01.24

PinG

Privacy in Germany

12. Jahrgang
Januar 2024
Seiten 1–46

www.PinGdigital.de

DATENSCHUTZ UND COMPLIANCE

ESV ERICH SCHMIDT VERLAG
100 Jahre

PinG-Podcast

Karina Filusch, LL. M., ist Fachanwältin für IT-Recht und auf Datenschutz spezialisiert. Sie ist zertifizierte Datenschutzbeauftragte und berät Unternehmen, Verbände, Vereine, Privatpersonen und Hochschulen.

Dr. Aleksandra Sowa ist zertifizierte Datenschutzauditorin und Datenschutzbeauftragte. Sie ist Sachverständige für IT-Sicherheit, Buchautorin und Spezialistin für Informationssicherheit und technischen Datenschutz.

Meldepflichten bei Sicherheitsvorfällen und Datenpannen

Status quo und Ausblick

Karina Filusch und Dr. Aleksandra Sowa

Pflichten zur Meldung von Datenpannen gemäß der DSGVO bestehen grundsätzlich für alle Organisationen. Meldepflichten für Sicherheitsvorfälle betreffen dagegen ausgewählte Zielgruppen, die sowohl im BSI-Gesetz, in der konkretisierenden BSI-KritisV als auch in einer Reihe weiterer Vorschriften definiert werden und inzwischen weit über die ursprünglichen Adressaten, die Betreiber Kritischer Infrastrukturen, hinaus reichen. Dadurch werden die Meldepflichten zunehmend intransparent. Der Beitrag berücksichtigt die aktuelle Rechtsprechung z. B. zum Entfallen der Erheblichkeitsschwelle in der Risikobewertung nach der DSGVO sowie die neue Rechtslage zur Meldung von Sicherheitsvorfällen.

I. Einführung

Komplexität sei der Feind der Sicherheit, heißt es in den entsprechenden Expertenkreisen. Dies trifft nicht nur auf die steigende Komplexität der IT-Infrastruktur oder IT-Landschaft zu, sondern auch auf die erhöhte Diversität und Komplexität der Soft- oder Hardware, die ihren Nutzern sowie Anwendern regelmäßig den Einblick in den Sourcecode der Apps oder das Innere der Geräte unter dem Verweis auf den Schutz der Urheberrechte, Patente, den Datenschutz etc. verbietet. Je unübersichtlicher die Architektur, je weniger Einblick in die IT-Systeme einer Organisation, die diese einsetzt, desto schwieriger gestaltet sich die Aufgabe, eine angemessene Sicherheit, im Sinne geeigneter Maßnahmen und Kontrollen, für das gesamte System und/oder seine Bestandteile zu gewährleisten. Gleichzeitig fallen die Identifizierung, die Analyse sowie die Bewertung von Risiken deutlich schwerer, die sich im Hinblick auf den Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit (personenbezogener) Daten und/oder der Systeme ergeben könnten.

Dies gilt auch für eine wirksame Umsetzung der Anforderungen an das Datenschutzmanagement, die sich nicht zuletzt gemäß Art. 32 DSGVO technischer und organisatorischer Mittel, der Verschlüsselung sowie weiterer Sicherheitsmaßnahmen bedient, um die Anforderungen des Schutzes informationeller Selbstbestimmung in informatischen Systemen zu erfüllen. Nicht ohne Grund versucht die Regulierung, die Komplexität einzugrenzen, beispielsweise durch Pflichten zur Führung von Verfahrensverzeichnissen. Für zahlreiche Organisationen oder Unternehmen war die DSGVO der erste Anlass seit Jahren, ihre Prozesse und die darin erfolgende Datenverarbeitung systematisch zu erfassen.

Ein weiterer Aspekt der wachsenden Komplexität kann sich negativ auf die Informationssicherheit auswirken. Gemeint ist das wachsende regulatorische Framework zu den Anforderungen an die IT-Sicherheit, das multiple Zielgruppen mit unterschiedlichen Anforderungen mittels verschiedener Rechtsvorschriften konfrontiert. Dies wirkt sich, wie wir in diesem Beitrag zeigen werden, insbesondere auf die Meldepflichten von Unternehmen und/oder Behörden bezüglich Sicherheitsvorfällen und Datenpannen aus.

Während das Anforderungsprofil der Meldepflichten über Datenpannen (Data Breach) gemäß Art. 33 DSGVO sowie Benachrichtigungspflichten an die Betroffenen gemäß Art. 34 DSGVO weitestgehend konstant geblieben ist und im Laufe der Jahre weitere Vereinheitlichung erfahren hat,[1] verhält es sich mit den Meldepflichten für Sicherheitsvorfälle eher umgekehrt. Anstelle einer Vereinheitlichung ist eine zunehmen-

1 Zuletzt im Kontext der europaweiten Bemühungen zur Vereinheitlichung der Höhe von Bußgeldern. Vgl. BfDI, Gemeinsame Pressemitteilung – Einheitliche Regeln für Datenschutzbußgelder in Europa (1/2023, 8. Juni 2023), 2023, https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2023/gemeinsame-PM-Bußgeld-Leitlinien.html.

de Komplexität und Diversifizierung zu beobachten: Zuerst mit dem Beschluss des IT-Sicherheitsgesetzes 2.0 (ITSiG 2.0), darauffolgenden Anpassungen, dessen Adressatenkreis im BSI-Gesetz (BSIG) ausgeweitet wurde, der Definition von Ausnahmen, die wiederum in anderen Rechtsvorschriften adressiert werden könnten, sowie der Diversifizierung im Hinblick darauf, was und wann und an wen gemeldet werden sollte. Dem folgt das KRITIS-DachG, wonach eine zusätzliche Meldeinstanz neben der zentralen Meldestelle, dem Bundesamt für Sicherheit in der Informationstechnik (BSI), etabliert werden sollte. Weitere Neuerungen sind zudem im Rahmen der Umsetzung der NIS2-Richtlinie der EU in die nationale Gesetzgebung mit dem Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit (NIS2UmsuCG)[2] zu erwarten.

Ziel des vorliegenden Beitrages ist es, (1) die aktuellen Änderungen in den Anforderungen an die Meldepflichten gegenüber den Anforderungen aus dem ersten ITSiG zu erfassen und zu systematisieren sowie (2) Synergien aufzuzeigen, die sich aus der gemeinsamen Umsetzung der Anforderungen aus den unterschiedlichen Gesetzen zur IT-Sicherheit und der DSGVO ergeben.

II. Melde- und Benachrichtigungspflichten nach der DSGVO in Zahlen

Die DSGVO sieht in Art. 33 und 34 DSGVO vor, dass in bestimmten Fällen eine Meldung an die zuständige Datenschutzaufsichtsbehörde bzw. die Betroffenen erfolgen muss. Seit Inkrafttreten der DSGVO im Mai 2018 habe sich die Zahl der Meldungen verzehnfacht, so der Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) Baden-Württemberg.[3] Im Bericht 2022 der Berliner Beauftragten für Datenschutz und Informationsfreiheit findet sich ein Anstieg von 52 Meldungen im Jahr 2017 auf 1.015 Meldungen im Jahr 2019. In den folgenden Jahren blieben die Meldungen konstant hoch.[4] Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) zählte 2022 10.614 Meldungen nach Art. 33 DSGVO.[5] Bei dieser Menge an Verstößen stellen sich Fragen zu den Meldungen und Benachrichtigungen.

III. Gemeinsame Voraussetzungen der Art. 33 und 34 DSGVO – Vorliegen einer sogenannten Datenpanne

Nach Art. 33 f. DSGVO ist das melde- bzw. benachrichtigungspflichtige Ereignis eine „Verletzung des Schutzes personenbezogener Daten". Gemäß Art. 4 Nr. 12 DSGVO in Verbindung mit Erwägungsgrund 75 und 85 ist dies unter anderem[6]

- eine Verletzung der Sicherheit,
- eine Vernichtung,
- ein Verlust,
- eine Veränderung,
- eine unbefugte Offenlegung,
- eine unbefugte Aufhebung der Pseudonymisierung oder
- ein Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten.

Personenbezogene Daten müssen gemäß Art. 5 Abs. 1 lit. f) DSGVO „in einer Weise verarbeitet werden, die ein angemessenes Schutzniveau der personenbezogenen Daten gewährleistet". Der Europäische Datenschutzausschuss (EDSA) unterteilt Datenschutzverletzungen in die drei Kategorien Verfügbarkeit, Integrität und Vertraulichkeit und unterscheidet überdies sechs verschiedene Datenschutzvorfälle:

- Ransomware-Angriffe,
- Angriffe mit Datenabfluss,
- Risiken durch internes Personal,
- Verlust oder Diebstahl von Geräten oder Dokumenten,
- Datenschutzverletzungen im Zusammenhang mit postalischen Versendungen und
- Social-Engineering-Attacken.[7]

1. Verletzung des Art. 32 DSGVO

Beispielfall: Das Unternehmen A trifft keinerlei Vorkehrungen zum Schutz von Personalakten. Die Personalerin B dieses Unternehmens lässt eine Personalakte mit Gesundheitsdaten des Mitarbeiters C offen liegen, sodass andere Mitarbeitende die Akte zur Kenntnis nehmen.

Die technischen und organisatorischen Maßnahmen sind verletzt, weil die Personalerin im Unternehmen nicht instruiert wurde, dass Personalakten so aufzubewahren sind, dass Dritte keine Kenntnisse erlangen können. Es liegt demnach ein Organisationsverschulden vor, und es fehlt an der technischen Absicherung.

Beispielfall: Anwalt R ist mit einem Fall beim Sozialgericht befasst. Sein System für den sicheren Übertragungsweg ist nicht verfügbar. Der Anwalt entschließt sich unter Zeitdruck, die Klageerwiderung an das Sozialgericht per Fax zu versenden.

Das Fax entspricht in einigen Bundesländern laut deren Landesdatenschutzbeauftragten wie z. B. in Bremen, Hessen

2 Vgl. BMI, 2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG, Referentenentwurf (Bearbeitungsstand 03.04.2023).

3 https://www.baden-wuerttemberg.datenschutz.de/datenschutzverletzungen-bereiten-zunehmend-sorge/ (zuletzt abgerufen am 4.12.2023).

4 https://www.datenschutz-berlin.de/jahresbericht-2022#_idTextAnchor114 (zuletzt abgerufen am 4.12.2023).

5 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/31TB_22.pdf?__blob=publicationFile&v=7, S. 111 (zuletzt abgerufen am 4.12.2023).

6 Mehr zu den einzelnen Begriffen: *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 65; *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 33 Rn. 32–38; *Becker*, ZD 2020, 175 f.

7 EDSA, Guidelines 1/2021 on Examples regarding Data Breach Notification (Version 2.0), Rn. 5.

und Bayern nicht den technischen Anforderungen an eine sichere Übermittlung[8] und ist im Hinblick auf die Sicherheit vergleichbar mit dem Versand einer Postkarte.[9]

2. Verletzung des Art. 6 DSGVO

Erfolgt dagegen keine Verletzung der technischen und organisatorischen Maßnahmen, sondern eine Verletzung des Art. 6 DSGVO, findet also eine Datenverarbeitung ohne Rechtsgrundlage statt und liegt kein sicherheitsrelevantes Ereignis vor, ergibt sich keine Melde- bzw. Benachrichtigungspflicht.[10]

3. Verletzungshandlung und -erfolg

Es müssen eine Verletzungshandlung und ein Verletzungserfolg vorliegen.[11]

Beispielfall: Hacker dringen in fremde Systeme des Unternehmens D ein. Sie haben keinen Zugang zu personenbezogenen Daten erlangt.[12]

Die Systeme waren nicht vor Hackerangriffen geschützt, die TOMs sind verletzt, aber der die Meldepflicht auslösende Verletzungserfolg fehlt (kein Zugriff auf die personenbezogenen Daten). In solchen Fällen, in denen ein Zugriff auf personenbezogene Daten ausgeschlossen werden kann, muss eine Meldung bzw. Benachrichtigung nicht erfolgen.

Beispielfall: Unbekannte hacken sich in die Systeme des Unternehmens E. Diesmal greifen die Hacker auf die personenbezogenen Daten zu und verschlüsseln diese zusätzlich und verlangen ein Lösegeld für die Entschlüsselung (Ransomware-Angriff).[13] Ein Backup ist nicht vorhanden.

Die rechtliche Bewertung ändert sich nun. Die Hacker konnten auf die Daten zugreifen und es gibt keine Datensicherung der Daten, sodass diese verloren gegangen sind. Damit ist eine Meldung nach Art. 33 DSGVO erforderlich.

Ist nicht sofort festzustellen, ob eine Verletzungshandlung oder ein Verletzungserfolg vorliegt, sind zunächst Nachforschungen anzustellen.[14] Ist nach weiteren Nachforschungen weiterhin unklar, ob es zu einer Verletzungshandlung oder einem Verletzungserfolg gekommen ist, empfiehlt der EDSA, den Sachverhalt im Zweifel der zuständigen Aufsichtsbehörde zu melden.[15]

4. Verletzungsverursacher

Aus dem zuvor genannten Beispiel geht bereits hervor, dass eine Verletzung des Schutzzwecks nicht durch den/die Verantwortliche*n ausgelöst werden muss. Sie kann auch andere Ursachen haben.

a. Gemeinsame Verantwortlichkeit

Eine Datenpanne kann auch im Rahmen gemeinsamer Verantwortlichkeit erfolgen. Einer Ansicht nach ist nach Außenverhältnis und Innenverhältnis getrennt zu unterscheiden. Im Außenverhältnis sind beide zur Meldung verpflichtet.[16] Die Parteien können vertraglich über die gemeinsame Verantwortlichkeit oder das „Joint Controller Agreement" vereinbaren, dass eine Partei meldet. Der vertraglich Verpflichtete muss melden; der Vertrag bindet lediglich im Innenverhältnis.[17] Einer anderen Ansicht nach soll Art. 26 Abs. 1 S. 2 DSGVO zufolge derjenige verpflichtet sein, die Meldung an die Aufsichtsbehörde zu machen, der vertraglich dazu verpflichtet wurde.[18] Sollte eine solche Vereinbarung fehlen, ist derjenige zur Meldung verpflichtet, in dessen Sphäre die Verletzung entstanden ist[19] bzw. einer anderen Ansicht nach sind beide für die Meldung verantwortlich.[20]

b. Auftragsverarbeitung

Nach Art. 33 Abs. 2 DSGVO meldet der Auftragsverarbeiter dem/der Verantwortlichen unverzüglich die Datenpanne – die Meldepflicht gilt qua Gesetz.[21] Der/die Verantwortliche meldet daraufhin der Datenschutzaufsicht, sofern eine Pflicht dazu besteht. Die Regelungen können auch in einem Vertrag geregelt werden, würden in diesem Fall jedoch nur neben der gesetzlichen Regelung stehen.[22]

5. Schuld (Fahrlässigkeit oder Vorsatz)

Weder die Datenpanne noch die sich daran anknüpfenden Melde- und Benachrichtigungspflichten setzen ein Verschulden voraus, sodass auch höhere Gewalt als Ursache einer Datenpanne denkbar ist.

Beispielfall: Der Serverraum des Unternehmens Z steht im Erdgeschoss. Am 14. Juli 2021 kommt es zu schwersten Regenfällen. Es kommt zu einem Wasserschaden. Die Server, auf denen alle personenbezogenen Daten und deren Backups sind, werden durch das Wasser zerstört.

8 https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/uebermittlung-personenbezogener-daten-per-fax (zuletzt abgerufen am 3.12.2023) https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen-und-handlungshilfen/telefax-ist-nicht-datenschutzkonform-16111 (zuletzt abgerufen am 3.12.2023) https://www.datenschutz-bayern.de/datenschutzreform2018/AP_Telefax.pdf (zuletzt abgerufen am 3.12.2023) https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/uebermittlung-personenbezogener-daten-per-fax (zuletzt abgerufen am 3.12.2023).

9 Niedersächsisches OVG, Beschl. v. 22.07.2020 – 11 LA 104/19.

10 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 64.

11 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 63–65.

12 Beispiel angelehnt an: *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 69.

13 Beispiel angelehnt an: *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 69.

14 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 74.

15 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_de, Rn. 119 (zuletzt abgerufen am 4.12.2023).

16 *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 33 Rn. 20.

17 *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 33 Rn. 20.

18 *Martini*, in: Paal/Pauly, DS-GVO, Art. 33 Rn. 14a; *Hanßen* in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 61.

19 *Hanßen* in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 61.

20 *Martini*, in: Paal/Pauly, DS-GVO, Art. 33 Rn. 14a.

21 *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 33 Rn. 22.

22 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 62.

In diesem Fall hat das Unternehmen Z nicht dafür gesorgt, dass die Server an einem sicheren ggf. georedundanten[23] Ort stehen, sodass ein Organisationsverschulden des Unternehmens vorliegt und somit eine Verletzung der Sicherheit der personenbezogenen Daten eingetreten ist, die sich in der Vernichtung aller personenbezogenen Daten konkretisiert hat.

6. Risikobewertung

Eine Meldung muss gemäß Art. 33 Abs. 1 S. 1 DSGVO nicht erfolgen, wenn die Datenpanne *„voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen“* führt. Demzufolge muss für eine Meldepflicht ein Risiko bestehen.

Daraus ergeben sich drei Risikobegriffe: kein Risiko, Risiko und das hohe Risiko[24] aus Art. 34 Abs. 1 Satz 1 DSGVO.

kein Risiko	Risiko	hohes Risiko

Laut Datenschutzkonferenz bestünde eine Meldepflicht nicht, wenn kein Risiko oder lediglich ein geringfügiges Risiko vorläge und begründet dies damit, dass es eine vollkommen risikolose Verarbeitung nicht geben könne und es deshalb als geringes Risiko zu verstehen sei.[25] Mit der EuGH-Rechtsprechung[26] dürfte sich die Einstufung des Risikos in verschiedene Erheblichkeitsschwellen erledigt haben. Nun muss nur noch unterschieden werden, ob ein Risiko (egal wie schwer) oder kein Risiko besteht.

Erwägungsgrund 85 S. 1 der DSGVO beschreibt, wann ein Risiko besteht: wenn Verletzungen des Schutzes personenbezogener Daten einen *„physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen“*. Wann dies im Einzelfall vorliegt, insbesondere was den immateriellen Schaden angeht, ist hochkomplex und wird aktuell von der Rechtsprechung[27] entwickelt. Die Darstellung dieses Themenkomplexes würde sich für einen gesonderten Aufsatz eignen.

IV. Weitere Voraussetzungen des Art. 33 DSGVO

1. Inhalt der Meldung

Eine Meldung soll nach Art. 33 Abs. 3 DSGVO, soweit bekannt, mindestens folgende Punkte enthalten:

- Nennung des/der Verantwortlichen, auch wenn das Gesetz das nicht explizit fordert,[28]
- Beschreibung der Verletzung,
- soweit möglich mit Angabe zu den Kategorien und der ungefähren Zahl der betroffenen Personen sowie der betroffenen personenbezogenen Datensätze,[29]
- Kontakt zum*zur Datenschutzbeauftragten oder zuständigen Person,
- Beschreibung der wahrscheinlichen Folgen der Verletzung und
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen.

2. Risiken bei der Meldung

Die Meldung an die Aufsichtsbehörden birgt Risiken und Chancen. Ein Unterlassen der Meldung dürfte im Entdeckungsfall Maßnahmen der Aufsichtsbehörde (Art. 58 DSGVO) sowie ein Bußgeld nach sich ziehen.

Die Meldung an die Aufsichtsbehörden unterliegt menschenrechtlichen sowie verfassungsrechtlichen Beschränkungen der Selbstbelastungsfreiheit (nemo tenetur se ipsum accusare).[30] Der Selbstbelastungsfreiheit steht jedoch der Erkenntnisgewinn der Aufsichtsbehörden und damit der Allgemeinheit entgegen.[31] Ein stringentes Durchsetzen des Grundsatzes „nemo tenetur“ könnte die proaktive Gefahrenabwehr im Datenschutz, insbesondere in der Entwicklung von ISO 27001 und DSGVO entsprechenden wirksamen TOMs, erschweren. Die öffentliche Verfügbarkeit von wirksamen TOMs und Erkenntnissen stellt dabei einen Fortschritt im Datenschutz dar.[32] Anonyme Meldungen sind dabei abzulehnen, da weitergehende Informationen zur Erarbeitung wirksamer TOMs in der Regel erforderlich sind. Ohne Meldepflichten, die Zusammenarbeit des technischen Datenschutzes durch das BSI und die Arbeit der Aufsichtsbehörden wäre ein Mehr an Datenschutz lediglich unter erschwerten Bedingungen erreichbar. In Bezug auf den BfDI ist für die Veröffentlichung der Berichte und Bescheide derzeit eine Anfrage nach dem Informationsfreiheitsgesetz (IFG) anhängig, deren Ausgang noch offen ist.[33] Der Grundsatz „nemo tenetur“ ist zumindest im deutschen Recht in den §§ 42 Abs. 4; 43 Abs. 4 BDSG durch den Gesetzgeber verankert worden. Die Risiken einer Sanktionierung durch den Staat bei einer Meldung sind durch „nemo-tenetur“ begrenzt. Betroffene haben die Möglichkeit, zum Beispiel durch Beschwerden nach Art. 77 DSGVO und Akteneinsicht oder IFG-Anfragen bei den Aufsichtsbehörden zivilrechtlich relevante Informationen zu erlangen. Die Aufsichtsbehörde kann daraufhin dennoch gegen den/die Verantwortliche*n vorgehen, weil dies nicht von der Selbstbelastungsfreiheit gedeckt ist.[34]

23 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/Standort-Kriterien_Rechenzentren.pdf?__blob=publicationFile&v=1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/Standort-Kriterien_Rechenzentren.pdf?__blob=publicationFile&v=1

24 Ausführlich hierzu Murati, PinG 2024, S. 33 ff.

25 Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, S. 2.

26 EuGH, Urt. v. 04.05.2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, ECLI:EU:C:2023:370.

27 Bspw. EuGH, Urt. v. 04.05.2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, ECLI:EU:C:2023:370.

28 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 70.

29 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 70.

30 BVerfG, Beschl. v. 13.10.2003 – 2 BvR 1321/02.

31 Niedersächsisches OVG, Beschl. v. 04.04.2012 – 8 ME 49/12.

32 BfV Cyber-Brief Nr. 02/2023: https://tinyurl.com/4z6ajhyt (zuletzt abgerufen am 4.12.2023).

33 Abrufbar unter: https://fragdenstaat.de/anfrage/saemtliche-bisher-erlassen-massnahmen-nach-art-58-dsgvo-1/ (zuletzt abgerufen am 4.12.2023).

34 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 1. Aufl. 2020, S. 82.

3. Formalien

a. Zuständige Behörde

Die Frage nach der zuständigen Behörde ist lediglich in bestimmten Konstellationen kompliziert (siehe unter III. 4. zur gemeinsamen Verantwortlichkeit). Handelt es sich um einen Auftragsverarbeiter, ist nicht dessen Aufsichtsbehörde zuständig, sondern die des/der Verantwortlichen. Der Auftragsverarbeiter meldet ausschließlich an den Verantwortlichen und unterstützt diesen ggf. bei dessen Meldung gegenüber der Aufsichtsbehörde.

Bei grenzüberschreitenden Sachverhalten, so auch der EDSA, sollte bei der Aufsichtsbehörde gemeldet werden, innerhalb deren Zuständigkeitsbereich der/die Verantwortliche seinen/ihren Hauptsitz hat (One-Stop-Shop-Prinzip). Zudem wird empfohlen die Aufsichtsbehörde, in deren Zuständigkeitsbereich das Ereignis örtlich stattfand, mit der Information, wohin die Meldung erfolgt ist, in Kenntnis zu setzen.[35] Bei Unklarheiten empfiehlt es sich bei der Behörde zu melden, in deren Zuständigkeitsbereich sich die Datenschutzverletzung örtlich ereignet hat.[36]

b. Frist: 72 Stunden

Nach Art. 33 Abs. 1 S. 1 DSGVO ist die Verletzung der Sicherheit personenbezogener Daten *„unverzüglich“* zu melden. Unverzüglich meint in der deutschen Auslegung *„ohne schuldhaftes Zögern“* im Sinne des § 121 Abs. 1 BGB,[37] wobei es an sich nicht möglich ist, dass nationales Recht Europarecht aufgrund des „effet utile“ determiniert. Laut Art. 33 Abs. 1 S. 1 DSGVO soll die Meldung *„möglichst binnen 72 Stunden“* erfolgen. Daraus wird deutlich, dass es sich nicht um eine starre Frist handelt. Die Frist läuft ab Kenntnis von den tatsächlichen Umständen, die die Meldepflicht des/der Verantwortlichen begründen. Benötigt diese/r länger, um festzustellen, ob es zu einer Verletzung der Sicherheit gekommen ist, darf er/sie diesen Ermittlungen nachgehen.[38] Er/sie muss gemäß Art. 33 Abs. 1 S. 2 DSGVO lediglich begründen, wieso es zu der Verzögerung kam.

c. Berechnung der Frist

Die DSGVO selbst sieht keine Regelung zur Berechnung der Frist vor. So muss überlegt werden, auf welcher Grundlage die Frist berechnet wird. In Betracht käme die Berechnung nach nationalem Recht, in Deutschland nach BGB, was jedoch dem „effet utile“ zuwiderlaufen würde. Die vorherrschende Meinung ist, dass die Frist nach der Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine (VO (EWG) Nr. 1182/71) berechnet wird.[39]

d. Form der Meldung

Art. 33 DSGVO schreibt keine bestimmte Form vor.[40] Die meisten Datenschutzaufsichtsbehörden bieten Onlineformulare zur Meldung von Datenpannen an.[41]

V. Abweichende Regelungen des Art. 34 DSGVO

1. Hohes Risiko

Art. 34 DSGVO verfügt über ähnliche Voraussetzungen wie Art. 33 DSGVO, aber es muss ein hohes Risiko vorliegen. Davon ist auszugehen, wenn besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO, personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO oder Daten aus Profilings sowie aus der systematischen Überwachung öffentlich zugänglicher Bereiche im Sinne des Art. 35 Abs. 3 DSGVO betroffen sind.[42] Auch Bankverbindungs- und Kreditkartendaten oder personenbezogene Daten, die einem Berufsgeheimnis unterliegen, fallen darunter.[43]

2. Ausnahmen von der Benachrichtigung

In einigen Fällen muss der/die Verantwortliche die betroffene Person gemäß Art. 34 Abs. 3 DSGVO nicht benachrichtigen:

- Der/die Verantwortliche hat zum Schutz der Rechte und Freiheiten der betroffenen Personen geeignete TOMs getroffen, die im konkreten Fall Anwendung finden,
- Der/die Verantwortliche hat nachfolgende Maßnahmen getroffen, sodass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht.
- Die Benachrichtigung würde einen unverhältnismäßig hohen Aufwand für den/die Verantwortliche*n bedeuten. In der Regel tritt an die Stelle der Benachrichtigung in diesem Fall die öffentliche Bekanntmachung.

3. Frist, Inhalt, Formalien

Die Meldung soll unverzüglich, also ohne schuldhaftes Zögern, erfolgen.[44] Inhaltlich soll die Meldung gemäß Art. 34 Abs. 2 DSGVO in Verbindung mit Art. 33 Abs. 3 lit. b)–d) DSGVO folgende Punkte erfassen:[45]

- Kontakt zum*zur Datenschutzbeauftragten oder zur zuständigen Person,
- Beschreibung der wahrscheinlichen Folgen der Verletzung und
- ergriffene und vorgeschlagene Maßnahmen.

35 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 1. Aufl. 2020, S. 76.

36 Artikel-29-Datenschutzgruppe, WP 250 rev.01 (Stand: 06.02.2018), S. 19 f., bestätigt durch den EDSA am 25.05.2018.

37 *Brink*, in: BeckOK DatenschutzR, 44. Ed. 01.02.2022, DS-GVO, Art. 33 Rn. 33.

38 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 74.

39 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 75; *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 33 Rn. 70.

40 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 76 f.; *Brink*, in: BeckOK DatenschutzR, 44. Ed. 01.02.2022, DS-GVO, Art. 33 Rn. 31.

41 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 78 f – Hinweis: Inzwischen hat auch die LDA Brandenburg ein Meldeformular online gestellt.

42 *Brink*, in: BeckOK DatenschutzR, 44. Ed. 01.02.2022, DS-GVO, Art. 34 Rn. 26.

43 *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 34 Rn. 9.

44 *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 34 Rn. 25.

45 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 80.

Die Meldung muss in „klarer und einfacher Sprache", Art. 34 Abs. 2 DSGVO, abgefasst sein und hat in präziser, transparenter und leicht zugänglicher Form zu erfolgen.[46]

4. Folgen bei Verstößen gegen die Melde- und Benachrichtigungspflicht nach DSGVO

Bei einer nicht erfolgten oder unvollständigen Meldung oder Benachrichtigung kann die Aufsichtsbehörde Bußgelder nach Art. 83 Abs. 4 lit. a) DSGVO verhängen. Auch gegen den Auftragsverarbeiter kann ein Bußgeld wegen einer fehlenden oder unvollständigen Meldung verhängt werden[47] und dies kann als Ordnungswidrigkeit von der Aufsichtsbehörde gemäß § 41 Abs. 2 BDSG verfolgt werden. Gemäß § 43 Abs. 3 BDSG können Bußgelder nicht für Behörden und öffentliche Stellen verhängt werden, solange diese nicht am Wettbewerb teilnehmen.[48] Die Aufsichtsbehörde kann dem/der Verantwortlichen gegenüber anordnen, die Benachrichtigung der betroffenen Personen gemäß Art. 58 Abs. 2 lit. e) DSGVO nachzuholen.[49] Die Datenschutzaufsicht kann zudem eine Anordnung zur Anpassung, Beschränkung oder sogar zum Verbot (Art. 58 Abs. 2 lit. f) DSGVO) von Verarbeitungen erlassen, zum Beispiel wenn der/die Verantwortliche wiederholt Verstöße begangen hat.[50] Des Weiteren kann die Datenschutzaufsicht eine Verwarnung gegenüber dem/der Verantwortlichen gemäß Art. 58 Abs. 2 lit. b) DSGVO aussprechen.

VI. Meldepflichten für (IT-)Sicherheitsvorfälle – Aktuelle Lage

Einen wesentlichen Beitrag dazu, einheitliche Meldepflichten für relevante Bereiche der Kritischen Infrastrukturen in Deutschland einzuführen, leistete das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, ITSiG). Mit dem IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) wurden die Meldepflichten weiter ausgebaut und umfassen weitere Gruppen von Unternehmen und Betreibern Kritischer Infrastrukturen. Welche Anbieter konkret betroffen sind, wird in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)[51] festgelegt. Mit dem ITSiG 2.0 sollte der *„mit dem IT-Sicherheitsgesetz geschaffene Ordnungsrahmen"* erweitert werden. Die Maßnahmen zielen – neben dem Schutz des Bürgertums und der Stärkung des Staats – auch auf *„eine resiliente Wirtschaft"* ab.

Meldepflichten für (wesentliche) Sicherheitsvorfälle werden, beginnend mit dem ITSiG 2.0, zunehmend dezentral reguliert. Verpflichtungen für Betreiber Kritischer Infrastrukturen gemäß Definition in § 2 Abs. 10 BSIG, konkretisiert durch die Rechtsverordnung nach § 10 Abs. 1 BSIG, für die digitalen Dienste bzw. Anbieter digitaler Dienste gemäß Definition in § 2 Abs. 11 BSIG sowie Unternehmen im besonderen öffentlichen Interesse (kurz: UBI) gemäß § 2 Abs. 14 BSIG, werden direkt im BSIG definiert. Hiervon gibt es zahlreiche Ausnahmen, beispielsweise für Betreiber öffentlicher Telekommunikationsnetze oder Energieanlagen, die mitnichten von den Meldepflichten befreit sind, sondern durch andere Rechtsvorschriften reguliert werden.

1. Meldepflichten und Rechte Betreiber Kritischer Infrastrukturen bei Störungen und erheblichen Störungen

Den Grundstein der KRITIS-Regulierung in Deutschland bildet das BSI-Gesetz (BSIG). Gemäß § 8b Abs. 1 BSIG ist das BSI die „zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik". Dies bringt zahlreiche Pflichten für das BSI mit sich – beispielsweise erstellt und veröffentlicht das BSI jährlich ein Lagebild zur IT-Sicherheit –, räumt ihm zugleich jedoch eine Vielzahl an Rechten und Befugnissen gegenüber den Betreibern Kritischer Infrastrukturen ein, die unter anderem dazu verpflichtet sind, sich gemäß § 8b Abs. 3 beim BSI zu registrieren und eine Kontaktstelle bzw. gemäß § 8b Abs. 5 eine „gemeinsame übergeordnete Ansprechstelle" (gilt nur für Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören) zu benennen.

Betreiber Kritischer Infrastrukturen haben gemäß § 8b Abs. 4 die folgenden Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse unverzüglich über die Kontaktstelle an das BSI zu melden:

- Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben (Nr. 1),
- erhebliche Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können (Nr. 2).

Die Meldung an das BSI muss die folgenden Angaben umfassen:

- Angaben zur Störung,
- zu möglichen grenzübergreifenden Auswirkungen sowie
- zu den technischen Rahmenbedingungen,
- insbesondere der vermuteten oder tatsächlichen Ursache,
- der betroffenen Informationstechnik,
- der Art der betroffenen Einrichtung oder Anlage sowie
- zur erbrachten kritischen Dienstleistung und
- zu den Auswirkungen der Störung auf diese Dienstleistung.

Die Meldung der Störung kann anonym erfolgen: *„Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat."*

46 *Brink*, in: BeckOK DatenschutzR, 44. Ed. 01.02.2022, DS-GVO, Art. 34 Rn. 30.

47 *Brink*, in: BeckOK DatenschutzR, 44. Ed. 01.02.2022, DS-GVO, Art. 33 Rn. 19 f. und Art. 34, Rn. 17.

48 *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 33, Rn. 80; mehr zum Thema Sanktionierung von Behörden: *Filusch/Henrich/Fünfstück*, PinG 2023, 77.

49 *Brink*, in: BeckOK DatenschutzR, 44. Ed. 01.02.2022, DS-GVO, Art. 34, Rn. 44; *Reif*, in: Gola/Heckmann, 3. Aufl. 2022, DS-GVO, Art. 34, Rn. 30.

50 *Hanßen*, in: Sowa, IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit, 2020, S. 81.

51 BSI-KritisV, 2016, Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV), Ausfertigungsdatum: 22.04.2016.

Das BSI kann im Einvernehmen mit der zuständigen Aufsichtsbehörde gemäß § 8b Abs. 4a *„[w]ährend einer erheblichen Störung“* beim Betreiber Kritischer Infrastrukturen gemäß § 8b Abs. 4 S. 1 Nr. 1 oder beim Unternehmen im besonderen öffentlichen Interesse (UBI) gemäß § 8f Abs. 7 S. 1 Nr. 2 bzw. Abs. 8 S. 1 Nr. 2 *„die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen“*. Betreiber Kritischer Infrastrukturen und UBI sind damit befugt, dem BSI *„auf Verlangen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, soweit dies zur Bewältigung einer erheblichen Störung […] erforderlich ist“*. § 8b Abs. 7 regelt darüber hinaus, dass eine *„über die vorstehenden Absätze hinausgehende Verarbeitung“* auf diesem Weg erfasster personenbezogener Daten *„zu anderen Zwecken“* unzulässig ist.

a. Definition einer IT-Störung

Bei der Definition einer IT-Störung verweist das BSI auf die Begründung des ITSiG:[52] *„Eine [IT-]Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken (vgl. BT-Drs 18/4096, 28).“* Das BSI benennt einige Beispiele für IT-Störungen, die zwar keine IT-Sicherheitsvorfälle, aber dennoch meldepflichtig sind, darunter:

- ein Bagger, der ein Kabel durchtrennt,
- ein Ausfall der Kühlung eines Rechenzentrums,
- ein falsch konfiguriertes System,
- ein fehlerhaftes Update oder ein fehlerhafter Patch, der eingespielt wird.

b. Definition einer erheblichen Störung

„Eine eindeutige, umfassend geltende Antwort, wann eine Störung erheblich ist, ist nicht möglich“, erläutert das BSI.[53] Fest steht allerdings, dass gemäß § 8b Abs. 4 Nr. 2 BSIG eine erhebliche Störung gemeldet werden muss – ungeachtet dessen, ob sie zum Ausfall oder zur Beeinträchtigung von Kritischen Infrastrukturen geführt hat oder führen kann. Es ist daher *„erforderlich, dass die Verantwortlichen in KRITIS-Unternehmen Einzelfallentscheidungen treffen“*. Hierfür ist es üblich, Prozesse zu definieren, die u. a. eine Bewertung immanenter Risiken, Wesentlichkeitsbetrachtung etc. umfassen.

Das BSI veröffentlichte eine Liste an Beispielkriterien als Orientierungshilfe für die meldepflichtigen Betreiber Kritischer Infrastrukturen, die die *„IT-seitigen Auswirkungen der IT-Störung, nicht jedoch ihren Einfluss auf die kritische Dienstleistung“* berücksichtigt. Diese sei erst in einem zweiten Schritt zu betrachten.

Eine erhebliche IT-Störung liegt insbesondere vor, wenn

- eine Nichtbehandlung zu immer gravierenderen negativen Auswirkungen führen würde (zum Beispiel wenn der Ausfall einer Anlagensteuerung zu immer umfangreicheren Schäden oder der Zerstörung einer Anlage führen würde),
- zusätzliche Aufwände und Mittel eingesetzt oder eingeplant werden, die über die Aufwände und Mittel des Regelbetriebs oder bereits geplanter Arbeiten hinausgehen (zum Beispiel zusätzliche Mitarbeiter, Überstunden, Einsatz von Ersatzkapazitäten, zusätzliche Geld- oder Sachmittel),
- wichtige IT-Systeme oder Komponenten zur Vermeidung weiterer Auswirkungen abgeschaltet oder isoliert werden,
- für den Bewältigungszeitraum Betriebsprozesse geändert werden,
- sie einen hohen finanziellen Schaden verursacht,
- die Vermutung naheliegt, dass das Unternehmen Ziel eines neuartigen, außergewöhnlichen, zielgerichteten oder aus technischer Sicht bemerkenswerten Angriffs oder Angriffsversuchs ist, zum Beispiel ein sogenannter Advanced Persistent Threat (APT), und
- besondere Berichtspflichten gegenüber der Unternehmensleitung für solche IT-Störungen bestehen.[54]

2. Meldepflichten bei Ausfällen und Störfällen in den Unternehmen im besonderen öffentlichen Interesse (UBI)

Mit dem zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0) wurde mit § 2 Abs. 14 eine neue Kategorie der Unternehmen eingeführt: Unternehmen im besonderen öffentlichen Interesse (kurz UBI). Dabei handelt es sich nicht um Betreiber Kritischer Infrastrukturen gemäß § 2 Abs. 10 BSIG. Unternehmen im besonderen öffentlichen Interesse werden in drei Kategorien unterteilt:

- UBI 1 (AWV-UBI): Dazu gehören Hersteller und/oder Entwickler von Gütern im Sinne von § 60 Außenwirtschaftsrechtsverordnung (AWV-RechtsVO vom Jahr 2020). Dazu zählen Unternehmen, die im Bereich Waffen, Munition und Rüstungsmaterial oder im Bereich von Produkten mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentlicher Komponenten solcher Produkte tätig sind.
- UBI 2 (Wertschöpfungs-UBI): Dies sind die nach ihrer inländischen Wertschöpfung größten Unternehmen Deutschlands sowie wesentliche Zulieferer für diese Unternehmen. Es liegt (noch) keine Rechtsverordnung für UBI 2 vor.
- UBI 3 (Störfall-UBI): Gemäß § 2 Abs. 14 Nr. 3 handelt es sich um Betreiber *„eines Betriebsbereichs der oberen Klas-*

52 BSI, n. d., Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz, https://www.bsi.bund.de/dok/kritis-faq-meldepflicht (zuletzt abgerufen am 15.11.2023).

53 BSI, n. d., Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz, https://www.bsi.bund.de/dok/kritis-faq-meldepflicht (zuletzt abgerufen am 15.11.2023).

54 BSI, n. d., Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz, https://www.bsi.bund.de/dok/kritis-faq-meldepflicht (zuletzt abgerufen am 15.11.2023).

se im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung" oder Betreiber, die *„nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind."* Die Störfall-RechtsVO vom Jahr 2020 liegt vor.[55]

Meldepflichten für Ausfälle und/oder Störfälle für die Unternehmen im besonderen öffentlichen Interesse werden in § 8f Abs. 7 (für die Kategorien UBI 1 und UBI 2) sowie in § 8f Abs. 8 (für die Kategorie UBI 3) definiert. Gemäß § 8f Abs. 7 sind UBI 1 seit dem 1. Mai 2023 verpflichtet, dem BSI die folgenden Störungen unverzüglich zu melden: *„Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben"* (Nr. 1) oder *„erhebliche Störungen"*, die zu einem Ausfall oder erheblichen Beeinträchtigung *„führen können"* (Nr. 2). Ein Ausfall liegt nach der Definition des BSI vor, *„wenn die Funktionsfähigkeit einer KRITIS nicht mehr gegeben ist"*[56]. Nicht als Ausfall gilt laut Definition des BSI beispielsweise eine geplante Betriebsunterbrechung.

Unternehmen im besonderen öffentlichen Interesse der zweiten Kategorie müssen dem BSI gemäß § 8f Abs. 8 seit dem 1. November 2021 die folgenden Störungen unverzüglich melden: *„Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung geführt haben" (Nr. 1) oder „erhebliche Störungen"*, die zu einem Störfall *„führen können"* (Nr. 2).

Darüber hinaus ist eine Registrierung und Benennung einer Kontaktstelle dem BSI gegenüber für UBI 1 seit dem 1. Mai 2023 verpflichtend und für UBI 3 auf freiwilliger Basis möglich. Für UBI 2 fehlt noch die notwendige Rechtsverordnung.[57]

Die Meldung von Störungen an das BSI durch UBI muss gemäß § 8f Abs. 7 und 8
- Angaben zur Störung,
- zu den technischen Rahmenbedingungen,
- insbesondere zu der vermuteten oder tatsächlichen Ursache,
- der betroffenen Informationstechnik und
- der Art der betroffenen Einrichtung oder Anlage

enthalten.

55 Vgl. BSI, 2023, Flyer, Unternehmen im besonderen öffentlichen Interesse, UBI-Büro, Bonn (September 2023), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Regulierte_Unternehmen/UBI/Flyer.pdf?__blob=publicationFile&v=5 (zuletzt abgerufen am 15.11.2023).

56 BSI, n. d., Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz, https://www.bsi.bund.de/dok/kritis-faq-meldepflicht (zuletzt abgerufen am 15.11.2023).

57 Vgl. BSI, 2023, Flyer, Unternehmen im besonderen öffentlichen Interesse, UBI-Büro, Bonn (September 2023), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Regulierte_Unternehmen/UBI/Flyer.pdf?__blob=publicationFile&v=5 (zuletzt abgerufen am 15.11.2023).

Ausnahmen: § 8f ist gemäß § 8d Abs. 1a nicht auf Kleinstunternehmen und kleine Unternehmen anzuwenden, deren Definition sich nach der Empfehlung 2003/361/EC der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36) richtet.

3. Meldepflichten und Ausnahmen für Anbieter digitaler Dienste

Für Anbieter digitaler Dienste gemäß § 2 Abs. 12 BSIG geltende Meldepflichten für Sicherheitsvorfälle sind in § 8c Abs. 3 festgelegt. Dennoch gelten für diese Unternehmen bereits jetzt zahlreiche Ausnahmen, die beispielsweise vom (geografischen) Sitz des Unternehmens abhängen.

Um welche digitalen Dienste es sich im Sinne des BSIG handelt, geht aus § 2 Abs. 11 hervor: Relevant sind Onlinemarktplätze, Onlinesuchmaschinen und Cloud-Computing-Dienste.

Gemäß § 8c Abs. 3 haben Anbieter digitaler Dienste jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem BSI zu melden. Darüber, ob ein Sicherheitsvorfall *„erhebliche Auswirkungen"* hat, wird anhand der folgenden Kriterien entschieden:
- die Zahl der vom Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,
- die Dauer des Sicherheitsvorfalls,
- das vom Sicherheitsvorfall betroffene geografische Gebiet,
- das Ausmaß der Unterbrechung der Bereitstellung des Dienstes und
- das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls gemessen an den oben genannten Parametern zu bewerten. Gemäß § 8d Abs. 4 BSIG gilt § 8c Abs. 3 über die Meldepflichten nicht für Anbieter, *„die ihren Hauptsitz in einem anderen Mitgliedstaat der Europäischen Union haben"* oder *„die, soweit sie nicht in einem Mitgliedstaat der Europäischen Union niedergelassen sind, einen Vertreter in einem anderen Mitgliedstaat der Europäischen Union benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden"*. Des Weiteren gilt § 8c Abs. 1 bis 3 nicht für Kleinstunternehmen und kleine Unternehmen.

Die Inhalte der Meldung an das BSI richten sich nach § 8b Abs. 4 BSIG und umfassen:
- Angaben zur Störung,
- zu möglichen grenzübergreifenden Auswirkungen sowie
- zu den technischen Rahmenbedingungen,
- insbesondere der vermuteten oder tatsächlichen Ursache,
- der betroffenen Informationstechnik,
- der Art der betroffenen Einrichtung oder Anlage sowie
- zur erbrachten kritischen Dienstleistung und
- zu den Auswirkungen der Störung auf diese Dienstleistung.

4. Ausnahmen und anderweitige Vorschriften: TKG & Co.

Ausnahmen, bei denen Meldepflichten nicht anzuwenden sind, definiert § 8d Abs. 3 BSIG. Darunter fallen unter anderem KRITIS-Betreiber, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, Betreiber von Energieversorgungsnetzen oder -anlagen, Genehmigungsinhaber nach Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz – AtG) etc.

Konkret sind § 8b Abs. 4 und 4a BSIG nicht anzuwenden auf:
- Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen (Nr. 1),
- Betreiber von Energieversorgungsnetzen oder Energieanlagen, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes (EnWG) unterliegen (Nr. 2),
- die Gesellschaft für Telematik nach § 306 Abs. 1 S. 3 des Fünften Buchs Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Abs. 6 und § 325 des Fünften Buchs Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 327 Abs. 2 bis 5 des Fünften Buchs Sozialgesetzbuch bestätigte Anwendungen nutzen (Nr. 3),
- Genehmigungsinhaber nach § 7 Abs. 1 des Atomgesetzes (AtG) für den Geltungsbereich der Genehmigung (Nr. 4) sowie sonstige Betreiber Kritischer Infrastrukturen, die aufgrund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Abs. 4 vergleichbar oder weitergehend sind (Nr. 5).

Wer annimmt, dass Betreiber öffentlicher Telekommunikationsnetze oder Erbringer öffentlich zugänglicher Telekommunikationsdienste durch die Ausnahmeregelung im BSIG von den Meldepflichten befreit wären, liegt falsch. Vielmehr besteht die Notwendigkeit, in weiteren Gesetzen oder Rechtsvorschriften spezielle Anforderungen und Meldepflichten für die oben genannten Ausnahmen zu eruieren. Beispielsweise werden Meldepflichten für IT- und Telekommunikationsunternehmen im Telekommunikationsgesetz (TKG) festgelegt. Für die Energiewirtschaft gelten die Bestimmungen des EnWG. Die Verpflichtung zur Meldung von IT-Störungen an das BSI betrifft nicht nur Betreiber von Energieversorgungsnetzen im Sinne der BSI-KritisV, sondern alle Energieversorgungsnetzbetreiber. Im Hinblick auf Zahlungsdienstleister führte beispielsweise das Bundesamt für Finanzaufsicht (BaFin) im März 2022 mit einem Rundschreiben Meldepflichten für *„schwerwiegende Zahlungssicherheitsvorfälle“* ein.[58]

Für die Telekommunikationsunternehmen bestehende Meldepflichten gehen auf das sogenannte Telecom Package aus dem Jahr 2011 zurück, das die Europäische Agentur für Netz- und Informationssicherheit (ENISA, European Network and Information Security Agency) dazu verpflichtete, jährlich einen Bericht über die Sicherheitslage auf Grundlage des Article 13a der Framework Directive (2009/140/EC) zu erstellen und den Aufsichtsbehörden der Mitgliedstaaten der ENISA Sicherheitsvorfälle mit *„significant impact on the operation of services, i. e. outages of the electronic communication networks and/or services“* zu melden.[59] In § 168 Abs. 7 des am 1. Dezember 2021 in Kraft getretenen TKG wird dementsprechend festgehalten, dass die Bundesnetzagentur (BNetzA) der Europäischen Kommission, der European Union Agency for Cybersecurity (ENISA) und dem BSI *„einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen“* vorlegt.

Mit der Novellierung des ITSiG infolge der Umsetzung der NIS-RL wurde in § 168 TKG (früher: § 109 Abs. 5 TKG) für Betreiber öffentlicher Telekommunikationsnetze oder Anbieter öffentlich zugänglicher Telekommunikationsdienste die gesetzliche Verpflichtung festgelegt, Sicherheitsvorfälle mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste unverzüglich sowohl dem BSI als auch der Bundesnetzagentur (BNetzA) zu melden.[60]

Bei der Entscheidung, ob es sich um einen Sicherheitsvorfall „mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste“ handelt, sollen den Betreibern und/oder Anbietern gemäß § 168 Abs. 2 TKG die folgenden fünf Kriterien helfen:
- die Zahl der vom Sicherheitsvorfall betroffenen Nutzer
- die Dauer des Sicherheitsvorfalls
- die geografische Ausdehnung des vom Sicherheitsvorfall betroffenen Gebiets
- das Ausmaß der Beeinträchtigung des Telekommunikationsnetzes oder des Diensts
- das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Eine Meldung muss auch nach § 168 TKG unverzüglich erfolgen und die folgenden Angaben umfassen:
- Angaben zum Sicherheitsvorfall
- Angaben zu den Kriterien nach Abs. 2
- Angaben zu den betroffenen Systemen
- Angaben zur vermuteten oder tatsächlichen Ursache.

Für die Meldung der Sicherheitsvorfälle stellen das BSI sowie die BNetzA verschiedene Möglichkeiten zur Auswahl. Betreiber öffentlicher Telekommunikationsnetze oder Erbringer öffentlich zugänglicher Telekommunikationsdienste, die Betreiber Kritischer Infrastrukturen im Sinne des BSI-KritisV sind, können, nach vorheriger Registrierung und Benennung der Kontaktstelle, Sicherheitsvorfälle über das Mel-

58 BaFin, 2022, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2022/rs_03_2022_schwerwiegender_Zahlungssicherheitsvorfaelle.html (zuletzt abgerufen am 4.12.2023).

59 Vgl. ENISA, 2021, Telecom Security Incidents 2021, 27.07.2022, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021 (zuletzt abgerufen am 4.12.2023).

60 Vgl. BNetzA, 2023, Mitteilung Sicherheitsvorfall, Saarbrücken, https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/MitteilungSicherheitvorfall/start.html sowie BSI, n. d., Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz, https://www.bsi.bund.de/dok/kritis-faq-meldepflicht (zuletzt abgerufen am 4.12.2023).

de- und Informationsportal des BSI (MIS)[61] einreichen. Die BNetzA stellt den Unternehmen das Formular *„Mitteilung eines Sicherheitsvorfalls nach § 168 Telekommunikationsgesetz (TKG)“*[62] zur Verfügung. Beide Behörden bieten zudem die Möglichkeit einer verschlüsselten, vertraulichen Kommunikation via E-Mail, indem sie ihre öffentlichen PGP-Schlüssel als Textdatei zum Download bereitstellen.[63] Ähnlich wie das BSI stellt die BNetzA Umsetzungshilfen zu den Meldepflichten zur Verfügung, aktuell mit dem *„Meldekonzept für die Mitteilung von beträchtlichen Sicherheitsvorfällen nach § 168 TKG“* vom 28. Februar 2022.[64]

VII. Meldepflichten für Vorfälle und Störungen – Ausblick

Es wird erwartet, dass mit der Umsetzung der NIS2-Richtlinie ins nationale Gesetz mit dem NIS2UmsuCG sowohl die Kategorisierung Kritischer Infrastrukturen als auch die Sektoren neu systematisiert werden. Darüber hinaus sollte ein zweistufiges Meldesystem für Sicherheitsvorfälle nach dem Vorbild der DSGVO eingeführt werden. Mit dem Referentenentwurf des KRITIS-DachG vom 17. Juli 2023 sollte auch die Rolle des BSI als zentrale Meldestelle für Vorfälle aufgeweicht und um einen weiteren Akteur – das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) – ergänzt werden.[65]

1. KRITIS-Dachgesetz

Während § 8b BSIG das BSI als zentrale Meldestelle für KRITIS-Betreiber und § 4 BSIG das BSI als zentrale Meldestelle für Bundesbehörden sowie § 4b BSIG als zentrale allgemeine Meldestelle für Sicherheit in der IT festlegen, werden die Zuständigkeiten im Referentenentwurf des KRITIS-DachG vom 17. Juli 2023 anders geregelt: In § 3 Abs. 1 KRITIS-DachG-E wird als nationale zuständige Behörde für die Resilienz kritischer Anlagen das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) festgeschrieben. Das BSI und die BNetzA übermitteln gemäß § 3 Abs. 2 *„dem BBK die für seine Aufgabenerfüllung erforderlichen Informationen hinsichtlich IT-Sicherheitsrisiken, -bedrohungen, -vorfällen, nicht IT-sicherheitsbezogenen Risiken, Bedrohungen und Vorfällen, die kritische Anlagen betreffen“*. Gemäß § 3 Abs. 2 übermittelt zudem eine weitere Aufsichtsbehörde, die BaFin, *„an das BBK die für dessen Aufgabenerfüllung erforderlichen Informationen“*.

Des Weiteren soll das *„Meldewesen für Störungen“* nach § 12 KRITIS-DachG-E neu geordnet und um eine *„gemeinsame Meldestelle“* erweitert werden.

2. Critical Entities Resilience / Umsetzung der NIS2-Richtlinie

Die NIS2-Richtlinie der EU aus dem Jahr 2022 sollte mit dem NIS2UmsuCG bis zum 17. Oktober 2024 ins nationale Gesetz überführt werden und gilt europaweit ab dem Folgetag, dem 18. Oktober 2024. Die Richtlinie ist mindestharmonisierend, das heißt, dass Mitgliedstaaten schärfere Gesetze und über die Anforderungen von NIS2 hinausgehende Regulierungen erlassen können.[66] Wesentliche Änderungen der NIS2-RL betreffen die Gruppierung der Sektoren in zwei übergeordnete Bereiche: in die Sektoren mit hoher Kritikalität und in die sonstigen kritischen Sektoren. Die NIS2-RL reguliert zudem wesentlich detaillierter die Einrichtungen bezüglich der Größe und/oder Schwellenwerte und unterscheidet auf Grundlage von Beschäftigtenzahl sowie Jahresumsatz zwischen wesentlichen sowie wichtigen Einrichtungen.

Meldepflichten für Stör- und Sicherheitsvorfälle sollen im NIS2UmsuCG angelehnt an die DSGVO organisiert werden und dreistufig erfolgen (vgl. § 31 BSIG n. F.): *„Die bislang einstufige Meldepflicht bei Vorfällen wird durch das dreistufige Melderegime der NIS-2-Richtlinie ersetzt. Dabei soll der bürokratische Aufwand für die Einrichtungen im Rahmen des Umsetzungsspielraums minimiert werden“*,[67] heißt es im Referentenentwurf von April 2023. Konkret sollte mit § 31 zu den Meldepflichten festgelegt werden, dass besonders wichtige sowie wichtige Einrichtungen dem BSI *„über eine vom Bundesamt im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Meldemöglichkeit“*, erstens, *„unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall“* eine Erstmeldung einreichen,[68] zweitens *„unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über den Sicherheitsvorfall“* machen und, drit-

61 Abrufbar unter: https://mip2.bsi.bund.de/ (zuletzt abgerufen am 4.12.2023).

62 Abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/mitteilungeinersicherheitsverletzung/EntwurfMeldeformular168TKG.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 4.12.2023).

63 BNetzA, 2023, Mitteilung Sicherheitsvorfall, Saarbrücken, https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/MitteilungSicherheitvorfall/start.html sowie BSI, n. d., Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz, https://www.bsi.bund.de/dok/kritis-faq-meldepflicht (zuletzt abgerufen am 4.12.2023).

64 BNetzA, 2022, „Meldekonzept für die Mitteilung von beträchtlichen Sicherheitsvorfällen nach § 168 TKG“ (Entwurf), 28.02.2022, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/mitteilungeinersicherheitsverletzung/EntwurfMeldekonzept168TKG.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 4.12.2023).

65 Gesellschaft für Informatik (GI), 2023, GI-Stellungnahme zum KRITIS-Dachgesetz: Ein stärkeres BSI statt undurchsichtiger neuer Strukturen, 24.08.2023, https://gi.de/meldung/gi-stellungnahme-zum-kritis-dachgesetz-ein-staerkeres-bsi-statt-undurchsichtiger-neuer-strukturen (zuletzt abgerufen am 4.12.2023).

66 Deutscher Bundestag, 2015, Bundesregierung legt IT-Sicherheitsgesetz vor, https://www.bundestag.de/webarchiv/textarchiv/2015/kw12_ak_it_sicherheitsgesetz-364984 (zuletzt abgerufen am 4.12.2023).

67 BMI, 2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG, Referentenentwurf (Bearbeitungsstand 03.04.2023), S. 2.

68 BMI, 2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG, Referentenentwurf (Bearbeitungsstand 03.04.2023), S. 103.

tens, *„spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls“* eine Abschlussmeldung erstatten.[69]

Die (Abschluss-)Meldung sollte nach dem aktuellen Stand des NIS2UmsuCG die folgenden Aspekte umfassen:[70]

- eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen,
- Angaben zur Art der Bedrohung bzw. der zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat,
- Angaben zu den getroffenen und laufenden Abhilfemaßnahmen,
- gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

Betreiber kritischer Anlagen sollten, wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die von ihnen betriebene kritische Anlage hat oder haben könnte, zusätzlich dazu verpflichtet werden, Angaben zur Art der betroffenen Anlage, zur kritischen Dienstleistung und zu den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung zu machen. Eine Meldung sollte sich auf wesentliche bzw. erhebliche Sicherheitsvorfälle beziehen und (voraussichtlich) an das BSI und BBK erfolgen. Ausnahmen werden im aktuellen Entwurf weiterhin vorgesehen, unter anderem für Betreiber öffentlicher Telekommunikationsdienste oder Betreiber von Diensten der Telematikinfrastruktur,[71] ähnlich den Ausnahmen in § 8d Abs. 3 Nr. 1 und 3 des aktuell geltenden BSIG.

VIII. Relevante Geldbußen und Sanktionen nach dem BSIG

In § 14 BSIG über die Bußgeldvorschriften wird in Abs. 2 Nr. 7 festgelegt, dass jemand, der *„vorsätzlich oder fahrlässig“* entgegen § 8b Abs. 4 Satz 1 (Meldepflichten für KRITIS-Betreiber), § 8c Abs. 3 Satz 1 (Meldepflichten für Anbieter digitaler Dienste), § 8f Abs. 7 Satz 1 oder Abs. 8 Satz 1 (Meldepflichten für UBI) *„eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht“*, ordnungswidrig handelt.

§ 14 Abs. 5 bestimmt die Höhe der Bußgelder je nach Ordnungswidrigkeit und bestimmt unter anderem nach dem Vorbild der DSGVO, dass bestimmte Ordnungswidrigkeiten *„mit einer Geldbuße bis zu zwei Millionen Euro“* sowie *„mit einer Geldbuße bis zu einer Million Euro geahndet werden“* können. Dies trifft jedoch nicht auf die Verletzungen der Meldepflichten zu. Hier gilt lediglich: *„Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 […] Nummer 5 und 7 bis 11 […] mit einer Geldbuße bis zu fünfhunderttausend Euro“* geahndet werden.

IX. Zusammenfassung

Zusammenfassend lässt sich feststellen, dass Meldepflichten zu den Sicherheitsvorfällen von steigender Komplexität geprägt sind. Die wesentliche Entscheidung für die Unternehmen oder Organisationen liegt in der Festlegung der Kriterien und anschließenden Prüfung, ob man – ganz oder ggf. Teile des Unternehmens – von der Meldepflicht betroffen ist. Dazu gehören auch die Identifizierung relevanter Gesetze und Verordnungen sowie die regelmäßige Überprüfung, ob die Schwellenwerte (nicht) überschritten wurden. Je nach Ergebnis müssen auch Rundschreiben oder weitere gesetzesähnliche, von den Aufsichtsbehörden erlassene Normen berücksichtigt werden. Inzwischen bieten externe Dritte den Unternehmen Unterstützung bei der Auswertung und Aufstellung relevanter Kriterien an.

Soweit das „Ob“ und „an wen“ geklärt ist, ist es ratsam, Meldeprozesse i. S. v. Ablauforganisation für Sicherheitsvorfälle und/oder Datenpannen aufzusetzen, auf die man im Stör- oder Notfall zurückgreifen kann. Auch, wenn die Inhalte der Meldungen sich oft nur im Detail unterscheiden, so sind es wichtige Details, die zu Rückfragen, Nachfragen oder gar einer, aus der Perspektive der Aufsichtsbehörden, unvollständigen Meldung führen können. Eine „One fits all“-Lösung ist aktuell nicht in Sicht. In den Meldeprozessen sollte daher detailliert festgehalten werden, welche Informationen zu welchem Zeitpunkt an die Aufsicht (ungefragt, aber verschlüsselt) weitergegeben werden müssen.

Was die Melde- und Benachrichtigungspflichten nach DSGVO angeht, so hat sich seit Einführung der Art. 33–34 DSGVO eine wesentliche Änderung ergeben: Mit der neuen Rechtsprechung des EuGH[72] dürfte sich die Einstufung des Risikos in verschiedene Erheblichkeitsschwellen erledigt haben. Das bedeutet für die Risikobewertung, dass nur noch unterschieden werden muss, ob kein Risiko oder ob ein Risiko besteht, ohne das Risiko noch zusätzlich in verschiedene Stufen zu unterteilen (z. B. geringes Risiko).

X. Fazit

Bei einer Neuregulierung der Meldepflichten für Sicherheitsvorfälle, wie es im NIS2UmsuCG oder im KRITIS-DachG angedacht ist, muss berücksichtigt werden, dass die Umsetzung von Meldeprozessen, die Etablierung einer geeigneten Aufbau- und Ablauforganisation, die Freistellung kompetenter Ressourcen, die Definition der Zuständigkeiten und viele weitere Aspekte einen nicht unerheblichen Aufwand für die betroffenen Organisationen bedeuten. Des Weiteren bestehen heutzutage für alle Organisationen Meldepflichten für sogenannte Datenpannen bzw. Data-Breaches gemäß DSGVO, für die ebenfalls relevante Prozesse sowie Verfah-

69 BMI, 2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG, Referentenentwurf (Bearbeitungsstand 03.04.2023), S. 104.

70 BMI, 2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG, Referentenentwurf (Bearbeitungsstand 03.04.2023), S. 104–105.

71 BMI, 2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG, Referentenentwurf (Bearbeitungsstand 03.04.2023), S. 94.

72 EuGH, Urt. v. 04.05.2023, Österreichische Post (Préjudice moral lié au traitement de données personnelles), C-300/21, ECLI:EU:C:2023:370.

ren zur Risikoermittlung und gegebenenfalls Meldung an die zuständigen Aufsichtsbehörden etabliert sind.

Nicht zuletzt wegen der Annäherung der Anforderungen an die Umsetzung von Meldepflichten zwischen NIS2 und DSGVO wäre ein integrierter Ansatz für meldepflichtige KRITIS-Betreiber, wesentliche oder wichtige Einrichtungen effektiver, bürokratiemindernd und schließlich auch effizienter.[73] Synergien entstehen insbesondere dort, wo es darum geht, Fristen besser einhalten zu können, auch wenn die Inhalte der Meldungen nach DSGVO oder NIS2 zwar vergleichbar, aber nicht identisch sind.

Für betroffene Unternehmen empfiehlt sich die Entwicklung und Bereitstellung eines Meldekonzepts, das sowohl Meldepflichten für Datenpannen als auch Sicherheitsvorfälle umfasst, um die Fristen effektiver einhalten zu können, und das gemeinsame Prozesse sowie Verfahren zur Meldung gemäß BSIG bzw. NIS2 und DSGVO definiert.[74] In diesem Zusammenhang spielt es eine große Rolle, dass das Meldekonzept, ob nun als Bestandteil des Notfallmanagements, des Informationssicherheitsmanagements (ISMS), des Krisenmanagements, der Verfahren zum „Incident Handling“ oder zum Anschluss an die Systeme zur Angriffserkennung (SzA), nicht nur auf einem internen oder externen Laufwerk, im Intranet oder „irgendwo im Netz“ liegt, sondern auch stets aktuell vor Ort in einem Ordner abgelegt wird, in dem sich auch die Kontaktdaten für den Notfall befinden. Infolgedessen kann darauf auch dann zugegriffen werden, wenn sich eine *„erhebliche (IT-)Störung“* ereignet.

73 Vgl. Gesellschaft für Informatik (GI), 2023, GI-Stellungnahme zum KRITIS-Dachgesetz: Ein stärkeres BSI statt undurchsichtiger neuer Strukturen, 24.08.2023.

74 Vgl. Sowa, PinG 2019, 213 ff.