Susan Gonscherowski, Marit Hansen, Martin Rost

Resilienz – eine neue Anforderung aus der Datenschutz-Grundverordnung

Nach den drei klassischen Schutzzielen der Informationssicherheit führt Art. 32 DSGVO „Belastbarkeit" (engl. „Resilience") auf. Der deutsche Begriff wird dem umfassenden Konzept der Resilienz nicht gerecht. Dieser Artikel verdeutlicht, dass „Belastbarkeit" (besser: Resilienz) als eine Strategie bei der Umsetzung von Schutzmaßnahmen, nicht aber als ein weiteres, eigenständiges Schutzziel auf der Ebene Vertraulichkeit, Integrität und Verfügbarkeit aufzufassen ist.

1 Einleitung

Art. 32 Datenschutz-Grundverordnung (DSGVO) betrifft die Sicherheit der Verarbeitung und stellt eine Reihe von Anforderungen auf, die Verantwortliche und Auftragsverarbeiter durch das Treffen geeigneter technischer und organisatorischer Maßnahmen umsetzen müssen. Wer sich bisher mit den klassischen Schutzzielen der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – beschäftigt hat, mag von Art. 32 Abs. 1 lit. b DSGVO überrascht sein, in dem der Begriff „Belastbarkeit" in die Aufreihung dieser klassischen Schutzziele aufgenommen wird: „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen". Dies legt den Gedanken nahe, Resilienz[1] nicht nur als einen normativen Anker für Schutzmaßnahmen, sondern mehr noch als ein weiteres eigenständiges Schutzziel der Informationssicherheit bzw. des Datenschutzes aufzufassen. Auf jeden Fall handelt es sich um eine normative Anforderung, die operativ umzusetzen ist.

Mit Bezug zum Datenschutz ist die Anforderung „Resilienz" auf personenbezogene Verarbeitungstätigkeiten von Organisationen – also auf eine Einheit von Daten, IT-Systemen und Prozessen – zu fokussieren. Resilienz einer Verarbeitung personenbezogener Daten zielt darauf ab, dass diese Verarbeitung dauerhaft beherrscht wird und dass damit die Risiken für die Rechte und Freiheiten natürlicher Personen sowie für die Informationssicherheit eingedämmt werden.

Neben „Belastbarkeit" bieten sich weitere Begriffe zur Übersetzung von „Resilienz" an, die jeweils wichtige Aspekte der Resilienz betonen, nämlich Widerstandsfähigkeit, Robustheit, Elastizität oder Anpassungsfähigkeit. Der Resilienz-Begriff in der Informatik geht davon aus, dass Sicherheit nicht vollständig garantiert werden kann, selbst wenn man versucht, alle etwaigen Situationen vorab zu berücksichtigen (vgl. Bishop et al. 2011: 95, 100ff). Ziel der Resilienz ist es, auch in solchen Fällen weiterhin eine – im Sinne der DSGVO rechtskonforme – Verarbeitung zu gewährleisten.

Der Begriff Resilienz leitet sich ab von dem lateinischen Wort resilire mit der Bedeutung „zurückspringen". Im Technikkontext wurde der Begriff erstmals in den Materialwissenschaften

Susan Gonscherowski

wiss. Mitarbeiterin im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

E-Mail: sgonscherowski@datenschutzzentrum.de

Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

E-Mail: marit.hansen@datenschutzzentrum.de

Martin Rost

Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

E-Mail: martin.rost@datenschutzzentrum.de

1 Wir werden nachfolgend bevorzugt von „Resilienz" sprechen, weil wir die deutsche Übersetzung von „Resilience" als „Belastbarkeit" für unzureichend halten, da sie die vielfältigen Facetten des Begriffs nicht abbildet.

verwendet, um die Fähigkeit eines Materials zu beschreiben, das nach einer Verformung in den Ausgangszustand zurückkehrt. In der Informationssicherheit muss Resilienz jedoch nicht bedeuten, dass nach einer Störung oder Schädigung ein Zurückspringen in den ursprünglichen Zustand geschieht; zumindest aber soll die Funktionalität mit ihren definierten Eigenschaften möglichst weitgehend aufrechterhalten bleiben (vgl. Madni/Jackson 2009: 181). Resilienz bezeichnet aber nicht nur einen Aspekt von Widerstandsfähigkeit im Sinne eines Tolerierens von Umweltstörungen. Vielmehr umfasst sie sowohl die strukturelle, proaktive Systemeigenschaft von „Robustheit" als auch eine zeitliche, nämlich reaktive Eigenschaft der „Agilität" (zur Unterscheidung proaktiv/agil vgl. Wielang/Wallenburg 2013). Dass dabei weniger Technik an sich, sondern eine geeignete Organisation eine wichtige Rolle spielt, beschreibt die acatech-Studie „Resilienz by Design", die mit folgender Definition aufwartet: „*Resilienz ist die Fähigkeit, tatsächliche oder potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen. Widrige Ereignisse sind menschlich, technisch sowie natürlich verursachte Katastrophen oder Veränderungsprozesse, die katastrophale Folgen haben.*" (Thoma 2014: 17)

Resilienz ist besonders wichtig bei autonomen Systemen, z. B. Connected Cars oder anderen Verkehrsmitteln mit automatisierter Steuerung, Robotern, sich spontan vernetzenden Geräten des Internet of Things oder Cyber-Physical Systems. In diesen Fällen treten typischerweise nicht vollständig vorhersehbare Situationen auf, die bei der Verarbeitung in geeigneter Weise zu berücksichtigen sind.

2 Weitere Annäherungen aus Sicht des Datenschutzes

In der juristischen Kommentarliteratur zu Art. 32 DSGVO wird die zu kurz greifende Übersetzung von Resilience als „Belastbarkeit" offenbar weitgehend akzeptiert.[2] Belastbarkeit wird teilweise als eigenständiges Ziel benannt, in der eigentlichen Auslegung dann jedoch durchgängig als ein Aspekt der Verfügbarkeit interpretiert. Hjadik subsumiert sowohl Belastbarkeit als auch Verfügbarkeit wiederum unter dem von ihm neu eingeführten Ziel der Nachhaltigkeit (vgl. Hjadik 2017: Art. 32 Rn. 8).

Jergl beschreibt Belastbarkeit als ein bestimmtes Verhältnis der Informationsverarbeitung je Zeiteinheit, das ein System garantieren soll, um Verfügbarkeit zu gewährleisten (vgl. Jergl 2018: Art. 32 Rn. 32-33). Jandt sieht in Belastbarkeit die Fähigkeit eines Systems oder Dienstes, Aufgaben innerhalb eines bestimmten Zeitrahmens zu erfüllen, und betont ausdrücklich, dass es sich dabei nicht um ein eigenständiges Schutzziel handelt (vgl. Jandt 2018: Art. 32 Rn. 26). In beiden Fällen werden Maßnahmen genannt, die im Zusammenspiel die Verfügbarkeit der Datenverarbeitung sicherstellen. Folglich ist Belastbarkeit eine Anforderung an die Performance der Datenverarbeitungssysteme unter bestimmten Bedingungen, etwa zu einem bestimmten Verarbeitungszeitpunkt wie beispielsweise bei Auslastungsspitzen. Ähnlich buchstabengetreu – ohne Rückgriff auf die englische Sprachfassung – interpretiert Martini (Martini 2018: Art. 32 Rn. 39) Belastbarkeit als Funktionsfähigkeit der Verarbeitungssysteme bei starkem Zugriff oder sonstiger starker Auslastung. Als Beispiel nennt er den Schutz gegen (D)DoS-Angriffe, die sich durch einen gezielte Überlastung der Systeme auszeichnen. Piltz knüpft die Fähigkeit zur Belastbarkeit nicht an einen Zeitparameter, sondern an die ordnungsmäßige Funktionsfähigkeit eines Systems bzw. Dienstes bei starker Belastung (vgl. Piltz 2018: Art. 32 Rn. 30). Im Unterschied zu den zuvor genannten Auslegungen sollen die an das System gestellten Aufgaben jedoch nicht nur „irgendwie" abgearbeitet, sondern den Vorgaben des Normalbetriebs entsprechend erfüllt werden. Die Gewährleistung einer ordnungsmäßigen Datenverarbeitung zielt hier nicht mehr primär auf die Verfügbarkeit, sondern zumindest ebenso auf die Integrität eines Systems ab.

Weitere Überlegungen zur Rekonstruktion von „Belastbarkeit" finden sich im Kontext der Diskussionen zu Gewährleistungszielen des SDM. So schlug Rost vor, „das etwas überraschend geforderte Schutzziel ‚Belastbarkeit' mit den Bordmitteln der vorhandenen Schutzziele als *integritätsgesicherte Verfügbarkeit* mit den entsprechend zu wählenden Schutzmaßnahmen zu konzipieren" (vgl. Rost 2018: 16). Aber was hieße „integritätsgesichert" mit Blick auf die bspw. im SDM zugeordneten Schutzmaßnahmen genau? Wenn ein Verfahren eben nicht „irgendwie" oder „nur zu einem Teil" auf unvorhergesehene interne oder externe Störungen reagieren, sondern weiterhin erwartungsgemäß zumindest eine Zeit lang im Normalbetrieb funktionieren soll, dann ist damit wesentlich die Integrität eines Verfahrens angesprochen.

Ein ENISA-Report zum Begriff der Resilience betont deren umfassendes Konzept und benennt sechs Resilience-Metriken: „Availability, Reliability, Safety, Confidentiality, Integrity and Maintainability" (ENISA 2011: 18).

Hansen legt Wert darauf, dass Resilienz nicht reduziert werden darf auf Informationssicherheit, sondern der Blick – wie stets in der DSGVO – zu weiten ist auf die vielfältigen Aspekte aller Datenschutz-Grundsätze des Art. 5 DSGVO (vgl. Hansen 2018: Art. 32 Rn. 42-45). Resilienz umfasst als Eigenschaften insofern sowohl strukturelle Robustheit als auch zeitliche Agilität in Bezug auf die Datenschutz-Grundsätze, die trotz etwaiger „Störungen" umgesetzt werden müssen. Daraus folgt: Die Anforderung „Belastbarkeit" bzw. „Resilienz" erfordert keine Umsetzung durch eine spezielle Resilienz-Maßnahme, sondern zum einen müssen die Maßnahmen zur Umsetzung von Datenschutzanforderungen in ihrer Gesamtheit bereits ausreichend resilient ausgelegt sein (siehe Abschnitt 3), zum anderen dürfen Resilienz-Maßnahmen nicht gegen die Datenschutz-Grundsätze verstoßen (siehe Abschnitt 4). Dies führen wir im Folgenden aus.

3 Maßnahmen zur Umsetzung von Resilienz

Die Umsetzung von Resilienz wie auch anderer Sicherheitseigenschaften leidet am mangelhaften Status Quo der heutigen Informations- und Kommunikationstechnik bezüglich eingebauter Informationssicherheits- und Datenschutzanforderungen. So wäre es hilfreich, wenn alle verwendeten Komponenten von möglichst geringer Komplexität mit dokumentierten oder gar bewiesenen Sicherheits- und Datenschutz-Eigenschaften wären. Allerdings – und auch dies passt zur Resilienz – ist es für ein sicheres Gesamtsystem nicht erforderlich, dass alle Komponenten sicher ausgelegt sind (Dobson/Randell 1986: 192; Shamir 1979: 612f).

2 Anders der umfassende Ansatz der Resilienz von Hansen: Art. 32 Rn. 42-45.

Um Resilienz für ein Verfahren zu erreichen, sollten für jedes der sechs Schutzziele im Datenschutz resiliente Maßnahmen implementiert werden, deren Schutzwirkung sich agil entfaltet. Um dies zu erreichen, lassen sich zwei Strategien nutzen. Eine Strategie besteht darin, den Betrieb einer Maßnahme für ein Schutzziel als eine Verarbeitungstätigkeit zu implementieren, auf die ihrerseits die Maßnahmen der anderen Schutzziele anzuwenden sind (siehe Abschnitt 3.1). Die zweite Strategie setzt auf die Diversifikation bei der Wahl der Maßnahmen: Es wird eine Datenverarbeitung aufrechterhalten mit Rückgriff auf unterschiedliche Daten, Systeme und Prozesse (siehe Abschnitt 3.2).

3.1 Resilienz durch resiliente Schutzmaßnahmen

Diese Strategie entspricht im Wesentlichen dem Vorgehen beim Standard-Datenschutzmodell, um Schutzmaßnahmen für „hohen Schutzbedarf" zu bestimmen. In der Regel kommen bei Verarbeitungen mit hohem Schutzbedarf keine völlig neuen Schutzmaßnahmen gegenüber normalem Schutzbedarf hinzu. Der Unterschied des Betriebs von Schutzmaßnahmen für normalen und für hohen Schutzbedarf besteht vielmehr ganz überwiegend darin, dass die gleichen Maßnahmen bei hohem Schutzbedarf mit einer erhöhten Wirksamkeit ausgestattet sind (vgl. Rost 2018: 15f). Dies führt in der Gesamtheit in der Regel auch zu einer höheren Resilienz der Verarbeitung.

Als Beispiel: Bei einem Grundrechtseingriff geringer Intensität bzw. bei normalem Schutzbedarf eines Verfahrens müssen zur Umsetzung des Schutzziels „Transparenz" Prozesse und Systeme protokolliert werden. Die Frage ist nun: Wie revisionsfest ist diese Protokollierung? Kann sich eine Organisation darauf verlassen, dass die Protokollierung Einträge relevanter Ereignisse enthält, an deren Bezeichnung und Zeitpunkten kein Zweifel besteht? Bei hohem Schutzbedarf müssen die Daten der Prozesse und Systeme qualitativ verbessert protokolliert werden, bspw. dadurch, dass die Protokolldaten durch Backups gesichert verfügbar, integritätsgesichert signiert und vertraulichkeitsgesichert verschlüsselt werden. Außerdem muss ein Rollen- und Berechtigungskonzept für den Zugriff auf die Protokolldaten vorliegen, um anhand dieser Daten gezielte Verhaltenskontrollen zu ermöglichen, aber Leistungskontrollen auszuschließen. Auch für das Ändern oder Löschen von Protokolldaten sind Spezifikationen notwendig, wie die Prozesse zu gestalten sind, damit bei sich aus den Protokolldaten ergebenen Erkenntnissen die vorgesehenen Schritte, z. B. Klärungs- oder Heilungsprozesse, vorgenommen werden. Zudem muss transparent sein, welche Ereignisse zu welchem Zweck protokolliert werden. So kann eine Maßgabe sein, dass IT-Funktionen nicht ausgeführt werden, wenn die Protokollierung der Funktionen nicht gesichert ist. Ohne Protokollierung ist es nicht möglich, die Quellen für kleinere Störungen, die sich zu Problemen auftürmen, zu erkennen.

Generell muss auch eine Protokollierung allen Anforderungen von Art. 5 DSGVO genügen. Protokollierung als organisationsweites Verfahren ist geeignet, um Störungen, die erstmals in einem Verfahren auftreten, daraufhin zu prüfen, ob sie organisationsweit riskante Auswirkungen haben können.

Zwischenfazit: Die Resilienz einer Verarbeitungstätigkeit lässt sich im Allgemeinen verbessern, wenn (einzelne) Maßnahmen betrieben werden, die für einen erhöhten Schutzbedarf vorgesehen sind.

3.2 Resilienz durch Verschiedenartigkeit der Maßnahmen

Diese Strategie basiert wesentlich darauf, Resilienz durch Verschiedenartigkeit der Mittel und Maßnahmen bei der Umsetzung der gleichen Verfahrenstätigkeit zu erreichen.

In Bezug auf die resiliente Sicherung der *Verfügbarkeit* einer personenbezogenen Datenverarbeitung durch Redundanz kommen eine unterbrechungsfreie Stromversorgung, eine verteilte Speicherung von Daten, Ersatzhardware, ein Mechanismus zum Neuaufsetzen von Systemen mit Betriebssystem und Software oder eine Datensicherung infrage. Die Resilienz ließe sich jedoch dadurch steigern, wenn ein zweites IT-System, eine zweite Backup-Technik oder ein Neben-Prozess mit anderen Mitteln umgesetzt würde. Bei einem redundant betriebenen zweiten IT-System wäre darauf zu achten, dass es von einem anderen Hersteller wenn möglich mit anderen elektrischen Komponenten, einem anderen BIOS, einem anderen Betriebssystem und einer anderen Anwendungssoftware als das erste Produktivsystem läuft. So erhöht sich die Wahrscheinlichkeit, dass ein spezifisches, aber bislang unerkanntes Problem, das auf dem Hauptsystem festgestellt wird, nicht auch auf dem Zweitsystem entsteht. Lösungen mit mehrfach redundanter Auslegung aller Komponenten führen zu erhöhten Kosten.

In Bezug auf die resiliente Sicherung der *Vertraulichkeit* funktionieren die Ansätze für Verfügbarkeit allenfalls eingeschränkt. Dies zeigen Arbeiten zur Backdoor-Toleranz, d. h. zu einem Systementwurf, der Vertraulichkeit und Integrität trotz möglicherweise vorhandener Software- oder Hardware-Hintertüren zu garantieren sucht (für Hardware-Komponenten: Mavroudis et al. 2017: 1595): Naive Redundanz hilft nicht gegen Hintertüren, wenn private Schlüssel in mehreren parallelen Verarbeitungen verwendet werden und damit vervielfacht angreifbar werden.

Ein generelles Problem besteht dann, wenn eine Abhängigkeit von zentralen Komponenten besteht. Dies kann bspw. der verwendete Verschlüsselungsmechanismus sein, der ab einem gewissen Zeitpunkt als nicht mehr ausreichend sicher einzustufen ist und daher ausgetauscht werden muss. Solche Effekte müssen vorab bedacht werden, um geeignete Prozesse vorzusehen, damit entsprechende Komponenten ersetzt werden können. Inwieweit ein temporärer Parallelbetrieb mit den Sicherheits- und Datenschutzanforderungen vereinbar ist, muss im Einzelfall geprüft werden. Zudem ließen sich Daten einer Verarbeitung bspw. nacheinander mehrfach verschlüsseln. Sicherzustellen ist dabei, dass die zweite Verschlüsselung sich in Verfahren, Algorithmus und Implementierung von der ersten Verschlüsselung unterscheidet, so dass entstehende Probleme nicht beide Verschlüsselungen negativ beeinflussen. Die Idee der „multiple Lines-of-Defense" ist alt, aber nach wie vor wirksam: Ist der erste Schutzwall gebrochen, hält vielleicht der zweite (vgl. Three-Lines-of-Defense-Modell für Risiko-Management, IIA 2013: 7).

In Bezug auf eine resiliente Sicherung der *Nichtverkettbarkeit* würde man auf ein hohes Maß an Trennungen zwischen Verfahrenskomponenten achten. Die Maßgabe ist, dass Störungen, die in einem Teil einer Datenverarbeitung auftreten, sich nicht auf das ganze System ausbreiten können. Dies entspricht den Schotten bei einem Schiff, damit ein Schiff trotz eines an sich gefährlichen Lecks weiterhin schwimmt, oder den Brandmauern bei großen Häusern, damit ein Haus trotz eines Brandes nicht als Ganzes in Gefahr gerät und zumindest noch für die Zeit von Ret-

tungsmaßnahmen nicht einstürzt. Auch hier zeigt sich wieder, dass Abhängigkeiten von Komponenten oder von Dienstleistern zu vermeiden sind.

In Bezug auf eine resiliente Sicherung der *Intervenierbarkeit* würde man auf den Einbau eines hohen Maßes an Aktoren in eine Verarbeitung achten, um möglichst gut kontrollierbar gesichert jederzeit und ohne Verzug Änderungen auslösen zu können. Als Gestaltungsoption kommt ein definierter Fail-Safe-Mode infrage: Bei einem Vorfall wechselt die Verarbeitung in diesen Modus, der bestimmte Sicherheitsgarantien aufweist oder für den der mögliche Schaden begrenzt ist. Eine solche Maßnahme greift den Aspekt der Agilität auf, so dass zwischen dem Erkennen, der Analyse bzw. Bearbeitung und der Reaktion auf eine Störung möglichst wenig Zeit verloren geht.

In Bezug auf eine resiliente Sicherung der *Transparenz* ließe sich an eine Protokollierung denken, die im Zuge einer zumindest teilautomatisierten Auswertung zunehmend zu einem Monitoring wird: Welches Ereignis ist von welchem Sensor genau zu diesem Zeitpunkt registriert worden? Eine auf Resilienz achtende Transparenz würde insofern zum Einsatz vieler Sensoren (oder gar Prüfagenten, die nicht nur einen Ist-Zustand messen und melden, sondern Soll-Ist-Differenzen ermitteln und ggfs. bereits warnwürdige Zustände melden) in den Komponenten einer Verarbeitung führen. Im Zusammenspiel mit zahlreichen Aktoren in vielen relativ kleinteilig eingerichteten Komponenten lassen sich so Störungen frühzeitig erkennen und bearbeiten. Resilienzfördernd können sowohl technische als auch organisatorische und menschliche Mechanismen sein, um auf etwaige Probleme aufmerksam zu werden und damit umgehen, z. B. ein Intrusion-Detection-System oder aufmerksame und geschulte Beschäftigte.

Dieser zuletzt genannte Aspekt verweist darauf, dass die resiliente Sicherung der *Integrität* einer Verarbeitung im Sinne einer Beherrschbarkeit auf die Möglichkeiten zur Steuerung einer Verarbeitung bestehen muss. Es bedarf des Einsatzes von Überwachungsmaßnahmen, von denen ihrerseits wieder zu fordern ist, dass auch diese allen Datenschutz-Grundsätzen (z. B. ausgedrückt über die von den Schutzzielen formulierten Anforderungen) genügen. Auch das in Art. 32 Abs. 1 lit. d geforderte Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung bedingt ein Testen der Gesamtheit der technischen und organisatorischen Maßnahmen auf ihre Wirksamkeit. Dies alles wäre im Rahmen eines Datenschutz-Managementsystems umzusetzen.

Eine integre Steuerung aufgrund von derartigen Prüfungen muss so konzipiert sein, dass sie festgestellte „Störungen" weder ignoriert noch zu sensibel darauf reagiert, nur weil die Qualität einer Störung zunächst ungeklärt ist. Deshalb darf man vermuten, dass bei der zunehmenden Automatisierung der wesentliche Aspekt der Resilienz, nämlich möglichst intelligent auf Störungen zu reagieren, am Ende von der besonders leistungsfähigen menschlichen Intelligenz zu erbringen ist. Selbstlernende Systeme spielen sicher eine wichtige Rolle; hierbei müssen aber Interventions- und Überprüfungsmöglichkeiten vorgesehen sein, um die Beherrschbarkeit und Nachvollziehbarkeit zu wahren.

4 Gegenläufige Resilienz-Maßnahmen

Die DSGVO wird mit ihren Anforderungen dazu führen, dass sich der Markt verändert. So ist davon auszugehen, dass künftig die Resilienz-Eigenschaften von Systemen besonders herausgestellt werden. Allerdings genügt nicht jeder Resilienz-Mechanismus den Datenschutz-Grundsätzen nach Art. 5 DSGVO; zumindest wären bei der Gestaltung der Systeme möglicherweise antagonistisch wirkende Maßnahmen – wie stets im SDM – angemessen im Auswahl- und Umsetzungsprozess zu berücksichtigen.

Beispielsweise erfordert ein erhöhter Grad an Autonomie der Verarbeitung die Erfassung von Daten, um auf dieser Basis Störungen erkennen und behandeln zu können. In vielen Fällen wird nicht ausgeschlossen sein, dass auch personenbezogene Daten – beispielsweise beim selbstfahrenden Auto Informationen über die Menschen in der Umgebung – erfasst und analysiert werden. Hier wäre zu prüfen, inwieweit diese Verarbeitung überhaupt rechtmäßig ist und inwieweit die Datenschutz-Grundsätze insbesondere der Transparenz, der Datenminimierung und der Speicherbegrenzung erfüllt sind. Hinzu kommt, dass selbstlernende Systeme sich ständig verändern, so dass die Herausforderung besteht, jederzeit Transparenz über die Funktionsweise zu gewährleisten. Andernfalls wären jedoch Überprüfbarkeit und Beherrschbarkeit der Verarbeitung infrage gestellt. Auch ist es notwendig, etwaigen Einschränkungen der Intervenierbarkeit entgegenzuwirken: Sonst könnte es dazu kommen, dass eine menschliche, notwendige Intervention für ein autonom arbeitendes Verarbeitungssystem nicht unterscheidbar ist von einer Störung oder einen Angriff und abgewehrt würde. Hier erlangen die drei Robotergesetze von Asimov[3] neue Relevanz, deren Reihenfolge deutlich macht, dass Resilienz zwar wichtig ist, aber nicht in Konflikt geraten darf mit höherrangigen Regeln, die dem Schutz der Menschen dienen (in Übertragung auf beliebige informationstechnische Systeme vgl. Clarke 1993/1994: 57ff).

5 Resilienz – (k)ein elementares Schutzziel?

Es spricht aus unserer Sicht vieles dafür, dass mit den sechs bereits ausgewiesenen „elementaren Schutzzielen" des Datenschutzes eine theoretisch kontrollierbare, „historisch relative" Vollständigkeit erreicht ist, die nicht durch leichtfertiges Hinzufügen beliebig weiterer „Ziele" aufgegeben werden sollte (vgl. Rost 2018: 13).[4] Schutzziele sind Bestandteile von Modellierungen – bspw. auch der Informationssicherheit –, deren Funktion darin besteht, „normative Optimierungsgebote" (vgl. Bock/Robrahn 2018: 9f), die aus ganz unterschiedlichen Quellen stammen und mit ganz unterschiedlichen Legitimationsgraden ausgestattet sein können, mit technischen und organisatorischen Konstruktionsanweisungen zu verbinden (vgl. Rost/Storf 2013). Bislang ist es noch immer zufriedenstellend gelungen, weitere Schutzzielkandidaten als Unterfall in einen generativen Bezug zu den sechs elementaren Schutzzielen zu setzen (vgl. Rost/Bock 2011: 32). Resilienz ist zunächst als eine normative Anforderung zu verstehen, deren Modellierung – ob als Schutzziel, als Kombination aus

3 1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.

2. A robot must obey the orders given [to] it by human beings except where such orders would conflict with the First Law.

3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws. (Asimov 1942)

4 Dies gilt in vergleichbarem Maße auch für die normative Anforderungen „Datenminimierung", die im Kontext des SDM bislang als eigenes Datenschutzziel ausgewiesen ist. Datenminimierung ist normativ abhängig von der Erforderlichkeit und damit eine Untermenge der Nichtverkettung.

Schutzzielen oder als Eigenschaft oder Maßnahme – noch ausgiebig zu diskutieren ist. Dieser Artikel hat Argumente dafür stark gemacht, Resilienz nicht als eigenständiges Schutzziel, sondern als eine Eigenschaft auf der Ebene der bereits bekannten Datenschutz-Maßnahmen anzusiedeln.

6 Fazit

Resilienz ist nicht als ein eigenständiges Schutzziel aufzufassen, das für einen ganz eigenen Typ von Schutzmaßnahmen stünde. Resilienz ist aber auch keine Eigenschaft, die vornehmlich der Sicherstellung der Verfügbarkeit personenbezogener Verarbeitungstätigkeiten dient. Resilienz stellt stattdessen stärker noch auf die Integrität einer Datenverarbeitung, also auf die Aufrechterhaltung einer Funktionalität mit bestimmten bzw. bestimmbaren Eigenschaften, ab. Insgesamt muss Resilienz aber auf alle Schutzziele – und auf alle Datenschutz-Grundsätze – wirken.

Die für den Datenschutz geforderten operativen Eigenschaften einer resilienten Verarbeitung werden durch die Schutzziele des Datenschutzes erfasst und mit den jeweils zugeordneten Maßnahmen umgesetzt. Zur Resilienz einer Verarbeitung im Sinne der DSGVO kann beitragen, wenn a) das gesamte Set an Schutzmaßnahmen geschützt ist, b) dabei eine Vielfalt unterschiedlicher Implementationen und Prozesse eingesetzt wird und c) durch die Resilienz-Maßnahmen keine gegenläufigen Effekte auftreten. Wie auch bei den anderen Anforderungen appelliert die DSGVO dafür, die notwendigen Garantien in die Technik und Prozesse einzubauen. Insoweit adressiert Art. 25 DSGVO, der mit seiner Gestaltungsanforderung auf die gesamte Grundverordnung wirkt, selbstverständlich auch „Resilience by Design". Das führt technologisch zwangsläufig zu einer weiteren Erhöhung des Automatisierungsgrads und letztlich zu Schutzverfahren, mit denen einzelne Schutzmaßnahmen betrieben werden.

Wichtig aber ist, dass die Systemgestaltung der Grundverordnung nicht bei der Informationssicherheit stehenbleibt. Zwar mangelt es heutzutage mit einer agilen „Quick & Dirty"-Entwicklung nicht nur an eingebautem Datenschutz, sondern auch an „Security by Design", doch muss mit der Datenschutz-Grundverordnung der Fokus gegenüber den etablierten, oft weitgehend ausdifferenzierten Frameworks und Standards deutlich verschoben werden: Es geht nicht um die Assets der Organisation, die Datenschutz möglicherweise primär als leidige Compliance-Aufgabe und Absicherung gegen Haftungsansprüche oder einen etwaigen Shitstorm begreift. Sondern im Mittelpunkt stehen die europäischen Grundrechte und damit der Mensch: Die Risiken für die Rechte und Freiheiten natürlicher Personen sind einzudämmen. Es müssen nicht nur physische und materielle, sondern auch immaterielle mögliche Schäden bedacht werden; beispielsweise dürfen potenzielle Diskriminierungen oder gesellschaftliche Nachteile nicht ignoriert werden (vgl. ErwGr. 75). Aus diesem Grund reicht ein reines Copy & Paste von Maßnahmen aus der bisherigen Resilienz-Literatur mit Fokus auf Informationssicherheit nicht aus, sondern es bedarf – wie auch bei den anderen Anforderungen der Systemgestaltung – der neuen Perspektive der DSGVO, die nicht nur Einzug halten muss in alle Frameworks und Standards, die von den Anwendern herangezogen werden, sondern darin als zentrales Leitmotiv die Vorgaben im Sinne eines eingebauten Datenschutz formulieren soll.

Literatur

Asimov, 1942: Runaround, in Astounding Science-Fiction, März 1942, 94-103.

Bishop et al., 2011: Resilience is More than Availability, in Proc. 2011 New Security Paradigms Workshop.

Bock/Robrahn, 2018: Schutzziele als Optimierungsgebote, in DuD 42(1), 30-35.

Clarke, 1993/1994: Asimov's Laws of Robotics – Implications for Information Technology, IEEE Computer 26 (12/1993), 53-61, und 27 (1/1994), 57-66.

Dobson/Randell, 1986: Building Reliable Secure Computing Systems out of Unreliable Insecure Components, in Proc. IEEE Symposium on Security and Privacy, 187-193.

ENISA, 2011: Ontology and taxonomies of resilience, V1.0.

Hansen in Simitis/Hornung/Spiecker gen. Döhmann, 2018: Datenschutzrecht: DSGVO mit BDSG (im Erscheinen).

Hjadjk in Ehmann/Selmayr: Datenschutz-Grundverordnung: DS-GVO, 1. Auflage, München 2017.

IIA (The Institute of Internal Auditors), 2013: The Three Lines of Defense in effective Risk Management and Control. Position Paper, Januar 2013, https://www.theiia.org/3-Lines-Defense.

Jandt in Kühling/Buchner: Datenschutz-Grundverordnung, 1. Auflage, München 2017.

Jergl in Gierschmann et al.: Kommentar Datenschutzgrundverordnung, Köln 2018.

Madni/Jackson, 2009: Towards a Conceptual Framework for Resilience Engineering, in IEEE Systems Journal Vol. 3 Issue 2.

Martini in Paal/Pauly: Datenschutz-Grundverordnung, 2. Auflage, München 2018.

Mavroudis et al., 2017: A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components, in 24th ACM Conference on Computer and Communications Security, 1583-1600.

Piltz in Gola: Datenschutz-Grundverordnung VO (EU) 2016/679: DS-GVO, 1. Auflage, München 2017.

Rost/Bock, 2011: Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen, in DuD (42)1, 30-35.

Rost/Storf, 2013: Zur Konditionierung von Technik und Recht mittels Schutzzielen, in Horbach (Hrsg.), 2013: Informatik 2013 – Informatik angepasst an Mensch, Organisation und Umwelt, LNI, Vol P-220, 2149-2166.

Rost, 2018: Die Ordnung der Schutzziele, in DuD (42)1, 13-18.

Shamir, 1979: How to Share a Secret, Comm. ACM 22, 11, 612-613.

Thoma, 2014: Resilienz By Design, Strategien für die technologischen Zukunftsthemen, acatech-Studien, April 2014.

Wieland/Wallenburg, 2013: The influence of relational competencies on supply chain resilience: a relational view. International Journal of Physical Distribution & Logistics Management, Vol. 43 No. 4, 300-320.