
unbekannt	**unbekanntes Wissen** ***Entscheiden unter Ungewissheit*** Dem Entscheider ist vorhandenes Wissen unbekannt.	**unbekanntes Nicht-Wissen** ***Entscheiden unter Ungewissheit*** Selbst das Nicht-Wissen ist dem Entscheider nicht bekannt.

(2) Was ist unbekannt und worüber besteht kein Wissen?

In einem weiteren Schritt soll genauer beschrieben werden, worauf sich die (*Un)bekanntheit* sowie das *(Nicht-)Wissen* beziehen können. Ausgehend von den Dimensionen des Risikos ist nur dann von *bekanntem Wissen* also einem antizipationsfähigen Risiko zu sprechen, wenn sowohl Wissen zur Eintrittswahrscheinlichkeit als auch zur Folgenschwere beim Entscheider vorliegt oder zumindest (mit vernünftigem Aufwand) gehoben werden kann. Bezüglich der Unbekanntheit bzw. des Nicht-Wissens lassen sich somit drei Kategorien zusammenfassen:

Zunächst kann das Ereignis *gänzlich unbekannt sein bzw. keinerlei Wissen darüber existieren*. Hierunter fallen insbesondere Ereignisse im Bereich

500 Geht man hier (abweichend von den genannten Beispielen) von einem schuldhaften Verkennen aus, d.h. dass dem Normadressaten der Umstand des Nicht-Wissens hätte bekannt sein müssen (bekanntes Nicht-Wissen), kann ihm das Unterlassen entsprechender spezifischer Resilienzmaßnahmen als unzureichende Sicherheitsgewährleistung vorgehalten werden.

501 Vgl. *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, Abb. 3, S. 57.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

das sog. *unbekannten Nicht-Wissens*. Auch in Fällen unbekannten Wissens fehlt dem Entscheider jegliche *Kenntnis, wenn Schwachstellen vollständig übersehen wurden* (theoretisch aber hätten erkannt werden können). Schließlich könnten auch Fälle des *bekannten Nicht-Wissens* hierunterfallen, etwa beim bereits angesprochenen Einsatz von ML-Systemen, bei dem sich aufgrund des Blackbox-Charakters weder die Wahrscheinlichkeit noch der Grad möglicher Abweichungen (und damit auch die Folgenschwere) der Ergebnisse sicher vorhersagen lässt.

Zweitens kann Wissen *nur bezüglich der Eintrittswahrscheinlichkeiten* eines Ereignisses nicht aber bzgl. der Folgenschwere bestehen bzw. bekannt sein.[502] Beispielsweise kann in Fällen des *bekannten Nicht-Wissens* zwar die Eintrittswahrscheinlichkeit eines Ereignisses (z.B. der Ausfall bzw. die Manipulation eines Dienstes bekannt sein, allerdings kann die Folgenschwere in einem sehr komplexen, offenen System nicht vorher antizipiert werden, etwa wenn Dienstergebnisse später auch von unbekannten Drittdiensten genutzt werden.[503]

Drittens kann das Wissen umgekehrt *nur bezüglich der Folgenschwere* bestehen, nicht aber bzgl. der Eintrittswahrscheinlichkeit. Dies ist anzunehmen, soweit das Wissen über ein mögliches Ereignis und seine Folgen (z.B. die Folgen des Ausfalls einer Komponente) besteht, nicht aber darüber, wie wahrscheinlich es ist, dass es zu diesem Ereignis kommt. Dies ist besonders häufig bei Ereignissen anzutreffen, die durch menschliche Angreifer:innen verursacht werden, da häufig kein Wissen über deren Anzahl, Motivation und Fähigkeiten vorhanden ist. Spieltheoretische Berechnungen[504] können dabei die Ungewissheit zwar reduzieren, aber zumeist nicht vollständig ausschließen. Da dieses Wissensdefizit dem Entscheider bekannt ist, handelt es sich um einen Fall des *bekannten Nicht-Wissens*.

---

502 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 33 vertreten hierzu die Auffassung, man könne in diesen Fällen auch von einem sehr hohen oder sogar dem höchstmöglichen Schadensausmaß ausgehen. Dies ebnet den Weg zurück in das Risikomanagement.

503 Der soeben genannte Fall unbekannten Wissens mit den übersehenen Schwachstellen kann hierunter hingegen nur selten fallen: Denkbar ist zwar die Eintrittswahrscheinlichkeit aus Statistiken über die generelle Häufigkeit von Schwachstellen abzuleiten; mangels konkreter Kenntnis der Schwachstelle kann aber die ebenso wichtige Ausnutzungswahrscheinlichkeit derselben nicht bestimmt werden und damit bleibt am Ende (auch) die Eintrittswahrscheinlichkeit eines Ereignisses infolge übersehener Schwachstellen ungewiss.

504 *Beyerer/Geisler*, EJSR 2016, 135 (138 f.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Soweit Eintrittswahrscheinlichkeit und Folgenschwere ungewiss sind, können somit im Ergebnis alle drei Formen der Ungewissheit vorliegen. Ist hingegen nur die Eintrittswahrscheinlichkeit oder Folgenschwere ungewiss, ist stets ein Fall des bekannten Nicht-Wissens gegeben.

(3) Resilienz als spezifische Antwort

Insgesamt zeigt sich somit, dass ein großer Bereich besteht, in dem das Wissen des Entscheiders über Risiken gänzlich fehlt oder unvollständig bleibt und er mit dem Risikomanagement somit nicht alle drohenden Einwirkungen behandeln kann. Die Resilienz kann nun eben diesen ungewissen Ereignissen entgegengesetzt werden, die sich infolgedessen, dass sie sich nicht vorher als Risiko antizipieren und verhindern lassen, manifestieren können.[505] Umgekehrt kann zur Abgrenzung auch formuliert werden: Um antizipationsfähigen Ereignissen (Risiken) zu begegnen, ist keine Resilienz erforderlich,[506] dies ist vielmehr tradierter Bestandteil bei der Gewährleistung von Datensicherheit (und Sicherheit im Allgemeinen). Die Resilienz tritt vielmehr als Komplementär zum klassischen Risikomanagement auf,[507] welches bei ungewissen, d.h. unbekannten Ereignissen und solchen bei denen es an dem notwendigen Wissen fehlt, an seine Grenzen stößt.

Eine weitere Unterscheidung ergibt sich aus dem Betrachtungsraum: Durch seine Beschränkung auf Risiken ist das Risikomanagement auf die Betrachtung singulärer Vorgänge beschränkt, die sich als Ketten von Einwirkung, Schwachstelle und Ereignis bis hin zum Schaden beschreiben lassen. Insbesondere die Analyse der informationstechnischen Systeme hinsichtlich der möglichen Einwirkungen und Schwachstellen bis zum (zu verhindernden) Ereignis wird bereits seit langem durch sog. Angriffs-

505 Vgl. *Wildavsky*, Searching for safety, S. 85; *Fritz*, Resilienz als sicherheitspolitisches Gestaltungsbild, S. 102; *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (118); Resilienz als Antwort insbesondere auf „unvorhergesehene Störungen" bei *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39 bzw. „nicht vorhergesehene Änderungen in den Abläufen" bei *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 43.

506 *Scharte*, Resilience Engineering, S. 453.

507 Vgl. *Fritz*, Resilienz als sicherheitspolitisches Gestaltungsbild, S. 23; *Park et al.*, Risk analysis 2013, 356 (357); *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (121).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

bäume beschrieben.[508] Oft besteht wie dargestellt bereits kein (vollständiges) Wissen über diese singuläre Ereignisketten (etwa die Existenz von Schwachstellen oder die Motivation möglicher Angreifer:innen). Daneben ist die Beschränkung auf singuläre Ereignisketten auch für die vollständige Sicherheitsgewähr unzureichend,[509] da in komplexen Systemen zusätzlich betrachtet werden muss, welche Auswirkungen daraus resultieren, wenn mehrere betrachtete Ereignisse gleichzeitig eintreten. Da dies aber häufig zu einer unüberschaubaren Anzahl von Kombinationsmöglichkeiten führt, kann dies mitunter nicht mehr mit vernünftigem Aufwand durchgeführt werden. Auch insoweit greift die Resilienz ein und adressiert explizit den Umgang mit dem *Unbekanntem* und der *Ungewissheit*,[510] so dass die Resilienz das Risikomanagement ergänzt und beide Ansätze gemeinsam einen angemessenen Schutz gewährleisten können.[511]

Schließlich ist anzumerken, dass das Risikomanagement wie die Resilienz (nur) eine Methodik bietet (dazu sogleich), welche allein aber noch keine Vorgabe hinsichtlich bestimmter zu wählender Maßnahmen beinhaltet.[512]

(4) Folgen für die Risikodefinition

Wie oben bereits dargestellt ist die Definition des Risikobegriffs in der DSGVO sehr weit gefasst und erstreckt sich von den Einwirkungen auf die Verarbeitung, die zu einer „Verletzung des Schutzes personenbezogener Daten" (Art. 4 Nr. 12 DSGVO) führen können bis zu den finalen Schäden an den Rechten und Freiheiten natürlicher Personen.

Insofern scheint es zunächst auch nachvollziehbar, dass nach Art. 32 Abs. 1 DSGVO die Resilienz nur einen Aspekt darstellt, um diese Risiken im Sinne der Gewährleistung eines „angemessenen Schutzniveaus" zu bewälti-

508 Grundlegend: *Schneier*, Dr. Dobb's journal, Vol. 24 (1999), Heft 12, 21 (21 ff.).

509 *Sheridan, Hum Factors 2008, 418* (421).

510 Nur abstellend auf „Ungewissheit" (en: uncertainties): *Wildavsky*, Searching for safety, S. 85; ähnlich auch *Bröckling*, Resilienz: Über einen Schlüsselbegriff des 21. Jahrhunderts, 2017, S. 14; *Rajamaki/Nevmerzhitskaya/Virag*, in: Proceedings of 2018 IEEE Global Engineering Education Conference (EDUCON), Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF), 2042 (2044 f.).

511 *Park et al.*, Risk analysis 2013, 356 (359, 366).

512 Ähnlich auch: *Fritz*, Resilienz als sicherheitspolitisches Gestaltungsbild, S. 90, der insoweit von einem „Formalismus" spricht.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

gen. Die Resilienz steht nach diesem Verständnis somit nicht neben dem (antizipationsfähigen) Risiko, sondern ist ein Teil der Risikobewältigungsstrategie.

Allerdings führt dies zu einem Widerspruch, sofern man es für „Risiken" im Sinne der Entscheidungstheorie wie bereits zuvor dargestellt als konstitutiv erachtet, dass sie in Eintrittswahrscheinlichkeit und Folgenschwere im Vorfeld mess- und kalkulierbar[513], also anders als die Ungewissheit gerade antizipierbar sind[514] und so im Sinne der Risikomethodik identifiziert, analysiert, bewertet und behandelt werden können. Die Resilienz als Antwort auf Ungewissheit kann in diesem Fall somit nicht als Teil der Risikomethodik gesehen werden, sondern ist wie bereits dargestellt ein Komplementär hierzu.

Auflösen lässt sich dieses Dilemma mit einer Begriffsauslegung des Risikos, die auch die Ungewissheit einschließt, d.h. auch objektiv unbekannte, mit vernünftigem Aufwand nicht erkennbare und somit weder durch Empirie noch durch Schätzungen hinsichtlich Eintrittswahrscheinlichkeit und Schadensschwere bezifferbare Risiken umfasst. Man kann dies als eine *naturalistische Betrachtungsweise* bezeichnen, mit der anerkannt wird, dass Risiken objektiv nicht ihre Existenz einbüßen, nur weil sie nicht erkannt und infolgedessen auch nicht behandelt werden (können).

Dies entspricht auch der teleologischen und historischen Zielsetzung der DSGVO. Es erscheint zweckwidrig anzunehmen, dass mit der DSGVO nur solche antizipationsfähigen Risiken adressiert und der Verantwortliche bzw. der Auftragsverarbeiter im Übrigen vollständig freigestellt werden sollte, zumal für die Resilienz dann nach dem dargestellten Verständnis kein Raum verbliebe.

ii. Methodische Einordnung

Für die methodische Implementierung gilt aber gleichwohl, dass es bei der Gewährleistung von Resilienz nicht um die Beurteilung und Behandlung antizipierter Risiken gehen kann. Mithin ist die Resilienz auch nicht durch das Risikomanagement abgedeckt, sondern es bedarf insoweit ergänzender bzw. modifizierende Methodiken für den resilienten Umgang mit Ungewissheit.

513 *Luhmann*, Soziologische Aufklärung 5, S. 129; *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (52).

514 *G. Menges*, Statistische Hefte 1963, 151 (152).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Dabei ist in einem ersten Schritt zu beachten, dass sich die Methodik zur Gewährleistung der Resilienz in Abhängigkeit von den Formen der Ungewissheit unterscheidet (1). Zweitens: Die zu treffenden Resilienzmaßnahmen müssen zwar angemessen sein, allerdings kann die Angemessenheit aufgrund der Ungewissheit gerade nicht auf die Risikoreduktion bezogen werden; auch hier ergeben sich insoweit methodische Unterschiede (2). Weiterhin stellt sich die Frage, wie bei einem Wissenszuwachs zwischen Risikomanagement (Iteration) und Resilienzmethodik (Lernen) zu differenzieren ist (3). Am Ende schließt dieser Abschnitt mit einer Zusammenfassung von Risikomanagement und Resilienzmethodik (4).

(1) Adressierung unterschiedlicher Formen der Ungewissheit

Hinsichtlich der Entwicklung einer Resilienzmethodik muss zunächst zwischen den unterschiedlichen Formen der Ungewissheit wie sie in Abschnitt i.(1)[515] dargestellt wurden, differenziert werden. Hierfür sind im Ergebnis zwei unterschiedliche methodische Ansätze erforderlich:

Mit dem ersten Ansatz ist mit Blick auf das *unbekannte Wissen* und das *unbekannte Nicht-Wissen* zu untersuchen, welche Beeinträchtigungen wesentlicher Schutzobjekte (etwa Daten oder Systeme sowie deren Komponenten und Schnittstellen) unabhängig von den ungewissen Ursachen eines Ereignisses zu hohen Auswirkungen für die Schutzgüter führen können, mithin kritisch sind.[516] In Abhängigkeit von dieser Kritikalität sind dann im Rahmen der abstrakten Angemessenheit (dazu sogleich) entsprechende Resilienzmaßnahmen zu ergreifen, um diese Schutzobjekte besonders zu sichern.

Der zweite methodische Ansatz der Resilienz richtet sich auf das *bekannte Nicht-Wissen*. Die klassische Risikomethodik steht insoweit nach wie vor an erster Stelle: Zunächst sind die Risiken, die als solche antizipiert werden können, d.h. über die Wissen vorliegt oder zumindest erzeugt werden kann, im Rahmen der „klassischen" Risikomethodik zu bewältigen. Soweit sich im Rahmen der Risikoidentifikation und -analyse aber herausstellt, dass ein

515 S. 170 ff.

516 Vgl. *Sharkov*, in: Multari/Singhal/Manz, Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense - SafeConfig'16, 3 (5); *Alderson*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 66 (71).; *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (126).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bereich des bekannten Nicht-Wissens besteht[517] sind hierfür entsprechende Resilienzmaßnahmen vorzusehen. Für den Umfang der Maßnahmen ist wiederrum auf die Kritikalität des jeweiligen, mit Ungewissheit behafteten Schutzobjekts[518] im Rahmen der abstrakten Angemessenheit (dazu sogleich) abzustellen. Der Unterschied zum ersten Ansatz liegt darin, dass sich anhand der Risikomethodik der Bereich der Ungewissheit bereits entsprechend als bekanntes Nicht-Wissen eingrenzen lässt.

Als Zwischenfazit lässt sich insoweit festhalten: Die Resilienz steht nicht losgelöst von der klassischen Risikomethodik, sondern ergänzt diese hinsichtlich bestehender Ungewissheit. Sowohl mit der Resilienz als auch der Risikomethodik wird eine Reduktion der naturalistischen Risiken für die jeweiligen Schutzgüter angestrebt. Der Unterschied besteht darin, dass die Resilienz kein Wissen über die spezifischen Einzelrisiken voraussetzt. Sofern ein Fall des bekannten Nicht-Wissens vorliegt, ergibt sich bereits aus der Risikoidentifikation und -analyse hinsichtlich welcher Schutzobjekte Ungewissheit besteht. Hinsichtlich unbekannten Wissens und unbekannten Nicht-Wissens ist hingegen eine selbstständige Kritikalitätsanalyse durchzuführen, d.h. welche Schutzobjekte für die jeweiligen Schutzgüter von besonderer Bedeutung sind und somit auch in Ungewissheit konkreter Risiken besonders geschützt werden müssen.

(2) Angemessenheit von Resilienzmaßnahmen

Im Ergebnis zielt die Risikomethodik der DSGVO wie bereits voranstehend beschrieben auf die Herstellung eines „angemessenen Schutzniveaus". Die Angemessenheit ist dabei ein Ausdruck des Verhältnisses von Aufwand bzw. Kosten der Maßnahmen und der damit erreichten Risikoreduktion.[519]

Das Verhältnismäßigkeitsprinzip muss an sich auch für die Resilienzmaßnahmen gelten. Allerdings kann der Nutzen von Resilienzmaßnahmen nicht in Form der Risikoreduktion bemessen werden, da diese wie die Risiken selbst unbekannt bzw. ungewiss ist. Um den Auftrag zu Resilienzmaßnahmen auch mit Blick auf die kritischen Schutzobjekte nicht grenzenlos

517 Vgl. *Scherzberg*, in: Engel/Halfmann/Schulte, Wissen, Nichtwissen, unsicheres Wissen, 113 (137), der fordert, dass „erkennbare Ausmaß des Nichtwissens" im Risikomanagement zu berücksichtigen.

518 Je nach Einwirkungsmöglichkeit des Schutzobjekts, bei dem ein Nicht-Wissen erkannt wurde sind mehr oder weniger Resilienzmaßnahmen erforderlich.

519 Siehe hierzu bereits S. 167.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

werden zu lassen, muss dem Aufwand folglich ein anderer Anknüpfungspunkt zur Abwägung gegenübergestellt werden.

Als Alternative zur Bemessung des Nutzens in Form der konkreten Risikoreduktion bietet es sich insofern an auf die Schutzgüter, mithin die Rechte und Freiheiten natürlicher Personen an sich abzustellen. Insoweit ist zu untersuchen, welche (Kategorien von) Schutzgüter(n) betroffen sind (in der DSGVO stets Grundrechte, z.B. das Datenschutzgrundrecht oder das Diskriminierungsverbot)[520] und welche Beeinträchtigungen an diesen drohen. Dies ergibt sich gemäß Art. 32 Abs. 1 DSGVO aus *der Art, dem Umfang, der Umstände und der Zwecke der Verarbeitung*.[521] Dabei ist bei personalisierten Diensten auch auf die jeweiligen Entscheidungen abzustellen (z.B. Personalisierung von Produktwerbung oder aber die Personalisierung eines politischen Informationsangebots). Es kann außerdem angenommen werden, dass die Bedrohung der Schutzgüter umso intensiver ist, je mehr und je sensiblere Daten verarbeitet werden bzw. je weiter der als Verarbeitungszweck erbrachte Dienst in die persönliche Lebenssphäre der betroffenen Personen hineinreicht.[522] Dabei sind auch die aus der Verarbeitung allgemein resultierenden *Schäden bzw. Schadkategorien* (EG 75 DSGVO) zu berücksichtigen.

Diese Betrachtung, in der die Kosten für Resilienzmaßnahmen zu der abstrakten Exposition ins Verhältnis gesetzt werden, kann als *„abstrakte Angemessenheit"* bezeichnet werden. Demgegenüber steht die schon beschriebene *risikobezogene Angemessenheit,* die sich mit den Kosten für Maßnahmen befasst, mit denen die Risiken für antizipierte Ereignisse mit deren Eintrittswahrscheinlichkeiten und Folgen gesenkt werden sollen.

(3) Resilienzlernen und Risikomanagement-Iteration

Wie im Rahmen der Wortlautdefinition herausgearbeitet, umfasst die Resilienz auch die lernende Verbesserung in der Erholungsphase. In Abgrenzung der Resilienz als Antwort auf Ungewissheit zum Risikomanagement ist hierbei besonders zu differenzieren: Das Risikomanagement geht

520 Siehe hierzu bereits S. 106.

521 Als „Steuerungsvariablen der Sicherheitsrelevanz" bezeichnet von: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn 55.

522 Vgl. *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 27; *Freund*, in: Schuster/Grützmacher, IT-Recht 2020, Art. 32 DSGVO, Rn. 20.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

zwangsläufig von einem begrenzten Wissen aus, auf dessen Basis die Risiken zunächst identifiziert und anschließend analysiert, bewertet und behandelt werden. Dies ist jedoch kein statischer Zustand: Wird neues Wissen über neue Ereignisse und damit Einzelrisiken verfügbar, so ist das Risikomanagement zu wiederholen (Iteration, s.o.: S. 168). Dieses Lernen (etwa beim Auftauchen und ggf. auch der Ausnutzung einer bislang unbekannten Schwachstelle) durch Schließung derselben ist bereits methodischer Bestandteil des Risikomanagements in Form der Iteration.

Soweit es die Resilienz betrifft, ist das Lernen mithin in systematischer Abgrenzung nur auf die eigentlichen Resilienzmaßnahmen zu beziehen, d.h. auf einen künftigen besseren Umgang mit (weiterhin verbleibender) Ungewissheit (lernende Verbesserung). Es wird insoweit kein *explizites Wissen* über neue Einzelrisiken wie in der Iteration des Risikomanagements genutzt, sondern die Resilienzmaßnahmen werden durch *implizites Wissen* für den Umgang mit Ungewissheit weiter optimiert und verbessert. Implizites Wissen meint im Umkehrschluss kein Wissen über Einzelrisiken, sondern vielmehr übergeordnetes Wissen über Bewältigungsstrategien, die v.a. auf Erfahrung und Intuition basieren.[523]

Kondensiert auf die einzelnen Elemente der Resilienz betrifft dies zunächst die (fortlaufende) Verbesserung der Ereigniserkennung. Heutige ML-basierte Anomalie-[524] und Angriffserkennungssysteme bewältigen ständig Ungewissheit, indem sie die eingehenden Datenflüsse fortlaufend auswerten und sich dabei kontinuierlich verbessern (inkrementelles bzw. online Lernen).[525] Damit sind sie auch für künftige ungewisse Angriffe, etwa durch noch subtiler manipulierte Daten, besser gerüstet. Hier wird insofern auch gerade kein explizites Wissen erzeugt, vielmehr beruhen sie auf der „Erfahrung" des ML-Systems und sind aufgrund des Blackbox-Charakters solcher Systeme auch nicht als explizites Wissen erklärbar. Weiterhin ist eine Verbesserung der Anpassungsmöglichkeiten denkbar, etwa in Form besserer Strategien der Resilienzsysteme (z.B. bei der Netzwerksegmentierung). Schließlich können auch die Erholungsfähigkeiten optimiert werden, etwa in Form einer schnelleren Wiederherstellung des Normalzustandes.

523 Vgl. *Scherzberg*, in: Schuppert/Voßkuhle, Governance von und durch Wissen, 240 (242, 244).

524 Siehe in einem Überblick: *Nassif et al.*, IEEE Access, Vol. 9 (2021), 78658 (78658 ff.).

525 Vgl. *Müller-Quade et al.,* Whitepaper: Künstliche Intelligenz und IT-Sicherheit, April 2019, S. 6 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

(4) Zusammenfassung der Methodik

Die Resilienz gibt somit insgesamt eine Antwort auf ungewisse Ereignisse, indem sie abstrakt angemessene Maßnahmen zur Sicherung verlangt, mit denen ein Ereignis erkannt, sich daran angepasst oder sich schnellstmöglich davon erholt werden kann.

Resilienz setzt nicht an Einzelrisiken an, sondern auf einer höheren Ebene. Man könnte auch formulieren, dass im Sinne von verketteten Ereignissen die *Resilienz* nicht am Anfang einer oder mehrerer Kausalketten ansetzt, sondern bei einem auf ungewissen Ursachen beruhenden, höherrangigen Ereignis sicherstellt, dass angesichts dessen die Schutzgüter gleichwohl noch gesichert werden. Dies gilt sowohl für die Ungewissheit, die im Rahmen der Risikomethodik zumindest erkannt und eingegrenzt werden kann (bekanntes Nicht-Wissen) als auch für vollständig ungewisse Ereignisse an kritischen Schutzobjekten (unbekanntes Wissen, unbekanntes Nicht-Wissen).

Die Ergebnisse werden in der nachfolgenden Grafik zusammengefasst:

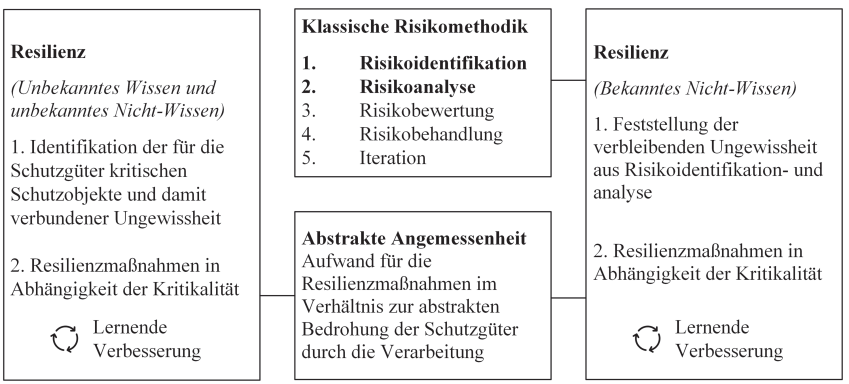

Abbildung 9: Risiko- und Resilienzmethodik

iii. Ergebnis und Folgen für den Resilienzbegriff

Im Ergebnis sind aus der Gegenüberstellung der Resilienz zum Risiko folgende systematische Auslegungsergebnisse festzuhalten:

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Zunächst adressiert die Resilienz anders als das Risiko im entscheidungstheoretischen Sinn die Bewältigung von Ungewissheit.[526] Die Ungewissheit besteht dabei aus den Komponenten der (Un)Bekanntheit und des (Nicht-)Wissens: In der Folge bestehen drei Kategorien, namentlich: *bekanntes Nicht-Wissen*, *unbekanntes Wissen* und *unbekanntes Nicht-Wissen*. Bekanntes Nicht-Wissen ist gegeben, wenn Wissen entweder absolut nicht verfügbar ist oder zumindest nicht mit vernünftigem Aufwand gehoben werden kann (Nicht-Wissen) und dies dem Entscheider bekannt ist (z.B. bei Einsatz einer KI-Komponente). Unbekanntes Wissen besteht dabei in den Fällen, in denen an sich vorhandenes Wissen nicht genutzt wird (z.B. wenn unbemerkt Konfigurations- oder Programmierfehler auftreten). Unbekanntes Nicht-Wissen liegt schließlich vor, wenn dem Entscheider das Nicht-Wissen nicht mal bekannt ist, weil er mit dem zugehörigen Ereignis in keiner Weise rechnet (z.B. global wirkende Sicherheitslücken wie *Heartbleed* in OpenSSL).

Die Ungewissheit kann sich dabei sowohl vollständig auf Ereignisse und damit verbundene Risiken erstrecken als auch nur auf die Eintrittswahrscheinlichkeit oder die Folgenschwere. Soweit Eintrittswahrscheinlichkeit und Folgenschwere ungewiss sind, können alle drei Kategorien der Ungewissheit vorliegen. Ist hingegen nur die Eintrittswahrscheinlichkeit oder die Folgenschwere ungewiss, liegt ein Fall des bekannten Nicht-Wissens vor.

Methodisch steht die Resilienz *komplementär neben der Risikomethodik*, indem sie entweder die verbleibende, bekannte Ungewissheit aus Risikoidentifikation und -analyse oder das unbekannte Wissen- bzw. Nicht-Wissen bzgl. der für die Schutzgüter besonders kritischen Schutzobjekte adressiert. Insofern ist bei der Vornahme von Resilienzmaßnahmen entweder an der bekannten Stelle der Ungewissheit (bekanntes Nicht-Wissen) anzusetzen, oder es sind, in Unkenntnis woher die Ungewissheit droht, von den Schutzgütern her gedacht die besonders kritischen Schutzobjekte zu sichern. Sachlich setzt die Resilienz in beiden Fällen nicht an dem Beginn einer Ereigniskette (einem Einzelrisiko wie etwa einem Angriff), sondern an einem i.d.R. höherrangigen Ereignis an, dessen Ursachen ungewiss sind.

Um trotz der Ungewissheit eine Angemessenheit der Resilienzmaßnahmen zu gewährleisten, ist der damit verbundene Aufwand methodisch statt mit der Risikoreduktion mit der aus der Verarbeitung resultierenden abstrakten Bedrohung der zu sichernden Schutzgüter abzuwägen. Schließlich

526 Zur Cyberresilienz als Antwort auf Ungewissheit (en: uncertainty) vgl. auch: *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2, 7 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ist das Lernen in der Erholungsphase der Resilienz als Optimierung von Resilienzmaßnahmen von der fortwährenden Erweiterung der Wissensbasis über Einzelrisiken innerhalb der Iteration des Risikomanagements zu unterscheiden.

2. Schutzziele nach Art. 32 Abs. 1 lit b) DSGVO

Im nun folgenden Abschnitt der systematischen Auslegung soll zweitens untersucht werden, wie sich die Resilienz zu der bestehenden Trias der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) verhält, die in Art. 32 Abs. 1 lit b) DSGVO neben der Resilienz und bezogen auf Systeme und Dienste genannt werden.

Hierfür wird zunächst eine historische Herleitung der Schutzziele in der Informationssicherheit vorgenommen (a.). Anschließend folgt eine Betrachtung der Entwicklung der Schutzziele im Datenschutzrecht (b.) und schließlich eine Beschreibung der Schutzziele in Art. 32 Abs. 1 lit b) DSGVO mit Blick auf die neuen Schutzobjekte Systeme und Dienste (c.) Nach einem Zwischenfazit zu den Schutzzielen (d.) wird erläutert, wie sich die Resilienz demgegenüber einordnet (e.).

a. Historische Entwicklung

Wesensmäßig taucht der Dreiklang dieser Schutzziele in der Informationssicherheit bereits in den 1970er Jahren als drei Kategorien „potenzieller Sicherheitsverletzungen" in informationstechnischen Systemen auf:[527]

1. Die unautorisierte Informationsfreigabe: Die Informationen können von einer nicht autorisierten Person gelesen und ausgenutzt werden. Auch die entsprechende Beobachtung des Informationsflusses sowie die unautorisierte Nutzung von Programmen wird hierunter gefasst (entspricht: Vertraulichkeit).
2. Die unautorisierte Informationsveränderung: Eine unautorisierte Person kann Änderungen an gespeicherten Informationen vornehmen (entspricht: Integrität).

527 *Saltzer/Schroeder*, Proc. IEEE 1975, 1278 (1280); *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (547 f.)

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Die unautorisierte Nutzungsverweigerung: Eine nicht autorisierte Person kann autorisierte Benutzer daran hindern, Informationen zu nutzen oder zu verändern (entspricht: Verfügbarkeit).

Zu beachten ist, dass die Schutzziele hier noch ausschließlich auf „Informationen" bezogen wurden und nicht etwa auf Systeme oder Dienste. Allerdings bezog die Definition von Sicherheit (en: Security) auch hier schon sowohl Maßnahmen zur Kontrolle der Nutzung oder Modifikation der gespeicherten Informationen als auch „des Computers" selbst mit ein.[528]

Auch in der Netzwerk-Sicherheit wurden die Schutzziele bald aufgegriffen. Angriffe auf die Vertraulichkeit und Integrität wurden dabei als (aktive) Sabotageakte klassifiziert. Umgekehrt wurden bloße Angriffe auf die Vertraulichkeit mitunter auch als „passive Angriffe" bezeichnet, da sie die Informationsverarbeitung bzw. den Informationsfluss nicht stören.[529] Im Weiteren wurden außerdem Angriffe auf die Authentizität etwa durch Veränderung der Metadaten aufgeführt,[530] wodurch eine falsche Zuordnung der Inhalte bewirkt werden kann. Umgekehrt werden Änderungen der Inhaltsdaten als Angriffe auf die Integrität von Informationen qualifiziert.[531]

Wenig später im Jahr 1985 schuf das US-Verteidigungsministerium einen Katalog von sog. „Trusted Computer System Evaluation Criteria". Auch hier galt als grundlegende Anforderung für die „Computersicherheit" die „*Verwendung spezifischer Sicherheitsfunktionen, so dass nur ordnungsgemäß autorisierte Personen oder Prozesse, die in ihrem Namen arbeiten, Zugriff auf Informationen haben und diese Lesen, Schreiben, Erstellen oder Löschen können.*"[532] Durch die Beschränkung des Zugriffs auf einen autorisierten Personenkreis steht dabei zunächst die Vertraulichkeit im Vordergrund. Die Nennung der unterschiedlichen Berechtigungen, insbesondere des Schreibens und Löschens legt daneben auch die Integrität und Verfügbarkeit von Informationen mit an.

528 *Saltzer/Schroeder*, Proc. IEEE 1975, 1278 (1279).
529 *Voydock/Kent*, ACM CSUR 1983, 135 (140, 142).
530 Dort statt „Metadaten" „protocol control information": *Voydock/Kent*, ACM CSUR 1983, 135 (142).
531 Wie zuvor.
532 En: "In general, secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information." DoD, Trusted Computer System Evaluation Criteria, 26.12.1985, S. 9.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

b. Einführung im deutschen und europäischen Datenschutzrecht

Im BDSG a.F.[533] war die Datensicherheit in § 9 und der zugehörigen Anlage geregelt. Die zwischenzeitlich weltweit standardisierten klassischen Schutzziele „Verfügbarkeit, Vertraulichkeit und Integrität" wurden dort, trotz intensiver Kritik,[534] bis zuletzt nicht ausdrücklich implementiert. Teilweise wurden die Schutzziele von der Literatur aber gleichwohl in die Anforderungen hineingelesen.[535]

Die Landesdatenschutzgesetze (LDSG) waren dagegen zum Teil schon weiter fortgeschritten. So setzte das LDSG in Schleswig-Holstein (SH)[536] in „§ 5 - Allgemeine Maßnahmen zur Datensicherheit" fest, dass im Rahmen der Datensicherheit durch technisch-organisatorische Maßnahmen u.a. Folgendes zu gewährleisten ist:

1. „Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit),
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität),
3. nur befugt auf Verfahren und Daten zugegriffen werden kann (Vertraulichkeit)."

Auch die DS-RL nannte die Trias der klassischen Schutzziele noch nicht ausdrücklich. Art. 16 stellte nach seiner Überschrift auf die „Vertraulichkeit der Verarbeitung" ab, beschränkte dies aber inhaltlich auf die interne Vertraulichkeit in der Form, dass nach dieser Vorschrift dem Verantwortlichem oder Auftragsverarbeiter unterstellte Personen die personenbezogenen Daten „nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten" dürfen.

---

533 bis zum 24.05.2018, aufgehoben durch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU).

534 *Ernestus*, in: Simitis/Dammann/Arendt, Bundesdatenschutzgesetz, § 9 Rn. 1; *Melling-Schultze*, in: Taeger/Gabel, Kommentar zum BDSG [a.F.], 2. Auflage 2013, § 9, Rn. 42; *Wedde*, in: Däubler, Bundesdatenschutzgesetz [a.F.], 5. Auflage 2016, § 9, Rn. 7.

535 *Bizer*, DuD 2007, 350 (355); als „Verfügbarkeit, Authentizität und Integrität": *Gola/Klug/Körffer*, in: Gola/Schomerus, Bundesdatenschutzgesetz [a.F.], 12. Auflage 2015, § 9, Rn. 2.

536 LDSG SH a.F. vom 09.02.2000 (zuletzt geändert am 16.03.2015), gültig bis zum 23.05.2018.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

In Art. 17 DS-RL „Sicherheit der Verarbeitung" hieß es weiterhin, dass

> *„der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muß [sic!], die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang […] und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind."*

In dieser Vorgabe sind bereits die drei klassischen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität zu erkennen, ohne dabei jedoch (was seinerzeit wie auch im BDSG kritisiert wurde) ausdrücklich benannt zu sein.[537]

Mit der DSGVO ist der Gesetzgeber dieser Forderung erfreulicherweise nachgekommen und hat die Schutzziele darüber hinaus auch noch wie bereits beschrieben in ihrer Bedeutung zwischen Art. 25 und 32 DSGVO weiter konturiert.[538] Außerdem hat er sich dazu entschieden, die Schutzziele nun in Art. 32 Abs. 1 lit b) DSGVO auch mit Bezug auf „Systeme und Dienste" in seine Sicherheitsanforderungen aufzunehmen (dazu sogleich ausführlich).

c. Vorkommen und Auslegung in der DSGVO

Die genannten Schutzziele „Verfügbarkeit, Vertraulichkeit und Integrität" werden in der DSGVO in Art 25 i.V.m. Art 5 Abs. 1 lit f. sowie in Art 32 Abs. 1 lit b), lit c), Abs. 2 ausdrücklich genannt.

Der Gesetzgeber hat die Schutzziele in der DSGVO nicht nur das erste Mal ausdrücklich normiert, sondern sie nun auch auf neue Schutzobjekte ausgedehnt. Wie voranstehend gezeigt, wurden die Schutzziele bis dahin wie etwa im LDSG SH überwiegend auf Daten bezogen; § 5 LDSG SH erstreckte die Verfügbarkeit und Vertraulichkeit zumindest noch auf „Verfahren".

Nun bezieht Art. 32 Abs. 1 lit b) DSGVO die klassischen Schutzziele im Kontext der Datensicherheit auf „Systeme und Dienste" im Zusammenhang mit der Verarbeitung. Diese Begriffe wurden bereits eingangs grundlegend

537 *Bock/Meissner*, DuD 2012, 425 (427, 432), verbunden mit der Forderung an den europäischen Gesetzgeber die Schutzziele ausdrücklich zu normieren.

538 Siehe oben: S. 90 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

definiert, wobei die Frage einer soziotechnischen Auslegung des Systembegriffs für die Resilienz zwar im Rahmen der Auslegung nach dem Wortlaut bejaht wurde, für die Schutzziele aber bislang offen ist. Im Rahmen der Definition des Systems wurde auch erläutert, dass die personenbezogenen Daten im Sinne des Art. 32 DSGVO nicht als Teil des Systems zu verstehen sind[539] und die Schutzziele sich an dieser Stelle somit auch nicht auf die personenbezogenen Daten beziehen. Nach anderer Ansicht sind hingegen alle Schutzziele[540] und v.a. die Vertraulichkeit[541] in Art. 32 Abs. 1 lit b) DSGVO (auch) auf die Daten zu beziehen. Allerdings sind alle Schutzziele durch Art. 32 Abs. 1 lit c), Abs. 2 DSGVO schon auf die personenbezogenen Daten bezogen, so dass sich durch eine solche Ausdehnung in der Sache kein Unterschied ergibt. Zu Unterschieden kommt es nur dann, wenn einzelne Schutzziele wie etwa die Vertraulichkeit (dazu sogleich) nur auf Daten und nicht eigenständig auf Systeme bezogen werden.

Im Weiteren wird deshalb auf den Inhalt der Schutzziele in Bezug auf Systeme und Dienste eingegangen und an geeigneter Stelle auch auf die unterschiedliche Bedeutung der Schutzziele bei der Anwendung auf personenbezogene Daten hingewiesen. Die Neuausrichtung der klassischen Schutzziele auch auf Systeme und Dienste verdient auch deshalb besondere Beachtung, weil im Datenschutzrecht die Sicherheit von Systemen und Diensten nach den Schutzgütern traditionell eine geringere Rolle einnimmt als etwa im IT-Sicherheitsrecht. Bei letzterem ist die Funktionsfähigkeit auch der Systeme und Dienste selbst von besonderer Bedeutung, weil deren informationsverarbeitende Tätigkeit für die Erbringung einer kritischen Versorgungsleistung benötigt werden.

Im Datenschutzrecht hingegen liegt der Fokus bei der Verarbeitung stärker auf den dabei genutzten personenbezogenen Daten. Durch die Verarbeitung sollen die Rechte und Freiheiten natürlicher Personen nicht beeinträchtigt werden; so sollen etwa insbesondere unbefugte Offenlegungen der personenbezogenen Daten verhindert werden. Die fehlende Funktionalität eines Systems oder eines Dienstes führt hingegen nicht per se zu einer Beeinträchtigung der Schutzgüter, sondern diesen kommt wie bereits zuvor dargestellt eine Vorfeldschutzfunktion zu.[542]

539 Siehe oben: S. 115.
540 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 35d ff.
541 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 38.
542 Siehe oben, S. 111.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Entsprechende Ausnahmen und die damit verbundenen Bedeutung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit (i. – iii.) an Systemen und Diensten werden im Folgenden dargestellt.

i. Verfügbarkeit

Die Verfügbarkeit von Systemen beschreibt pointiert deren „jederzeitige Nutzungsmöglichkeit".[543] Für das Datenschutzgrundrecht ist die Verfügbarkeit von Systemen insbesondere aus Gründen der Transparenz[544] geboten:

Die Systeme und Dienste ermöglichen den Zugriff auf die erhobenen personenbezogenen Daten sowie die daraus erzeugten Informationen. Ist der Zugriff nicht mehr möglich, kann der betroffenen Person keine Auskunft mehr erteilt werden bzw. sie kann die Daten auch nicht mehr einsehen. Dies ist zur aktiven Wahrnehmung des Rechts auf informationelle Selbstbestimmung bzw. des Datenschutzgrundrechts und damit zur Verwirklichung dieses Schutzgutes indes erforderlich, etwa um zu prüfen, ob die personenbezogenen Daten rechtmäßig auf Basis eines Erlaubnistatbestandes sowie entsprechend der Datenschutzgrundsätze verarbeitet wurden.[545] Konkret kann beispielsweise nur so überprüft werden, ob nur die für den Zweck tatsächlich erforderlichen Daten erhoben wurden (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit c) DSGVO). Dasselbe gilt für die Verfügbarkeit von Diensten, die etwa für die o.g. Auskunftserteilung erforderlich sind.

Wenn ein Dienst verfügbar sein soll, schließt dies notwendigerweise auch die Verfügbarkeit des Systems mit ein. Denkbar ist umgekehrt aber, dass ein System noch verfügbar ist und nur ein von diesem System bereitgestellter Dienst ausgefallen ist. Ob die Verfügbarkeit (auch) die ordnungsge-

543 *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn 25; ähnlich auch *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

544 Vgl. mit Verweis auf die Nachweispflichten der DSGVO: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 38b.

545 Vgl. *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (214); *Kramer/Meints*, in: Auernhammer, DSGVO BDSG, 7. Auflage 2020, Art. 32, Rn. 43.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

mäße Funktionsweise[546] (also das „Wie") erfasst oder nur wie hier zunächst beschrieben das „Ob" der Funktionsfähigkeit, ist zweifelhaft. Dies erscheint insbesondere in Abgrenzung zur Integrität problematisch (dazu sogleich).

ii. Integrität

Die Integrität von Systemen ist im IT-Recht bereits durch das BVerfG bekannt, soweit dieses im Rahmen seiner Entscheidung zur sog. „Online-Durchsuchung"[547] die Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelte. Diese nationale grundrechtliche Definition kann zumindest als indizielle Auslegungshilfe für den Begriff der „Integrität" in der DSGVO herangezogen werden.

Die Integrität eines IT-Systems ist nach dem BVerfG beeinträchtigt, sobald „auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können" und so die „entscheidende technische Hürde für die Ausspähung, Überwachung oder Manipulation des Systems" genommen ist.[548] Die Schutzziele Vertraulichkeit und Integrität stehen hier insofern in einer sehr engen Verknüpfung, da die Vertraulichkeit der im System enthaltenen Daten nicht mehr gewährleistet werden kann, wenn das System etwa durch eingebrachte *Spyware*[549] in seiner Integrität verletzt ist.

546 *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 58; zu § 9 BDSG a.F. bereits *Hennrich*, Cloud Computing, S. 208 m.w.N.

547 *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (822 ff.).

548 *BVerfG,* a.a.O., S. 827, Rn. 204. Deutlich erkennbar wird aus dieser Definition die korrespondierende Angriffssicht, die sich daraus ergibt, dass mit dem Urteil das o.g. Grundrecht in seiner Abwehrdimension gegen einen staatlichen Zugriff auf das IT-System durch den sog. „Staatstrojaner" beschrieben wurde, siehe auch: *Stadler*, MMR 2012, 18 (18, 20).

549 Spyware ist eine client-seitige, d.h. auf einem Endgerät installierte Schadsoftware, die unautorisiert Informationen auf diesem Endgerät aufzeichnet und an ein externes System übermittelt, Vgl. *Stamminger et al.*, in: Samarati, Information Security, 202 (205).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Die so beschriebene *Systemintegrität* ist somit auch strikt zu unterscheiden von der Integrität der personenbezogenen Daten.[550] Letztere wird gesondert in Art. 32 Abs. 2 DSGVO adressiert.[551] Hinsichtlich des Schutzzwecks der Systemintegrität greift erneut die schon angesprochene Perspektive des Vorfeldschutzes: Sind die Systeme selbst integer, also insbesondere frei von Schadsoftware, können sie die Vertraulichkeit sowie die anderen Schutzziele an den personenbezogenen Daten sicherstellen.[552] Z.T. wird unter Integrität von Systemen auch (nur) deren „korrekte Funktionsweise"[553] verstanden, die durch eine (etwa nur ausspähende Korrumpierung) abhängig vom Verständnis dieser Anforderung zumindest noch nicht zwingend beeinträchtigt ist. Dieses Verständnis dürfte daher (insbesondere in Abgrenzung zur Verfügbarkeit) zu kurz greifen.

In der Gesamtschau auch mit Blick auf die Erkenntnisse aus dem genannten Urteil des BVerfGs sollte die Integrität als Anforderung verstanden werden, wonach der Zustand des Systems frei von allen Manipulationen sein soll, die sich auf den Schutz der personenbezogenen Daten auswirken können. Andere Beeinträchtigungen, die sich auf die Funktion auswirken können, etwa technisches Versagen von Komponenten (Hardware-Defekte) sind dagegen mangels Manipulationstatbestand *dem Schutzziel der Verfügbarkeit* (des Systems bzw. des Dienstes) zuzuordnen.

Die *Integrität des Dienstes*, also die Integrität der Funktionalität eines Systems, kann als die Manipulationsfreiheit des erzeugten Ergebnisses verstanden werden. Dies umfasst nach dem im 2. Kapitel, A. vorgestellten Modell sowohl die Erzeugung unrichtigen Personenwissens (etwa einer tatsächlich nicht bestehenden Präferenz) als auch im Folgeschritt eine vom Dienst getroffene Entscheidung im Rahmen einer Personalisierung (ein individuelles Preisangebot, eine Empfehlung eines bestimmten Produkts oder Posts).

---

550 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (406), Rn. 40; *Bedner/Ackermann*, DuD 2010, 323 (326); a.A. *Mantz*, in: Sydow/Marsch, DS-GVO, BDSG, 3. Auflage 2022, Art. 32, Rn 14, der hinsichtlich der Nichterfassung der personenbezogenen Daten von einer „sprachlichen Ungenauigkeit" des Gesetzes ausgeht.

551 Vgl. *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 61.

552 Vgl. *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (406), Rn. 40.

553 *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

iii. Vertraulichkeit

Die Vertraulichkeit von Daten stellt wohl das bedeutendste Element der Datensicherheit dar. Umso wichtiger ist es, die Vertraulichkeit des Systems hiervon sauber abzugrenzen.[554] Als erster Anhaltspunkt für das Verständnis der Vertraulichkeit kann wiederrum auf das vom BVerfG geprägte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" abgestellt werden. Allerdings betrifft auch dieses Grundrecht im Detail mit der Vertraulichkeit die im „informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten".[555] Anders als bei dem Recht auf informationelle Selbstbestimmung geht es dabei allerdings noch nicht um ein konkretes personenbezogenes Datum, sondern übergreifend um alle personenbezogenen Daten, die einem informationstechnischen System „anvertraut" werden oder allein schon durch dessen Nutzung erzeugt werden.[556] Die „Vertraulichkeit des informationstechnischen Systems" stellt mithin hier im Ergebnis auf die Gesamtheit bzw. das Potential an darin verarbeiteten personenbezogenen Daten und nicht auf das System selbst ab. Dies entspricht auch den datensicherheitsrechtlichen Definitionen von Vertraulichkeit, in dem diese als der Schutz vor unbefugter Preisgabe von Informationen beschrieben wird.[557]

Insofern ist festzustellen, dass der Vertraulichkeitsbegriff auch hier stark mit Daten verknüpft ist; die Frage der Vertraulichkeitsanforderung an Systeme ist damit aber noch nicht beantwortet. In Anknüpfung an den Wortlaut und die Systematik von Art. 32 Abs. 1 lit b), Abs. 2 DSGVO sollte die Trennung zwischen Schutzzielen an personenbezogenen Daten einerseits und an Systemen und Diensten andererseits aufrechterhalten werden.

Zur Auflösung des Widerspruchs zwischen dem Wortlaut der Vertraulichkeit des Systems und der definitorischen Bindung der Vertraulichkeit an die Daten können hier anstelle der bereits adressierten personenbezogenen Daten die *systembezogenen Daten* zugrunde gelegt werden. Zu schützen sind damit jene Daten über die innere Struktur des Systems, die entsprechende Zustände oder Eigenschaften des Systems beschreiben. Beispiele sind etwa Daten über Versionen von Betriebssystemen, installier-

554 a.A. erneut *Mantz*, Fn. 550.
555 *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (827), Rn. 204.
556 *BVerfG*, a.a.O., Rn. 200.
557 *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

te Software, Update-Zustände sowie über die verwendete Hardware. Die rechtliche Anforderung der Vertraulichkeit dieser systembezogenen Daten lässt sich telelogisch wiederrum durch den Vorfeldschutz erklären. So könnte beispielsweise das Datum einer veralteten Softwareversion entsprechend für Angriffe ausgenutzt werden und somit im Ergebnis den Schutz personenbezogener Daten gefährden. Aus dieser Sicht heraus kann dem Schutzziel der Vertraulichkeit ein sinnvoller Anwendungsbereich bezüglich der Systeme zugewiesen werden. Die Vertraulichkeit umfasst insoweit den Schutz vor einem Ausspähen des Hardware-Designs oder des Software-Codes,[558] denn ebendies könnte spätere Angriffe zur Offenlegung, Manipulation oder Vernichtung personenbezogener Daten erleichtern.

Die *Vertraulichkeit des Dienstes* ist nur insofern abgrenzungsfähig, als dass es bei dem Dienstergebnis wie einer personalisierten Empfehlung um das Verarbeitungsergebnis handelt, dass ggf. in besonderer Weise schutzwürdig ist. Gleichwohl wird dieses Ergebnis als personenbezogenes Datum ausgedrückt, so dass keine kategorische Abgrenzung möglich ist. Insgesamt spricht somit in der Auslegung viel dafür, der Vertraulichkeit des Dienstes hier (anders als bei dem System) keinen eigenen Anwendungsbereich zuzugestehen.

d. Zusammenfassung

Ausgangspunkt war die Frage, wie die Schutzziele an Systemen und Diensten in Art. 32 Abs. 1 lit b) DSGVO zu beschreiben sind.

Diese Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität werden heute als die „klassischen Schutzziele der Datensicherheit" verstanden.[559] Aus der historischen, technischen Betrachtung heraus lassen sie sich allgemein definieren als „die erwünschte Fähigkeit eines Informationssystems einer bestimmten Kategorie von Bedrohungen zu widerstehen."[560] Juristisch zugeschnitten sind sie als Anforderungen an ein System oder einen Dienst zu verstehen, die zur Sicherung bestimmter Schutzgüter eingehalten wer-

558 Ebendies explizit ablehnend: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 38.

559 *F. Ritter/Reibach/Lee*, ZD 2019, 531 (532); *M. Rost*, DuD 2018, 13 (13 f.); *Trautwein/Kurpierz*, PinG 2018, 26 (29).

560 Vom Verfasser übersetzt aus *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (548).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

den müssen.[561] Als eine solche erwünschte Fähigkeit bzw. zu erfüllende Anforderung drücken sie zugleich einen bestimmten „Sollzustand“[562] aus, der angestrebt und möglichst erhalten werden soll.[563]

Insoweit stellen Schutzziele auch ein Maß für die gewährleistete Sicherheit dar. Umgekehrt folgt aus dem Zuschnitt auf „bestimmte Kategorien von Bedrohungen“ zugleich eine gewisse Bündelung von Maßnahmentypen, ohne allerdings ein exklusives Maßnahme-Schutzziel-Verhältnis zu begründen. Vielmehr existieren auch Maßnahmen, die mehreren Schutzzielen zugleich dienen (z.B. dient die in Art. 32 Abs. 1 lit a) DSGVO geforderte Verschlüsselung von Daten sowohl deren Integrität als auch deren Vertraulichkeit).[564]

Die Schutzziele in Art. 32 Abs. 1 lit b) DSGVO beziehen sich nur auf das technische System mit seinen Bestandteilen, d.h. auf die IT-Infrastruktur im engeren Sinn in Form der Hard- und Software.[565] Dies umfasst sowohl das System als auch den vom System erbrachten Dienst. Es wurden gegenüber den Schutzzielen an personenbezogenen Daten eigenständige Definitionen für die Verfügbarkeit und Integrität von Systemen und Diensten sowie die Vertraulichkeit von Systemen ermittelt.

Hingegen können die Schutzziele und insoweit auch der Systembegriff nicht auf die mitwirkenden natürlichen Personen erstreckt werden,[566] da die technischen Schutzziele auf diese keine definitorisch sachgerechte Anwendung finden können. Gleichwohl sind zur Gewährleistung der Schutzziele an dieser IT-Infrastruktur neben baulichen Maßnahmen (Zutrittskontrolle) auch Maßnahmen „an den“ bzw. für die Mitarbeitenden (z.B.

561 *Schmitz/Dall'Armi*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 32.

562 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (404), Rn. 33; Als „Zielbestimmungen“: *Bock/Meissner*, DuD 2012, 425 (426).

563 Soweit die Schutzziele auf Daten bezogen sind, lassen sie sich entsprechend definieren als eine erwünschte Eigenschaft von Daten mit Blick auf eine bestimmte Kategorie von Bedrohungen.

564 Vgl. *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 20; Auf der anderen Seite können Maßnahmen für ein Schutzziel auch andere Schutzziele gefährden: So gefährdet etwa die genannte Verschlüsselung von Daten deren Verfügbarkeit, insbesondere wenn es bei der Verschlüsselung zu Fehlfunktionen kommen sollte, *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 32, Rn 30.

565 *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 22; siehe im Übrigen bereits zuvor: S. 114 ff.

566 So aber wohl *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 37.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

entsprechende Schulungen und Sensibilisierungsmaßnahmen) erforderlich. Mitarbeitende müssen etwa geschult werden, um die Integrität der Systeme zu sichern, indem sie beispielsweise keine privaten, externen Speichergeräte in der betrieblichen Umgebung einsetzen. Dabei werden die Mitarbeitenden aber nicht Teil des Systems in dem Sinne, dass sie selbst die Schutzziele wie etwa das technische Erfordernis der „Integrität" erfüllen müssten.

e. Einordnung der Resilienz

Zu untersuchen ist nun, wie sich die Resilienz gegenüber den so beschriebenen Schutzzielen systematisch einordnet. Die Resilienz wird vom europäischen Gesetzgeber in der DSGVO grammatikalisch neben den klassischen Schutzzielen implementiert, die als historisch gewachsene Trias den anzustrebenden Zustand der Daten- und IT-Sicherheit auch heute noch vollständig abzubilden vermag.[567] Insoweit ist fraglich, ob sich die Resilienz als Erweiterung in die Systematik der Schutzziele einfügen und daher ebenfalls als Schutzziel qualifiziert werden kann. Wie die Schutzziele wird die Resilienz dabei auf Systeme und Dienste bezogen.

Teilweise wird die Resilienz als weiteres Schutzziel klassifiziert.[568] Auch inhaltlich wird der Resilienz ein Sollzustand zugewiesen, wie etwa dass ein System oder ein Dienst „auch unter hoher Inanspruchnahmefrequenz ordnungsgemäß funktionieren" können müsste.[569] Damit wird die Resilienz als eine besondere Ausprägung der Verfügbarkeit verstanden.[570] Dem ist jedoch entschieden entgegenzutreten: Die Resilienz stellt weder eine Ausprägung der Verfügbarkeit – dagegen spricht bereits historisch, dass der Gesetzgeber hierfür die Trias der tradierten Schutzziele gerade nicht hätte erweitern müssen – noch ein weiteres, neues Schutzziel dar.

---

567 Vgl. *Samonas/Coss*, JISSec, Vol. 10 (2014), Heft 3, 21 (37 f.).

568 Als weiteres „Sicherheitsziel": *Hladjk*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 32, Rn. 8; im IT-Sicherheitsrecht außerdem: *Klaus et al.*, DuD 2021, 738 (739).

569 So allerdings ohne Verwendung des Schutzzielbegriffs: *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

570 *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 32, Rn. 32; *Voskamp/D. Klein*, in: Kipker, Cybersecurity, S. 279, Rn. 19b; *Karg*, in: Lang/Löhr, IT-Sicherheit, 99 (111).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Vielmehr geht die Gegenansicht zu Recht von einer Sonderstellung dieses Merkmals aus und verneint die Klassifikation als viertes Schutzziel.[571] Betont wird dabei insbesondere der dynamische, funktionale Charakter der Resilienz als die Fähigkeit mit Störungen umgehen zu können.[572] Auch in der technischen Fachliteratur ist dieser Gedanke zu finden, wonach Resilienz keine intrinsische Eigenschaft, sondern eine (aktive) Fähigkeit eines Systems darstellt.[573]

Für letztere Ansicht streitet nach hiesiger Untersuchung neben der Wortlautauslegung in diesem Sinne auch der hier vorgenommene, systematische Vergleich der Resilienz mit den skizzierten Schutzzielen: Hier zeigt sich, dass die Resilienz als funktionale Anforderung den Schutzzielen nachgelagert ist. Die Schutzziele bilden wie beschrieben einen technischen Sollzustand ab,[574] der v.a. die gewährleistete Resistenz eines Systems sowie die Beeinträchtigungslosigkeit der personenbezogenen Daten sowie der Systeme und der Dienste umschreibt. Dieser Sollzustand soll durch die Härtung der Systeme erreicht und gehalten werden. Somit sollen Sicherheitsvorfälle in Form von Schutzzielverletzungen vermieden werden, die zunächst system- bzw. dienstbezogen sind und sodann eine Verletzung des Schutzes personenbezogener Daten (datenbezogener Sicherheitsvorfall) nach sich ziehen können.

Die Resilienz soll neben der Vermeidung von ungewissen Ereignissen insbesondere auch dann durch Anpassung des Systems eingreifen, wenn es bereits zu einem Sicherheitsvorfall gekommen und die Resistenz bzw. der Sollzustand somit bereits durchbrochen ist. Es kommt in diesem Fall auf die Fähigkeit des Systems an, mit diesem Ereignis umgehen zu können und so trotz einer Verletzung der Datensicherheit die Entstehung eines Scha-

571 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 42; *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (446); *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 26; *Laue*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage 2019, Art. 32 DSGVO, Rn. 14; ähnl. von einem „Prinzip" sprechend: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39.

572 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 42 ff.; *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 26; *Heitmann*, IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie, S. 13.

573 *Alderson*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 66 (74); *Hollnagel/Woods*, in: Hollnagel/Woods/Leveson, Resilience engineering, 347 (347 f.).

574 Siehe Fn. 562.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

dens an den Schutzgütern (Rechte und Freiheiten natürlicher Personen) zu vermeiden. Die Resilienz beschreibt somit gerade keinen sicherheitstechnischen Sollzustand (wie die Schutzziele), sondern eine funktionale Eigenschaft des Systems insbesondere im Umgang mit Sicherheitsvorfällen.

Weiterhin ergibt sich hinsichtlich der *Bedrohungssicht* auf Schutzziele ein gravierender Unterschied. Schutzziele lassen sich auch unter Berücksichtigung der historischen Betrachtung als Spiegelbild von bestimmten Bedrohungen bzw. Angriffen verstehen.[575] Ein Angriff auf die „Resilienz" von Systemen und Diensten ist aber jedenfalls strukturell kein finales Angriffsziel wie etwa auf deren Verfügbarkeit oder Integrität. Ein Angriff auf die Resilienz etwa durch Beeinträchtigung der Anpassungsfähigkeit kann vielmehr nur ein Hilfsmittel sein, um den eigentlich von dem/der Angreifer:in erstrebten Erfolg einer Schutzzielverletzung an dem System, dem Dienst oder den verarbeiteten Daten zu erreichen. Umgekehrt dient die Resilienz als Abwehrmechanismus auch nicht wie die anderen schutzzielbezogenen Maßnahmen der Abwehr spezifischer Risiken, sondern entspricht, wie im Rahmen der bisherigen Auslegung herausgearbeitet wurde, eher einer universalen Fähigkeit mit ungewissen, widrigen Ereignissen umgehen zu können.

Ob eine hinreichende Resilienz durch Maßnahmen gewährleistet wurde, kann sich mitunter auch darin ausdrücken, wenn es in Folge eines Ereignisses gerade nicht zu einer Verletzung der Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität kommt.[576] Dabei ist allerdings genau zu differenzieren: Zunächst wird wie beschrieben im Regelfall aufgrund des ungewissen Charakters des Ereignisses ein Sicherheitsvorfall eintreten, etwa die Verletzung der Integrität eines Systems (z.B. Infiltration durch bislang unbekannte Schadsoftware). Gleichwohl kann die Resilienz etwa noch die Vertraulichkeit von Daten gewährleisten, d.h. sicherstellen, dass es trotz dieser der unerwarteten und deshalb nicht zu verhindernden Integritätsverletzung am Schutzobjekt System nicht zu einer Offenlegung, d.h. einer Vertraulichkeitsverletzung an den personenbezogenen Daten kommt (z.B. durch Erkennung der Schadsoftware und einer entsprechenden Zugriffsbegrenzung). Resilienz kann somit eine drohende oder bereits begonnene Kette von Sicherheitsvorfällen bzw. Schutzzielverletzungen unterbrechen. Sie ist jedoch insoweit kein Maß für den Schutz der initial verletzten

575 *Freimuth,* Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, S. 61.

576 Vgl. *Klaus et al.*, DuD 2021, 738 (739); *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (444 f.); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Schutzziele. Dies würde die Abgrenzung zwischen risiko- und schutzzielbezogenen Maßnahmen (z.B. Verschlüsselung von Daten) einerseits und den auf Ungewissheit abzielenden Resilienzmaßnahmen (z.B. Erkennung eines und Reaktion auf einen unautorisierten Datenabfluss) andererseits konterkarieren.

Im Ergebnis bestimmt Art. 32 Abs. 1 lit b) DSGVO damit die drei klassischen Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit sowie zusätzlich die funktionale Anforderung der Resilienz. Die spezifische Systematik des Art. 32 Abs. 1 lit b) DSGVO ist insoweit zu kritisieren, als dass sie diesen Unterschied zwischen den Schutzzielen und der Resilienz nicht deutlich kennzeichnet und darüber hinaus auch eine zweigeteilte Auslegung des Systembegriffs (dazu sogleich ausführlich) notwendig macht.

3. Systeme und Dienste

Nach Art. 32 Abs. 1 lit b) DSGVO bezieht sich die Resilienz sowohl auf *Systeme* als auch auf *Dienste*.

Hinsichtlich der Systeme bestätigt sich als Folge der systematischen Auslegung der Schutzziele die Hypothese, dass der Systembegriff für diese zwar informationstechnisch, *für die andersartige Resilienz aber soziotechnisch zu verstehen ist.* Gerade der Umgang mit bereits eingetretenen Sicherheitsvorfällen verlangt ggf. ein menschliches Eingreifen, um die Resilienz etwa in Form einer Anpassung der Systeme zu gewährleisten.[577] Dagegen sind die Schutzziele selbst aufgrund ihrer technischen Ausrichtung wie bereits dargestellt auf ein technisches Systemverständnis ausgerichtet. Der Begriff der Systeme ist in Art. 32 Abs. 1 lit b) DSGVO mithin zweigeteilt auszulegen – als informationstechnisches System hinsichtlich der Schutzziele und als soziotechnisches System hinsichtlich der Resilienz.

Zum Begriff des Dienstes wurde bei der Darstellung der Vorbegriffe festgestellt, dass ein technisches Verständnis des Dienstbegriffs zugrunde zu legen ist, nach welchem der Dienst *die Funktionalität eines Systems* darstellt. Als Funktion steht etwa ein bestimmtes Ergebnis wie die Erzeugung bestimmten Wissens oder das Treffen einer Entscheidung. Daneben erfüllen die *Dienste* (und damit auch die Systeme) wie bereits beschrieben

577 Vgl. *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2, 14 f.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

eine Funktion bei der Erfüllung der Betroffenenrechte; ihre Verfügbarkeit ist etwa von Bedeutung, um Auskunftsrechte zu erfüllen.[578]

Für die Resilienz wurde aus dem Wortlaut zunächst herausgearbeitet, dass sie die *Fähigkeit eines soziotechnischen Systems beschreibt, ungewisse Ereignisse zu erkennen, sich an diese möglichst folgenmindernd anzupassen und sich nach einem solchen unter lernender Verbesserung schnellstmöglich zu erholen.*

Die einzelnen Leistungen der Resilienz können insofern nur durch das System selbst gewährleistet werden, etwa indem hier Maßnahmen zur Erkennung, Anpassung und anschließenden Erholung einschließlich der lernenden Verbesserung implementiert werden. Der Dienst selbst kann zwar in dem Sinne als resilient verstanden werden, als dass das durch ihn erbrachte funktionale Angebot trotz des Vorliegens ungewisser Ereignisse unbeeinträchtigt bleibt.[579] Dies divergiert aber vom inhaltlichen Kern der Resilienz, der gerade die Maßnahmen am System und damit dessen (weitere) Funktionen im Umgang mit Ungewissheit umschreibt, damit der Dienst im Ergebnis resilient ist:

> *Die Resilienz des Dienstes liegt vor, wenn das durch ihn erbrachte funktionale Angebot des Systems angesichts ungewisser Ereignisse unbeeinträchtigt bleibt.*

Im vorliegenden Szenario ist der (resiliente) Dienst die Personalisierung in Form der Erzeugung personalisierten Wissens und den daraus abgeleiteten Entscheidungen. Für die weitere Untersuchung steht gleichwohl die Resilienz des Systems im Vordergrund, die aus den genannten Gründen die entscheidende Rolle einnimmt.

Es sei an dieser Stelle ergänzend darauf hingewiesen, dass teilweise auch zwischen der eigentlichen Funktionalität eines Systems (hier: der Dienst) einerseits und nicht-funktionalen Eigenschaften wie der Gewährleistung der IT- bzw. Datensicherheit und damit auch der Resilienz andererseits, unterschieden wird.[580] In dieser Untersuchung wird der Funktionsbegriff hingegen holistisch für alle Funktionen eines Systems verwendet, d.h. so-

578 Siehe Fn. 545.

579 Vgl. hierzu die Definition von Fehlertoleranz/Resilienz in der Verlässlichkeitsforschung als das Vermeiden von Dienstausfällen: S. 133 ff.

580 Statt vieler: *Balzert*, Lehrbuch der Softwaretechnik, S. 109 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wohl für Sicherheitsfunktionen (einschließlich der Resilienz) als auch für den Dienst als das eigentliche funktionale Leistungsangebot des Systems.[581]

4. Fazit

Für die systematische Auslegung konnten in Gegenüberstellung mit dem Risikoverständnis der DSGVO folgende Ergebnisse gefunden werden:

Hinsichtlich des Risikos wurde herausgearbeitet, dass die Resilienz sich anders als die Risikomethodik mit der Bewältigung von Ungewissheit befasst. Sie hat insoweit eine Komplementärfunktion zur Bewältigung der Ereignisse, die sich nicht als Risiken antizipieren lassen, mithin ungewiss sind. Dabei wurden die Kategorien *bekanntes Nicht-Wissen*, *unbekanntes Wissen* und *unbekanntes Nicht-Wissen* bestimmt, die jeweils unterschiedliche Formen der Ungewissheit beschreiben. Dabei wird bekanntes Nicht-Wissen in der Risikoidentifikation und -analyse sichtbar, so dass hier an der entsprechenden Stelle mit Resilienzmaßnahmen reagiert werden kann. Für die übrigen Kategorien der Ungewissheit kann hingegen nur an den bekanntermaßen besonders kritischen Schutzobjekten (z.B. besonders sensible Daten, zentrale Schnittstellen oder andere wichtige Komponenten) angesetzt werden.

Methodisch ist im Ergebnis weiterhin zwischen der abstrakten Angemessenheit der Resilienzmaßnahmen, welche den Aufwand gegenüber der abstrakten Bedrohung der Schutzgüter durch die (unsichere) Verarbeitung abwägt einerseits und der bisher im Gesetz verankerten risikobezogenen Angemessenheit andererseits zu unterscheiden. Bei letzterer ist der Aufwand der risikospezifischen Maßnahmen gegenüber der damit zu erreichenden Risikoreduktion abzuwägen. Schließlich wurde dargestellt, dass bei dem Risikomanagement im Rahmen der Iteration neues, explizites Wissen über Risiken genutzt werden kann (z.B. eine neu bekannt gewordene Schwachstelle zu schließen). Dagegen bezieht sich das Lernen in der Erholungsphase der Resilienz auf die Nutzung impliziten Wissens, also kein Wissen über neue Einzelrisiken, sondern Wissen über neue Bewältigungsstrategien im Umgang mit Ungewissheit.

581 Ebenfalls kritisch zur Unterscheidung von funktionalen und nicht-funktionalen Eigenschaften: *Glinz*, in: 15th IEEE International Requirements Engineering Conference (RE '07), On Non-Functional Requirements, 21 (22 ff.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Gegenüber den Schutzzielen erweist sich die Resilienz als grundlegend andersartig. Bei den Schutzzielen handelt es sich um Anforderungen an technische Systeme und Dienste (oder in Art. 32 Abs. 2 DSGVO auch Daten) die zur Sicherung der Schutzgüter der DSGVO erfüllt sein müssen.[582] In dieser Funktion lassen sie sich als „Sollzustände" beschreiben: Die Vertraulichkeit eines Systems[583] ist dann gewahrt, wenn kein unbefugter Zugriff auf dieses stattfindet. Die Integrität ist gewahrt, solange das System oder der Dienst unversehrt, d.h. frei von Manipulationen ist. Schließlich ist ein System oder ein Dienst verfügbar, wenn es für den jeweiligen Nutzer jederzeit verwendbar ist.[584] Demgegenüber spezifiziert die Resilienz eine funktionale Anforderung an soziotechnische Systeme, die diese befähigt mit ungewissen Ereignissen, d.h. unmittelbar bevorstehenden oder bereits eingetretenen Sicherheitsvorfällen (mit entsprechenden Schutzzielverletzungen) umzugehen. Diese funktionale Anforderung ist in der Bedrohungssicht anders als die Schutzziele auch kein eigenständiges Angriffsziel.[585]

Aus der Positionierung der Resilienz als einem weiteren Merkmal neben den Schutzzielen folgt weiterhin, dass die Resilienz nur ein Bestandteil zur Gewähr der Sicherheit der Verarbeitung ist. Damit wird die Resilienz hier anders eingeordnet als etwa im CSA, bei dem die Resilienz als weiteres Prinzip neben der Sicherheitsgewähr verstanden wird oder etwa der DORA, bei der alle (Sicherheits-)Maßnahmen per se Resilienzmaßnahmen sind.

Schließlich wurde herausgearbeitet, dass die Resilienz mit Blick auf Systeme und Dienste unterschiedlich zu verstehen ist, wobei der zentrale Anknüpfungspunkt in der Resilienz der soziotechnischen Systeme zu sehen ist und der „resiliente Dienst" vielmehr ein Ergebnis der Resilienz der Systeme ist.

Ergänzend sei an dieser Stelle darauf hingewiesen, dass Art. 32 Abs. 1 lit c) DSGVO explizit die rasche Wiederherstellung der Verfügbarkeit der Daten nach einem Zwischenfall verlangt. Dies ist ebenfalls eine (in sozio-

582 Vgl. *Schmitz/Dall'Armi*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kapitel 1, Rn. 32, welche aber nur auf das „System" abstellen.

583 Für die Vertraulichkeit des Dienstes konnte demgegenüber kein eigenständiger Anwendungsbereich identifiziert werden, siehe oben, S. 195 ff.

584 Genannte Definitionen nach: *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 23 ff.

585 Allenfalls können diese Resilienzmaßnahmen im Falle eines Angriffs umgangen werden und so ggf. ihre vollständige Schutzwirkung nicht ausspielen.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

technischen Systemen zu implementierende) Maßnahme zur Bewältigung eines ungewissen Ereignisses[586] und fällt folglich auch unter die Erholung im Rahmen der Resilienz, wie sie in der Arbeitsdefinition nach der Wortlautauslegung bestimmt wurde. Für die systematische Auslegung ist somit anzunehmen, dass in Art. 32 Abs. 1 lit c) ein Aspekt der Resilienz gesondert hervorgehoben wird.

IV. Historische Auslegung

Im Rahmen der historischen Auslegung gilt es anhand der Entstehungsgeschichte den Willen des Gesetzgebers zu ermitteln; als „Gesetzgeber" sind alle Gesetzgebungsorgane zu zählen, „deren Zustimmung der Rechtsakt im konkreten Fall trägt".[587] Dies ist bei der DSGVO jedenfalls das Europäische Parlament. Die EU-Kommission fällt hingegen nicht unmittelbar darunter, da ihr lediglich ein Initiativrecht zukommt und ihre Gesetzesvorschläge durch das Parlament nach Belieben verändert werden können.[588] Allerdings kann nach der sog. „Paktentheorie" auch schon der Kommissionsvorschlag berücksichtigt werden, soweit das Parlament dessen Inhalte in seinen Willen aufgenommen hat.[589] Die Bedeutung der historischen Auslegung wird im europäischen Recht aber tendenziell eher als gering angesehen.[590]

Normativ können sowohl Vorgängervorschriften als auch vorangegangene Entwürfe eines Gesetzes betrachtet werden.[591] Im Folgenden sollen somit als Vorgängervorschrift[592] des Art. 32 DSGVO der Art. 17 DS-RL sowie die Entwicklung der DSGVO betrachtet werden.

---

586 So bezeichnet *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 65 ff. diese Maßnahme als Teil der Disaster-Recovery nach einem Vorfall. Insofern sei insbesondere auch ein Business-Continuity-Management bzw. ein Notfallmanagement auch unter Einbeziehung des Personals vorzusehen, um die Daten rasch wiederherzustellen zu können.

587 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (303), Rn. 33.

588 Wie zuvor.

589 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285, Rn. 34 m.w.N.

590 *Herdegen*, Europarecht, S. 226, Rn. 92; *Classen/Nettesheim*, Europarecht, § 9, Rn. 174; a.A. *Leisner*, EuR 2007, 689-706 (706).

591 *Pieper*, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, Rn. 48; *GA Mayras,* Schlussanträge EuGH Urt. v. 23.10.1974 – Rs. 32/74, S. 1215.

592 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 4.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

1. Vorgängervorschrift Art. 17 DS-RL

Bisher war die Sicherheit der Verarbeitung in Art. 17 der DS-RL normiert. Diese enthielt weder die Resilienz noch nannte sie die vorangehend skizzierten Schutzziele ausdrücklich. Allerdings wurde bereits der „Schutz [der personenbezogenen Daten] gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang […] und gegen jede andere Form der unrechtmäßigen Verarbeitung." erfasst. Mit diesen Begrifflichkeiten lassen sich wie gezeigt die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit assoziieren.

Vergleicht man nun diese Vorschrift mit Art. 32 Abs. 1 und 2 DSGVO, so ist festzustellen, dass der Gesetzgeber offensichtlich in zweifacher Hinsicht einen Handlungsbedarf identifizierte: Zum einen, dass diese Schutzziele auch explizit auf Systeme und Dienste bezogen und der Schutzumfang somit erweitert werden müssten und zum zweiten, dass die Schutzziele an dieser Stelle aber nicht hinreichend seien, sondern mit der „Resilienz" eine weitere spezifische Anforderung an die Systeme und Dienste gestellt werden müsste.

2. Entwicklung der DSGVO

Im Kommissionsentwurf zur DSGVO vom 25.01.2012 waren die Datensicherheitsvorgaben noch nicht weiter konkretisiert. Vielmehr hieß es in Art. 30 Abs. 1 (später Art. 32 Abs. 1 DSGVO) ähnlich zur finalen Fassung lediglich: „Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist."[593] Der 2. Hs. mit den Listenpunkten a) bis d) war noch nicht vorhanden.

Der europäische Datenschutzbeauftragte forderte in seiner Stellungnahme vom 07.03.2012 zu diesem Entwurf eine Klarstellung der Gesamtverant-

593 EU KOM (2012) 11 endgültig, Art. 30, S. 68.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

wortung des Verantwortlichen für die Datensicherheit und die Ergänzung einer Pflicht zur Durchführung einer Informationssicherheitsstrategie.[594]

Dem scheint das Parlament in seiner Konkretisierung (Beschluss vom 12.03.2014) gefolgt zu sein, die sich heute noch in leicht veränderter Form in S. 2 findet: „Eine solche Sicherheitspolitik umfasst – unter Berücksichtigung des Stands der Technik und der Implementierungskosten – Folgendes: […] b.) die Fähigkeit, die Vertraulichkeit, Vollständigkeit, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen;".[595]

3. Fazit

Insgesamt zeigt sich, dass konkrete Vorgaben zur Datensicherheit erst spät Eingang in das europäische Datenschutzrecht gefunden haben. Weder in der Vorgängervorschrift noch in den ersten Entwürfen wurden die Schutzziele oder die Resilienz (ausdrücklich) genannt und das obwohl die maßgeblich durch die Schutzziele beschriebene Datensicherheit an sich schon eine lange Geschichte aufweist.[596]

Hieraus lässt sich schließen, dass der Gesetzgeber auf erst in jüngster Zukunft vermehrt aufgetretene Phänomene in der Datensicherheit reagiert hat, denen mit dem bisherigen Regelungskonzept (Risiken und Schutzziele) nicht (mehr) beizukommen war. Somit ist auch für die Resilienz im Rahmen der sich anschließenden teleologischen Auslegung nach neuen Sachphänomen zu suchen, auf die das Prinzip der Resilienz eine Antwort geben könnte. Es stellt sich somit pointiert die Frage, warum die Resilienz (erst) jetzt vom Gesetzgeber gesondert normiert wurden.

---

594 EDSB, Zusammenfassung der Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket, S. 4.

595 Siehe hierzu: EU-Parlament, P7_TA(2014)0212 - Legislative Entschließung zum Vorschlag zur allgemeinen Datenschutzverordnung [später DSGVO], 12.03.2014, ABl. 2017 C 378/399 (445 f), Abänderung 124.

596 Exemplarisch im deutschsprachigen Raum als „Datensicherung" bereits: *Weck*, DuD 1989, 386 (386).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

V. Teleologische Auslegung

Für die teleologische Auslegung ist nach dem EuGH auf den „Sinn und Zweck" oder auch den „Geist" der jeweiligen Norm abzustellen.[597] Dabei kann bei der Auslegung des Sekundärrechts wie der DSGVO der dort in den Erwägungsgründen oder der Präambel niedergelegte Zweck herangezogen werden und dieser ggf. mit Blick auf das europäische Primärrecht und damit insbesondere auch die europäische Grundrechtecharta (Art. 6 Abs. 1 EUV) korrigiert werden.[598] Daneben kann jedenfalls nach einer Literaturauffassung auch auf den spezifischen Zweck einzelner Regelungen abgestellt werden.[599]

Der Zweck der DSGVO liegt wie bereits dargestellt insbesondere in der Sicherung der in Art. 1 Abs. 2 DSGVO niederlegten Schutzgüter, namentlich der Rechte und Freiheiten natürlicher Personen, insbesondere des Datenschutzgrundrechts nach Art. 8 Abs. 1 GRC (EG 1 DSGVO). Art. 32 DSGVO regelt mit der Datensicherheit hierfür einen Teilaspekt und die Resilienz stellt wiederrum eine spezifische Datensicherheitsvorgabe dar. In Umkehr dieser Ableitung ist mithin zu fragen, wie die Resilienz der Sicherung des Datenschutzgrundrechts und anderer Rechte und Freiheiten natürlicher Personen dienen kann und somit gegenüber welchen neuen Realweltphänomenen die Resilienz diese Schutzgüter sichern soll.

Systematisch wurde bereits dargelegt, dass Resilienz nicht unmittelbar auf den Umgang mit antizipationsfähigen Risiken, sondern auf den Umgang mit Ungewissheit gerichtet ist. Im Rahmen dessen wurden bereits auch einzelne Fallgruppen von Ungewissheit (*bekanntes Nicht-Wissen, unbekanntes Wissen, unbekanntes Nicht-Wissen)* aufgezeigt. Historisch konnte weiterhin gezeigt werden, dass es sich um eine in der Datensicherheit gänzlich neue Anforderung handelt und diese auch erst spät in das Gesetzgebungsverfahren aufgenommen wurde.

Entsprechend liegt teleologisch die These nahe, dass Resilienz als funktionale Anforderung soziotechnischer Systeme eine Antwort auf zuletzt stark zunehmende Ungewissheitssituationen in der Sicherheitsgewährleis-

597 *Pieper*, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, Rn 33; *EuGH*, Urt. v. 09.12.1965 – 44/65, BeckRS 2004, 71198.

598 *Pieper*, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, B. I. Rechtsquellen, Rn. 44.

599 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (308), Rn. 42; *Wank*, Juristische Methodenlehre, S. 445, Rn. 96 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tung gibt. Solche Ungewissheitssituationen können sich insbesondere aus den nachfolgenden Gründen ergeben, die auch bereits in der systematischen Auslegung bei den Kategorien von Ungewissheit[600] angesprochen wurden.

1. Ungewissheit in komplexen, offenen Systemen

Zunächst haben sich die verwendeten Systeme stark verändert: Ursprünglich bestanden vor allem geschlossene, räumlich abgrenzbare und auf einen bestimmten Kreis von Teilnehmer:innen beschränkte Systeme.[601] Demgegenüber entwickelten sich zunehmend offene Systeme, *die räumlich verteilt und vernetzt sowie offen für die Kommunikation mit möglichst vielen anderen Systemen sind.*[602] Zu offenen Systemen zählen insbesondere jene zur Bereitstellung der hiesigen digitalen Dienste (Online-Marktplätze, Online-Suchmaschinen sowie soziale Netzwerke).[603] Die DSGVO enthält zwar keine expliziten Verweise auf diese neuen Ungewissheiten, verweist in EG 6 aber zumindest auch pauschal auf „rasche technologische Entwicklungen" und eine Datennutzung in „noch nie dagewesenem Umfang".

Solche neuen offenen Systeme weisen starke *Interdependenzen* und eine *hohe Komplexität* mit unüberschaubar zahlreichen und teilweise auch nur subtilen und damit schwer erkennbaren Kommunikationsbeziehungen auf.[604] Wie bereits dargestellt spricht man in diesem Zusammenhang auch von *Emergenz*, wenn sich das Verhalten eines offenen Systems nicht mehr anhand einer Betrachtung seiner Komponenten und seiner einzelnen Kommunikationsbeziehungen erklären lässt.[605] Im Ergebnis ist somit eine vollständige Risikoanalyse nicht möglich und folglich auch nicht mehr hinreichend, um die Datensicherheit zu gewährleisten.

Erschwerend kommt hinzu, dass Normadressaten mitunter auch nur Betreiber kleinerer Gruppen von Komponenten oder sogar nur einzelner

600 S. 170 ff.
601 *Eckert*, IT-Sicherheit, S. 3.
602 *Eckert,* a.a.O.; ähnlich auch *Hiermaier/Scharte/Fischer*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 155 (155), der insoweit von auf zunehmender Vernetzung beruhenden soziotechnischen Systemen spricht.
603 So bereits in der Einleitung, S. 34.
604 *Park et al.*, Risk analysis 2013, 356 (358); *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (8, 12); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12, 32).
605 Siehe oben, S. 174.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Komponenten in solchen komplexen Systemen sind, etwa eines Servers, der von Dritten eingehende Informationen verwaltet, aufbereitet und die Ergebnisse wiederrum Dritten zur Verfügung stellt. Solche Betreiber sehen sich daher sowohl für empfangende Informationen als auch z.T. für die Folgen der Ergebnisse ihrer Informationsverarbeitung einer starken Ungewissheit ausgesetzt.

2. KI als ungewisse Komponente

Eine zusätzliche Ungewissheit kann durch den Einsatz von KI entstehen. Aufgrund des typischen *Blackbox-Charakters* vieler KI-Systeme[606] lassen sich die Lernentwicklung und die damit verbundenen Entscheidungen dieser Systeme nicht sicher vorhersehen. Gleiches gilt für das Verhalten der KI-Systeme im Falle eines Angriffs durch Datenmanipulation (sog. Adversarial Examples, insbesondere Data Poisoning[607]).

Die EU-Kommission schreibt hierzu in ihrem Weißbuch zur Künstlichen Intelligenz, dass entsprechende KI-Systeme technisch solide und präzise sein müssten, um vertrauenswürdig zu sein. Zu treffende Maßnahmen umfassen demnach u.a. die Gewährleistung, dass KI-Systeme sowohl gegen offene Angriffe als auch gegen subtilere Versuche, Daten oder die Algorithmen selbst zu manipulieren, widerstandsfähig [en: resilient] sind und dass in solchen Fällen Abhilfemaßnahmen ergriffen werden.[608] Auch der KI-VO-E sieht in Art. 15 Abs. 4, 5 vor, dass Hochrisiko-KI-Systeme sowohl gegenüber Fehlern, Störungen oder Unstimmigkeiten als auch gegenüber den Versuchen unbefugter Dritter, ihre Verwendung oder Leistung durch

606 *Eigner et al.*, in: Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Towards Resilient Artificial Intelligence: Survey and Research Issues, 536 (536).

607 Adversarial Examples bezeichnet als Oberbegriff jeden Input in ein ML-System, den ein(e) Angreifer:in absichtlich darauf ausgerichtet hat, dass das ML-System Fehler macht. Beim Data Poisoning (oder auch Poisoning Attack) werden Trainingsdaten manipuliert mit dem Ziel, das ML-System „umzutrainieren", so dass es künftig andere Entscheidungen trifft; davon zu unterscheiden sind insbesondere sog. *Evasion Attacks*, die das System nicht umtrainieren, sondern nur täuschen, z.B. schwarze Aufkleber auf einem Stop-Schild, so dass dieses von einem bilderkennenden ML-System nicht mehr richtig erkannt wird; *H. Xu et al.*, IJAC (International Journal of Automation and Computing) 2020, 151 (151 f., 159).

608 EU-Kommission, COM(2020) 65 final, Weißbuch zur Künstlichen Intelligenz, 19.02.2020, S. 24 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ausnutzung von Systemschwachstellen zu verändern, *widerstandsfähig [en: resilient]* sein müssen.

An dieser Stelle ist darauf hinzuweisen, dass in der DSGVO KI-Systeme (wie auch andere automatisierte Entscheidungssysteme) grundsätzlich von Art. 22 DSGVO erfasst werden, ohne jedoch spezifische Vorgaben an die Sicherheit dieser Entscheidungssysteme zu stellen. Jedenfalls in Fällen von o.g. Angriffen wäre hier auch unstreitig Art. 32 DSGVO einschlägig; für sich entwickelnde Fehler insbesondere bei KI-Systemen mit inkrementellem Lernen (Online Lernen) könnte man dies u.U. auch als Anforderung des Art. 22 Abs. 3 DSGVO verstehen. Insoweit erläutert EG 71 zur automatisierten Entscheidungsfindung, der Verantwortliche müsse „technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird". Systematisch dürfte dies aber eher auf Art. 32 DSGVO verweisen, der insofern neben vorsätzlichen Angriffen auch zufällige und fahrlässige Ereignisse erfasst.[609]

3. Ermöglichung von Resilienz durch Komplexität und Autonomie

Auf der Maßnahmenseite spielt die gestiegene Komplexität und Autonomie von IT-Systemen[610] ebenfalls eine tragende Rolle. Nach dem aus der Systemtheorie stammenden *ashby'schen Gesetz* benötigt ein System eine gewisse Eigenkomplexität, um flexibel auf Ereignisse reagieren zu können. Denkbar ist dies v.a. für den Ausfall einzelner und den entsprechenden Ausgleich durch andere Komponenten.[611] Somit ist jedenfalls hinsichtlich der technischen Systeme die Möglichkeit als auch die Notwendigkeit von solchen Resilienzmaßnahmen[612] erst durch die neuere Entwicklung besonders komplexer Systeme entstanden.

609 Siehe S. 98.

610 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 44.

611 *Fathi*, Resilienz im Spannungsfeld zwischen Entwicklung und Nachhaltigkeit, S. 68 mit Verweis auf *Ashby*, An introduction to cybernetics, S. 206 f.

612 Vgl. *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (12).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

4. Fazit

Insgesamt kommt der Resilienz somit nach dem Telos eine Ergänzungsfunktion vor allem für neue Ungewissheitssituationen zu, die im Bereich des *bekannten Nicht-Wissens* zum einen in offenen Systemen und zum anderen durch den vermehrten Einsatz von KI auftreten. Daneben treten bereits bestehende Ungewissheitssituationen, die aber durch Einführung der Resilienz nun spezifisch mitadressiert werden können wie das Übersehen von Fehlern und Schwachstellen (*unbekanntes Wissen).* Auch das Auftreten von sog. Black Swans (*unbekanntes Nicht-Wissen)* insbesondere durch die Ereignisse infolge globaler und sektorübergreifender IT-Sicherheitslücken (z.B. die bereits genannten *HeartBleed* und *Meltdown*)[613] ist zwar an sich kein neues, zunehmendes Phänomen innerhalb der Informationstechnik wie die steigende Komplexität oder der vermehrte Einsatz von KI. Allerdings nimmt die Folgenschwere solcher zentralen Sicherheitslücken durch die immer breitere Verwendung digitaler Technologien, die auf zentralen IT-Strukturen und IT-Produkten beruhen, stark zu.

All diesen neuen bzw. in ihrer Bedeutung zunehmenden Ereignissen kann nicht mit klassischen, risikospezifischen „Resistenzmaßnahmen", sondern nur mit der Ergänzung der Resilienz begegnet werden. Zugleich wird die Einführung der Resilienz insbesondere in Form adaptiver Maßnahmen erst durch die Flexibilität moderner, komplexer Systeme ermöglicht.

VI. Ergebnis

Nachfolgend soll als Ergebnis der Auslegung nach dem Wortlaut, der systematischen Auslegung sowie der historischen und teleologischen Auslegung eine Definition für den Begriff der Resilienz im Kontext des Art. 32 Abs. 1 lit b) DSGVO gebildet werden. Dabei ist zu beachten, dass bei der auslegenden Definition eines Rechtsbegriffs das Augenmerk auf der *Zweckmäßigkeit* liegen muss. Die Bestimmung eines Fach- bzw. Rechtsbegriffs kann nicht nach absoluten Maßstäben richtig oder falsch, sondern nur mehr oder minder zweckmäßig sein, wobei eine hohe Zweckmäßigkeit eine entsprechend hohe Eindeutigkeit bzw. umgekehrt eine geringe Mehrdeutigkeit

613 Siehe hierzu bereits: S. 170 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

voraussetzt.[614] Insbesondere in eine falsche Richtung gehen demnach Begriffsbestimmungen, die bestehende sachliche Zusammenhänge verbergen oder nicht bestehende Zusammenhänge intendieren.[615]

Aus dem *Wortlaut* ergab sich die grundlegende Feststellung, dass Resilienz die Fähigkeit eines soziotechnischen Systems beschreibt, ungewisse Ereignisse zu erkennen, sich an diese zur Minderung der Folgen anzupassen und sich nach einem solchen unter lernender Verbesserung schnellstmöglich zu erholen.

Die *systematische Auslegung* konkretisierte in Gegenüberstellung mit dem Risiko und der Risikomethodik die Erkenntnis, dass Resilienz nicht auf als Risiken antizipierbare Ereignisse, sondern auf ungewisse Ereignisse gerichtet ist.[616] Ihr kommt somit neben der Risikomethodik eine Komplementärfunktion zu.

Die zu adressierende Ungewissheit konnte konkretisierend in die drei Kategorien des bekannten Nicht-Wissens, des unbekannten Wissens und des unbekannten Nicht-Wissens unterteilt werden. Das *bekannte Nicht-Wissen* wird im Rahmen der Risikoidentifikation und -analyse festgestellt (z.B. bei einer vereinfachten Modellierung von Systemen), so dass Resilienzmaßnahmen in dem erkannten Bereich der Ungewissheit ansetzen können. Zum Umgang mit *unbekanntem Wissen* (z.B. Konfigurations- oder Programmierfehler) und *unbekanntem Nicht-Wissen* können hingegen durch die Resilienz nur die bekanntermaßen für die Schutzgüter besonders kritischen Schutzobjekte (besonders sensible Daten oder zentrale IT-Komponenten) betrachtet und diese angesichts der Ungewissheit besonders gesichert werden.

Darüber hinaus wurde festgestellt, dass Resilienzmaßnahmen (nur) *abstrakt angemessen* sein können und müssen, d.h. dass die Angemessenheit sich daran orientiert, welche Schutzgüter betroffen sind und in welcher Höhe hieran Beeinträchtigungen drohen (und nicht etwa wie im Risikomanagement an der zu erreichenden Risikoreduktion, da eine solche bei ungewissen Ereignissen gerade nicht feststellbar ist). Außerdem wurden die Unterschiede zwischen dem Resilienzlernen (neues implizites Wissen über

614 *Bull*, Die Staatsaufgaben nach dem Grundgesetz, S. 43; *Quaritsch*, Staat und Souveränität, S. 21.

615 Wie zuvor.

616 Ähnlich auch auf „insbesondere unvorhergesehene Störungen" abstellend: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39; „nicht vorhergesehene Änderungen": *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 43.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bewältigungsstrategien im Umgang mit Ungewissheit) und der Iteration im Risikomanagement (neues explizites Wissen, z.B. über neu entdeckte Schwachstellen, die nun geschlossen werden können) dargestellt.

Weiterhin konnte in der systematischen Auslegung gezeigt werden, dass sich die Resilienz als funktionale Anforderung insbesondere auch zur Reaktion auf bereits eingetretene Sicherheitsvorfälle wesensmäßig von den Schutzzielen unterscheidet und die Resilienz insofern insbesondere keinen solchen „Sollzustand" beschreibt und kein eigenständiges Angriffsziel darstellt.

Schließlich konnte in der *historischen Auslegung* herausgearbeitet werden, dass der Gesetzgeber mit dieser bislang unbekannten Anforderung auf neue Ungewissheitssituationen reagieren wollte, die dann in der *teleologischen Auslegung* insbesondere auf den vermehrten Auftritt offener, interdependenter Systeme sowie den Einsatz von KI exemplarisch verdichtet werden konnten.

Zusammenfassend ist die Resilienz wie folgt auszulegen:

> *Sie ist die Fähigkeit eines soziotechnischen Systems, unmittelbar bevorstehende oder bereits eingetretene Ereignisse, die aufgrund von Ungewissheit nicht vermeidbar sind, zu erkennen und sich an diese anzupassen sowie sich unter lernender Verbesserung schnellstmöglich davon zu erholen.*

Eingeordnet in Art. 32 Abs. 1 lit b) DSGVO muss der Verantwortliche oder der Auftragsverarbeiter somit die *Fähigkeit* der im Zusammenhang mit der Verarbeitung stehenden *(soziotechnischen) Systeme*[617] *unmittelbar bevorstehende oder bereits eingetretene Ereignisse, die aufgrund von Ungewissheit nicht vermeidbar sind, zu erkennen und sich an diese anzupassen sowie sich unter lernender Verbesserung schnellstmöglich davon zu erholen,* auf Dauer sicherstellen. Die Umsetzung erfolgt wie bei allen Punkten des Katalogs in Art. 32 Abs. 1 DSGVO durch technische und organisatorische Maßnahmen.

Die Resilienz als Fähigkeit eines soziotechnischen Systems zielt neben dem Schutz der personenbezogenen Daten insbesondere darauf ab, dass der diese Daten verarbeitende *Dienst*, der hieraus etwa *Personenwissen* erzeugt, trotz des Eintritts ungewisser Ereignisse unbeeinträchtigt bleibt, mithin „resilient" ist.

617 Der Dienst kann davon abweichend als resilient definiert werden, wenn das durch ihn erbrachte funktionale Angebot des Systems trotz Vorliegen ungewisser Ereignisse unbeeinträchtigt bleibt, siehe hierzu: S. 201 f.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

D. Demonstration anhand personalisierter Dienste

In diesem Abschnitt soll die rechtspraktische Funktion und Umsetzung der Resilienz anhand des gewählten Szenarios mit dem Angriffsvektor der singulären Informationsmanipulation bei personalisierten Diensten demonstriert werden. Durch das hiermit verbundene Einbringen unrichtiger, personenbezogener Daten in das Persönlichkeitsprofil einer Person können die Rechte und Freiheiten derselben (Schutzgüter), allen voran das Datenschutzgrundrecht, beeinträchtigt werden. Darüber hinaus kann aber auch die Informationsfreiheit beeinträchtigt sein, beispielsweise wenn infolge dieser Manipulation des Profils auch unrichtige Empfehlungen auf z.B. in Online-Suchmaschinen oder sozialen Netzwerken erteilt werden und somit der (personalisierte) Informationsraum manipuliert wird.[618]

I. Ungewissheit

Die personalisierten Dienste werden wie bereits zuvor beschrieben von offenen Systemen erbracht, die einen offenen Kreis von Nutzer:innen aufweisen und von deren Systemen (Endgeräte) Daten empfangen, verarbeiten und an diese ausgeben. Der Verantwortliche und Dienstanbieter hat keine Kontrolle über die diese Daten übermittelnden Endgeräte; sie liegen außerhalb seiner Systemgrenzen.[619]

In den Kategorien der Ungewissheit liegt hier ein Fall des *bekannten Nicht-Wissens* vor, da dem Anbieter des personalisierten Dienstes das fehlende Wissen hinsichtlich der Daten aus dem offenen System bereits bekannt ist. Eine entsprechende Risikoidentifikation und -analyse würde ergeben, dass die Möglichkeit einer Daten- und in der Folge einer Informationsmanipulation existiert, die sich dann auch auf die Wissensgenerierung und die Entscheidung auswirken könnte. Aufgrund der offenen Systemarchitektur und der damit verbundenen fehlenden Kontrolle über die Endgeräte kann aber weder die Wahrscheinlichkeit für das Vorhandensein einer Schwachstelle noch die Ausnutzungswahrscheinlichkeit zum Zwecke der Manipulation (auch unter Berücksichtigung der Motivation des Angreifenden) hinreichend sicher bestimmt werden.

618 *Grabenwarter*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 5, Rn. 1028; wohl auch *Schillmöller*, InTer 2020, 150 (152); vgl. außerdem zum Prinzip der Netzneutralität: *Hain*, AfP 2012, 313 (319 f., 325 f.).

619 Siehe S. 34.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Somit besteht auch Ungewissheit über Art, Umfang und das Ziel einer möglichen Manipulation, so dass auch die Auswirkungen auf das Persönlichkeitsprofil und die Entscheidungsfindung ungewiss sind. Anzumerken ist schließlich, dass bei den Empfehlungssystemen der personalisierten Dienste wie beschrieben häufig auch KI-Komponenten eingesetzt werden. Durch die nur *singuläre Datenmanipulation* werden diese aber im vorliegenden Szenario nicht beeinträchtigt.[620]

Ausgehend von einem der skizzierten personalisierten Dienste verlangt die Resilienz als Datensicherheitsanforderung in diesem Szenario nach den folgenden Gegenmaßnahmen:

II. Resilienzmaßnahmen

Auch die Resilienz wird in ihren einzelnen Ausprägungen durch technische und organisatorische Maßnahmen umgesetzt. Diese werden nachfolgend abstrakt beschrieben und durch einige Beispiele dargestellt.

1. Ereigniserkennung

Im Rahmen der Angriffserkennung müssen ungewisse Ereignisse zunächst durch *detektive Maßnahmen*[621] wie der Einführung sog. Angriffserkennungssysteme erkannt werden. Hierzu kann insbesondere auch eine Anomalieerkennung eingesetzt werden.[622] Sofern explizit das Verhalten der Nutzer:innen bzw. deren Endgeräte auf Anomalien überwacht wird, spricht man auch von User and Entitiy Behavior Analysis (UEBA).[623] Weiterhin können Plausibilitätsprüfungen angestellt werden um manipulierte Einga-

620 KI-Systeme lassen sich durch große, „vergiftete" Datenmengen umtrainieren, wie sie bei der *pluralen Informationsmanipulation* vorliegen, siehe zu diesem Szenario S. 318 ff.

621 Der Begriff „detektive Maßnahmen" findet sich ähnlich auch bei *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 16.

622 *Arzt et al.*, MMR 2022, 593 (610); man spricht hier im IT-Sicherheitsrecht (§ 8a Abs. 1a BSIG) auch von Angriffserkennungssystemen, die tradierte sowie KI-gestützte Muster- und Anomalieerkennung als auch heuristische Methoden zur Detektion eines Angriffs (hier Ereignis) einsetzen; *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn 23 f.

623 Vgl. *Shashanka/Shen/Wang*, in: 2016 IEEE International Conference on Big Data (Big Data), User and entity behavior analytics for enterprise security, 1867 (1867 f.).

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ben[624] oder auch unplausible Ergebnisse zu erkennen. Dabei können sehr plötzliche Veränderungen in den Verhaltensmustern oder den Ergebnissen auf eine Manipulation hindeuten.

Im vorliegenden Fall müssen die manipulierten Daten, die von den Endgeräten der Nutzer:innen kommen erkannt werden, so dass insbesondere eine UEBA in Betracht kommt. Nach Erkennung einer Anomalie kann zur Bestätigung derselben als Sicherheitsvorfall ggf. entweder Personal eingesetzt[625] und/oder mit entsprechendem Hinweis auf dieselbe *auch der/die Nutzer:in konsultiert* und zu einem entsprechenden Feedback zu der oder den Anomalie(n) aufgefordert werden, um ggf. schnelle Gewissheit über eine Manipulation der Daten zu erhalten.

2. Anpassungsfähigkeit

Das System muss sich weiterhin an das erkannte Ereignis anpassen, um die Auswirkungen möglichst gering zu halten.[626] Es sind mithin (vorher etablierte) *adaptive Maßnahmen* erforderlich, bei der insbesondere noch unbeeinträchtigte Daten und Komponenten geschützt werden. Dies kann allgemein sowohl technische Maßnahmen (z.B. bei Ausfall von Komponenten die Aktivierung von Redundanzen[627] oder bei Erkennen eines Angriffs das Aktivieren von (halb-)automatisierten Firewall-Regeln, so dass alles bis auf die wichtigsten Prozesse blockiert wird[628]) als auch organisatorische Maßnahmen (z.B. in Form von durch das Personal auszuführenden Notfallplänen[629]) einschließen.

Konkret im vorliegenden Szenario könnte, sofern noch manipulierte Daten eingehen, der Datenzufluss zunächst blockiert werden. Möglich ist dies je nach genauer Angriffskonstellation durch sog. CAPTCHAs, mit denen bei entsprechendem Verdacht geprüft werden kann, ob zumindest tatsäch-

624 Vgl. *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12, 25).
625 Vgl. *Sohr/Kemmerrich*, in: Kipker, Cybersecurity, 49 (102), Rn. 202.
626 Vgl. *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 24.
627 *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (125).
628 *Pohlmann*, in: Lang/Löhr, IT-Sicherheit, 1 (11); ähnlich auch: Datenisolation und Blockierung von Schnittstellen, so dass die Angreifer:innen nicht weiter im System vordringen können: *Arzt et al.*, MMR 2022, 593 (610).
629 Vgl. hierzu auch aus der Praxis den Angriff auf die zum Sparkassenverbund gehörige „Deutsche Leasing": IT Finanzmagazin, Schwerwiegender Cyberangriff auf Deutsche Leasing, 05.06.2023, 05.06.2023.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

lich ein Mensch die den Datenfluss auslösenden Eingaben durchführt.[630] Weiterhin sollten die bereits empfangenen Daten die möglicherweise manipuliert wurden, nicht ohne weiteres in die Personalisierung mit aufgenommen werden, um zu verhindern, dass sie das je nach Erkennungszeitpunkt noch unbeeinträchtigte Personenwissen verändern.

Im Zweifel sollten sie zunächst mit einem „Quarantäne-Status" versehen und deaktiviert werden, um ggf. auch bei einer False-Positive Erkennung noch reagieren zu können.[631] Die Daten können ggf. weiter in den Lernprozess einbezogen werden, die dadurch bedingte Veränderung des Personen- und Lernwissens muss aber jedenfalls reversibel sein, um das manipulationsfreie Profil im Falle des Nachweises eines Angriffs wiederherstellen zu können. Auch hierfür können sowohl technische Maßnahmen vorgesehen werden, also etwa entsprechende automatisierte Vorgänge nach Erkennung des Angriffs als auch organisatorische Maßnahmen wie etwa bei besonders zweifelhaften Fällen die manuelle Untersuchung einzelner Profile durch die Mitarbeitenden.

3. Erholung

Die Erholungsphase dient der Wiederherstellung des ordnungsgemäßen Zustandes (*wiederherstellende Maßnahmen*) der informationstechnischen Systeme, Dienste und Daten. Nach Möglichkeit soll hierbei auch eine lernende Verbesserung der Resilienzmaßnahmen stattfinden. Allgemein müssen in der Erholungsphase insbesondere ggf. gelöschte oder manipulierte Daten nach einem Ereignis aus vorab angelegten Backups wiederhergestellt werden und Systeme sowie Dienste wieder ihre ordnungsgemäße Funktion erbringen.[632] Hierbei können auch Priorisierungen angezeigt sein; etwa um besonders kritische Daten oder Dienste vorrangig wiederherzustellen.[633]

Vorliegend ist nach dem Ergebnis während der Anpassungsphase zu differenzieren: In jedem Fall sollte der personalisierte Dienst schnellstmöglich in den Normalzustand zurückkehren, d.h. entweder die verwendeten

630 *G. Yang/Gong/Cai*, in: Proceedings 2017 Network and Distributed System Security Symposium, Fake Co-visitation Injection Attacks to Recommender Systems, S. 13, der gleichzeitig aber auch auf die Umgehungsmöglichkeit hinweist. Man könnte diese Maßnahme auch als weitere detektive Maßnahme verstehen, sie weist insofern einen Doppelcharakter auf.

631 Vgl. *Arzt et al.*, MMR 2022, 593 (610).

632 Vgl. *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 17.

633 Vgl. *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 24.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Quarantäne-Daten dauerhaft von der Verarbeitung ausschließen oder die zu Unrecht nicht verwendeten Daten in die weitere Verarbeitung aufnehmen. Etwaige manipulative Veränderungen am Profil müssen umgehend revidiert werden.

Um künftigen Ereignissen besser begegnen zu können, sollte das aus den detektierten Angriffen zu erzielende Wissen genutzt werden (*Lernen*), um insbesondere die Anomalieerkennung sowie ggf. auch die Anpassungsfähigkeiten zu optimieren.

III. Abstrakte Angemessenheit

Für die Frage der abstrakten Angemessenheit und damit den Umfang der zu treffenden Resilienzmaßnahmen ist auf die Modalitäten der Verarbeitung abzustellen, um zu bestimmen welche Schutzgüter betroffen sind und wie stark diese infolge von zumindest teilweise ungewissen Sicherheitsverletzungen beeinträchtigt sein können.

Bei den für die Datensicherheit typischen Vertraulichkeitsfällen wird man insbesondere betrachten müssen, ob und inwieweit besonders sensible Daten (Art. 9 Abs. 1 DSGVO) verarbeitet werden, die ggf. auch ein lohnenswertes Ziel für Angreifer:innen (z.B. für Erpressung) darstellen und welche Schutzgüter bei einer Offenlegung betroffen werden (z.B. neben dem Datenschutzgrundrecht auch das Diskriminierungsverbot).[634]

Bei personalisierten Diensten können infolge der ungewissen Manipulationen der Daten und der insofern manipulierten Informationsinterpretation und Wissenserzeugung *(Personenwissen)* falsche Persönlichkeitsbilder entstehen. Auch die daraus folgenden falschen Dienstentscheidungen können gravierende Folgen haben: Bei sozialen Netzwerken und Online-Suchmaschinen kann dies die individuelle Persönlichkeitsentfaltung stark beeinträchtigen sowie insbesondere auch zu einer politischen Beeinflussung führen. Dies gilt in besonderem Maße soweit durch Manipulationen die ohnehin tendenziell bestehenden Filterblasen (Filter Bubbles)[635] verstärkt

634 Zur Veranschaulichung sei hier exemplarisch auf einen Sicherheitsvorfall verwiesen, bei dem Hacker in Finnland vertrauliche Gesprächsinformationen aus Psychotherapiesitzungen erlangten und die Patient:innen anschließend unter Androhung der Veröffentlichung erpressten: *Muth*, Cyber-Erpresser in Finnland, Süddeutsche Zeitung vom 29.10.2020.

635 *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 98 (110); *Pariser*, Filter Bubble, S. 17 ff., 24, 169 ff; welcher die durch ubi-

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

werden. Aus Sicht der Angreifenden dürften außerdem Journalist:innen[636] und Politiker:innen aufgrund ihres Einflusses auf politische Entscheidungen sowie die öffentliche Meinungsbildung[637] besonders attraktive Ziele darstellen, so dass diese möglicherweise auch individuell besonders gefährdet sind. Im Ergebnis dürfte die abstrakte Angemessenheit somit bei den genannten Diensten Resilienzmaßnahmen in großem Umfang rechtfertigen können.

IV. Fazit

Insgesamt zeigte die Demonstration anhand des konkreten Anwendungsbeispiels der personalisierten Dienste welche Ungewissheit konkret bestehen kann und wie dieser mit der Resilienz begegnet werden kann. Dabei wurde auch gezeigt, wie die einzelnen Elemente der Resilienz durch technische und organisatorische Maßnahmen umgesetzt werden können. Zuletzt wurde konkretisiert, wie der Umfang der angemessenen Resilienzmaßnahmen mit Blick auf die abstrakt drohenden Schutzgutverletzungen durch die Manipulation der personalisierten Dienste bestimmt werden kann.

quitäre Personalisierung geschaffene Filter Bubble als einen individuellen, fremdbestimmten und für den Nutzer nicht direkt wahrnehmbaren beschränkten Informationsraum im Internet beschreibt und auf dessen mögliche negative Folgen wie eine (unbemerkte) schwindende Selbstbestimmtheit und eine Beeinträchtigung des demokratischen Austauschs hinweist; Zur Filter Bubble in der Online-Suchmaschine auch: *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 75 (91).

636 Zum generellen Einfluss von sozialen Netzwerken, in diesem Fall X (vormals Twitter), auf die Tätigkeit von Journalist:innen: *McGregor/Molyneux*, Journalism 2020, 597 (597 ff., 607).

637 Hierzu später noch ausführlich: S. 259 ff.

https://doi.org/10.5771/9783748947523-81 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY