MASTER THESIS | MASTER'S THESIS

Titel | Title

Die Harmonisierung von Compliance und Security im digitalen Zeitalter: Eine Analyse der DSGVO sowie NIS-2-RL

verfasst von | submitted by

Emrecan Ceyhan B.Sc.

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht (LL.M.)
Betreut von | Supervisor:	ao. Univ.-Prof. Mag. Dr. Siegfried Fina

Abstract (Deutsch)
Die zunehmende Bedrohungslage im digitalen Zeitalter verdeutlicht, dass die Verzahnung von Compliance- und Sicherheitsanforderungen für Unternehmen und öffentliche Einrichtungen von zentraler Bedeutung ist. Die Europäische Union hat mit der Datenschutz-Grundverordnung (DSGVO) und der NIS-2-Richtlinie zwei wesentliche Regulierungsinstrumente geschaffen, die sowohl den Schutz personenbezogener Daten als auch die Sicherheit von Netz- und Informationssystemen gewährleisten sollen. Ziel dieser Arbeit ist es, die Harmonisierungswirkung beider Rechtsakte zu untersuchen und zu bewerten, inwieweit sie ein kohärentes Sicherheitsmanagement ermöglichen.
Ausgehend von zwei Forschungsfragen – erstens, welches Sicherheitsmanagement die beiden Regelungen explizit verlangen und wie deren Angemessenheit zu beurteilen ist, sowie zweitens, welche Synergien und Spannungsfelder zwischen den Vorgaben bestehen – erfolgt eine systematische Analyse.
Die Untersuchung zeigt, dass die DSGVO ein vielschichtiges Sicherheitsmanagement auf Grundlage normativer Prinzipien, technischer und organisatorischer Maßnahmen sowie exekutiver Pflichten etabliert, dessen flexible Ausgestaltung zugleich Interpretationsspielräume eröffnet. Die NIS-2-Richtlinie hingegen erweitert den Fokus auf sektorspezifische und organisatorische Dimensionen, insbesondere durch die Verankerung von Governance-Verantwortlichkeiten auf Leitungsebene, einen verbindlichen Maßnahmenkatalog und gestufte Berichtspflichten.
Die vergleichende Analyse verdeutlicht zahlreiche Schnittmengen, etwa bei den risikobasierten Anforderungen, der Orientierung an internationalen Standards wie ISO/IEC 27001 oder der institutionellen Verankerung von Rechenschaftspflichten. Gleichzeitig treten Divergenzen zutage, insbesondere hinsichtlich der Schutzlogik (personenbezogene Daten versus systemische Resilienz), der Schwellenwerte und der Meldepflichten. Die Arbeit kommt zu dem Ergebnis, dass ein integriertes Sicherheits- und Compliance-Management erforderlich ist, um die Synergiepotenziale beider Regime auszuschöpfen und Konfliktlinien wirksam zu adressieren.

Abstract (Englisch)

The increasing threat landscape in the digital age highlights the central importance of aligning compliance and security requirements for companies and public institutions. With the General Data Protection Regulation (GDPR) and the NIS 2 Directive, the European Union has established two key regulatory instruments aimed at safeguarding both personal data and the security of network and information systems. This thesis examines the harmonization effects of these legal frameworks and assesses the extent to which they enable a coherent security management approach.

Building on two research questions – first, what type of security management is explicitly required by the two regulations and how its adequacy can be evaluated, and second, which synergies and potential tensions exist between their provisions – a systematic analysis is conducted. The findings reveal that the GDPR establishes a multilayered security management system based on normative principles, technical and organizational measures, as well as executive obligations, while its flexible design also creates interpretive uncertainties. By contrast, the NIS 2 Directive expands the focus to sector-specific and organizational dimensions, particularly by embedding governance responsibilities at the management level, introducing a binding catalogue of measures, and establishing staged reporting obligations. The comparative analysis demonstrates significant overlaps, for instance in the risk-based approach, the reference to international standards such as ISO/IEC 27001, and the institutional anchoring of accountability obligations. At the same time, divergences become apparent, particularly regarding the underlying protection logic (personal data versus systemic resilience), applicable thresholds, and reporting duties. The thesis concludes that an integrated security and compliance management approach is essential to leverage the synergies of both regimes and to effectively address existing conflicts.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AEUV – Vertrag über die Arbeitsweise der Europäischen Union

Art. – Artikel

BSI – Bundesamt für Sicherheit in der Informationstechnik

BSIG – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik

BfDI – Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

CNIL – Commission Nationale de l'Informatique et des Libertés (französische Datenschutzaufsicht)

CRM – Customer Relationship Management

DSB – Datenschutzbeauftragter

DSFA – Datenschutz-Folgenabschätzung

DSGVO – Datenschutz-Grundverordnung

EDSA – Europäischer Datenschutzausschuss

EU – Europäische Union

GBP – Britisches Pfund Sterling

GRCh – Charta der Grundrechte der Europäischen Union

ICO – Information Commissioner's Office (britische Datenschutzaufsicht)

ISB – Informationssicherheitsbeauftragter

ISO – International Organization for Standardization

IT – Informationstechnologie

KI – Künstliche Intelligenz

KMU – Kleine und mittlere Unternehmen

NIS-2-RL – NIS-2-Richtlinie (Nachfolger der NIS-Richtlinie)

NIS-RL – Richtlinie über Maßnahmen zur Gewährleistung einer hohen Netz- und Informationssicherheit

OLG – Oberlandesgericht

PDCA – Plan-Do-Check-Act

RL – Richtlinie

SaaS – Software as a Service

TOM – Technische und organisatorische Maßnahmen

USD – United States Dollar

VVT – Verzeichnis von Verarbeitungstätigkeiten

A. Security und Compliance im digitalen Zeitalter

I. Einführung in die Bedrohungslage

In Anbetracht der zunehmenden Bedrohungslage im digitalen Zeitalter ist das Ereignis eines Cyberangriffs längst keine hypothetische Annahme mehr, sondern eine zeitlich absehbare Wahrscheinlichkeit. Diese unvermeidbare Realität macht die Implementierung effektiver Sicherheitsmaßnahmen zu einer zentralen Herausforderung für betroffene Einrichtungen. Der Bericht des Bundesamts für Sicherheit in der Informationstechnik (2024) kristallisiert den deutlichen Anstieg von Cyberangriffen heraus, was die zunehmende Bedrohungslage für Unternehmen verdeutlicht. DDoS-Angriffe verdoppelten sich zum Vorjahr, Angriffe auf öffentliche Cloud-Dienste führten zu eingeschränkten Schutzzielen der Informationssicherheit und Ransomware bedrohte die Betriebsfähigkeit von Großunternehmen sowie KMU.[1] Die Unerlässlichkeit adäquater Sicherheitsmaßnahmen wurde am 19. Juli 2024 erneut eindrucksvoll unter Beweis gestellt, als ein fehlerhaftes Update der *CrowdStrike-Software* weltweit Ausfälle bei über 8,5 Millionen Windows-Geräten verursachte.[2] Dieser Vorfall verdeutlicht eindrucksvoll, wie entscheidend der Schutz von Unternehmenswerten[3] ist – insbesondere angesichts der zunehmenden Bedrohung durch Cyberangriffe. Diese Assets sind für Einrichtungen unabdingbar, da sie nicht nur betriebliche Effizienzen fördern, sondern auch essenzielle Informationsvorteile bieten.
Der technologische Fortschritt gleicht damit einem zweischneidigen Schwert: Auf der einen Seite ermöglicht er Hebel für Effizienzen und schafft neue Möglichkeiten für Unternehmen, wettbewerbsfähig zu bleiben. Auf der anderen Seite wird der Raum für Risiken eröffnet, da jedes neue System, jede Vernetzung und jede Digitalisierung neue potenzielle Schwachstellen bergen, die von Cyberkriminellen ausgenutzt werden könnten.[4]

II. Ziel der Ausarbeitung

Die Europäische Union hat die Risiken der fortschreitenden Digitalisierung früh erkannt und kontinuierlich Maßnahmen ergriffen, um ein Gleichgewicht zwischen Innovationsförderung und regulatorischer Stabilität herzustellen.

---

[1] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2024, S. 9.
[2] *Hötzel/Völkl*, BC 2024, 402 (402).
[3] Damit sind etwaige schützenswerte Vermögenswerte des Unternehmens gemeint, im Sinne dieser Ausarbeitung unter anderem: Personenbezogene Daten, Applikationen, Software und weitere Informationssysteme. So definiert die Normenfamilie der ISO 2700x Schutzziele der Informationssicherheit, um die Verfügbarkeit, Vertraulichkeit sowie Integrität dieser Assets zu gewährleisten. In der weiteren Ausarbeitung werden die Schutzmaßnahmen in den einzelnen Regulierungsblöcken ausgiebig analysiert. Vgl. *Votteler*, MMR 2023, 403 (403).
[4] Im Ergebnis ebenso: *Schmidl*, Corporate Compliance, 4. Auflage 2024, Rn. 2.

Schon 1995 wurde die Datenschutzrichtlinie erlassen, die seinerseits bereits durch die Datenschutzkonvention Nr. 108 vorgezeichnet war.[5] Die umfassende Harmonisierung auf dem Feld der Datenverarbeitung mit Personenbezug wurde mit der DSGVO intendiert. Zum unionsweit harmonisierten Schutz kritischer Infrastrukturen und digitaler Dienste verabschiedete die EU 2016 die NIS-RL, die durch die erweiterte NIS-2-RL im Januar 2023 ersetzt wurde.[6]

Die DSGVO und die NIS-2-Richtlinie spielen folglich eine zentrale Rolle bei der Sicherstellung des Umgangs mit jenen Assets. Für die Adressaten der zuvor genannten Regulierungen ist es daher von immenser Wichtigkeit, einen Spagat zwischen Compliance-Anforderungen und Sicherheitsmaßnahmen zu finden, um die digitale Transformation erfolgreich zu realisieren und das Vertrauen von Stakeholdern trotz der zunehmenden Bedrohungslage zu gewährleisten. Ausgehend von der zentralen Rolle der DSGVO und der NIS-2-Richtlinie, fokussiert sich diese Masterthesis auf die Harmonisierungswirkung der Regulierungsblöcke. Dabei wird ein Asset-basierter Ansatz verfolgt, der den roten Faden dieser Arbeit definiert: Der Fokus liegt dabei in der Abhandlung der geforderten Sicherheitsmaßnahmen zu Gunsten der schützenswerten Assets im Sinne der beiden Regulierungen. Mit dem weiten Begriff des Sicherheitsmanagements ist die Organisation, Umsetzung sowie Planung von Maßnahmen gemeint, die zur Aufrechterhaltung der IT-Sicherheitsziele dienen.[7]

Im Zuge dessen werden zwei zentrale Forschungsfragen adressiert: Erstens, welches Sicherheitsmanagement von den zwei Regulierungen explizit gefordert wird und wie angemessen dieses ist und zweitens, welche Synergien und potenziellen Spannungsfelder zwischen den Vorgaben dieser Regulierungen bestehen. Ziel ist es, ein fundiertes Verständnis für die Interdependenzen und Konfliktlinien herauszuarbeiten und adäquat zu bewerten.

B. Die Datenschutzgrundverordnung im Sicherheitsmanagement

Die DSGVO schützt personenbezogene Daten, sofern sie automatisiert verarbeitet oder manuell in einem Dateisystem gespeichert werden, unabhängig davon, ob die Verarbeitung durch öffentliche oder private Stellen erfolgt.[8]

Mithin wird der Schutz personenbezogener Daten explizit in den Mittelpunkt gestellt. Dabei verweisen die Erwägungsgründe der DSGVO primär auf Art. 8 GRCh als grundrechtliche Verankerung des Datenschutzes und ergänzend auf Art. 16 AEUV, der diesen Schutz

[5] *Helfrich*, Handbuch Multimedia-Recht, 62. EL Juni 2024, Rn. 19.
[6] *Kipker/Birreck/Niewöhner/Schnorr,* MMR 2023, 214 (214).
[7] *Maseberg*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, 573, Rn. 1.

[8] *Zerdick*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 3.

unionsrechtlich konkretisiert.[9] Während der grundrechtlich verankerte Schutz dieser Assets durch die DSGVO gemeinhin als umfassendes Compliance-Gerüst wahrgenommen wird, gehen auch weitreichende Sicherheitsanforderungen einher, die für ein effektives Sicherheitsmanagement von entscheidender Bedeutung sind.

Dieser Themenblock widmet sich der vertieften Analyse der Rolle der DSGVO im Kontext eines ganzheitlichen Sicherheitsmanagements. Im Zuge dessen wird elaboriert werden, inwiefern die Verordnung als rechtlicher Ankerpunkt nicht nur Compliance-Aspekte abdeckt, sondern auch grundlegende Sicherheitsmaßnahmen enthält. Ferner soll die Angemessenheit dieser Sicherheitsansätze in Anbetracht der Schutzgüter sowie Harmonisierungswirkung bewertet werden.

I. Art 5 DSGVO: Grundprinzipien der DSGVO im Lichte des Sicherheitsmanagements

1. Auslegung der Norm

Vorauszuschicken ist, dass die in Art. 5 Abs. 1 dargelegten Grundprinzipien der Datenverarbeitung als übergeordnete Strukturprinzipien fungieren, die als roter Faden für die Auslegung und Anwendung sämtlicher Einzelregelungen der DSGVO dienen und dieser als konsistenter Orientierungspunkt zugrunde liegen.[10] Die eingangs angeschnittenen Schutzziele der ISO 2700x Normenfamilie, somit auch von immenser Wichtigkeit für das Sicherheitsmanagement, werden in den Grundprinzipien der DSGVO ebenfalls aufgegriffen: Der Grundsatz der *Integrität und Vertraulichkeit* verpflichtet dazu, durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten sicherzustellen, im Sinne des Art. 5 Abs. 1 lit. f) DSGVO.[11] Für die weitere Ausarbeitung ist eine Darlegung der Semantik unabdingbar. Das Schutzziel *Integrität* zielt darauf ab, die Unversehrtheit von Daten und die korrekte Funktionsweise von Systemen zu gewährleisten. Es schützt vor unautorisierten Modifikationen und umfasst sowohl den Inhalt als auch die Metadaten (Urheber, Absender oder Erstellungszeitpunkt).[12] *Vertraulichkeit* bedeutet, Informationen vor unbefugter Weitergabe zu schützen und den Zugang zu sensiblen Daten

[9] In der Rechtsprechung des Europäischen Gerichtshofs werden Art. 7 GRCh (Recht auf Achtung des Privat- und Familienlebens) und Art. 8 GRCh (Recht auf Schutz personenbezogener Daten) regelmäßig nebeneinander angewendet. Diese parallele Heranziehung der beiden Grundrechte zeigt die enge Verbindung zwischen dem allgemeinen Schutz der Privatsphäre und dem spezifischen Schutz personenbezogener Daten. *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 6.

[10] *Pötters*, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 4.

[11] *Spindler/Dalby*, Recht der elektronischen Medien, 4. Auflage 2019, Rn. 15.

[12] *Martini*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 36.

ausschließlich autorisierten Personen zu ermöglichen.[13] Die beiden Schutzziele bilden zentrale Eckpfeiler des technischen Datenschutzes und finden ihre Umsetzung insbesondere in den Anforderungen an die Datensicherheit gemäß Art. 25 und 32 DSGVO.[14] Ferner statuieren die Art. 33 und 34 die Melde- und Benachrichtigungspflichten, sofern es zu etwaigen Datenschutzverletzungen kommen sollte.

Ein besonderes Augenmerkt gilt Art. 5 Abs. 2 DSGVO. Die Norm verankert mit dem Rechenschaftsprinzip eine zentrale Neuerung, wonach Verantwortliche die Einhaltung der Datenschutzgrundsätze jederzeit nachweisen müssen – ein Grundsatz mit erheblicher praktischer Tragweite und hohen Anforderungen an Dokumentation und Umsetzung.[15]

Die Grundprinzipien der DSGVO, wie sie in Art. 5 DSGVO formuliert sind, dürfen jedoch niemals isoliert betrachtet werden. Der oben beschriebene roten Faden zieht sich somit auch durch sämtliche Einzelvorschriften. Die weiteren Prinzipien wie *Rechtmäßigkeit*, *Transparenz*, Zweckbindung und *Datenminimierung* sind daher kumulativ zur *Integrität* und *Vertraulichkeit* zu berücksichtigen. Die Grundsäulen des Datenschutzes sind nicht als bloßes Optimierungsgebot, sondern als verbindliche Prinzipien zu verstehen, dessen Missachtung erhebliche Geldbußen nach sich ziehen kann.[16]

2. Angemessenheit im Kontext des Sicherheitsmanagements

a) Die Grundprinzipien im Sicherheitsmanagement

Die Umsetzung der *Integrität* und *Vertraulichkeit* erfordert von Verantwortlichen und Auftragsverarbeitern Weitsicht: Dabei müssen sie die Kritikalität der verarbeiteten Daten und die potenziellen Risiken und Bedrohungen bewerten, denen diese Daten und damit mittelbar auch die betroffenen Personen ausgesetzt sind. Auf Grundlage dieser Bewertung sind angemessene Technische und Organisatorische Maßnahmen zu entwickeln und kontinuierlich anzupassen. Für Verantwortliche bringt der Grundsatzkatalog umfangreiche Verpflichtungen mit sich, die deutlich über die reine Einhaltung der Datenschutzvorgaben hinausreichen. Insbesondere der Grundsatz der Rechenschaftspflicht verlangt ein systematisches Datenverarbeitungsmanagement, das auch die aktive und sorgfältige Dokumentation sämtlicher Maßnahmen zur Erfüllung der Anforderungen der DSGVO umfasst.[17]

---

[13] *Martini*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 35d, 35e-.

[14] Anders *Heberlein*, der die Einzelvorschrift der datenschutzfreundlichen Voreinstellungen gemäß Art. 25 DSGVO als Ausführung des Prinzips der Datenminimierung sieht. *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 6.

[15] *Jung*, ZD 2018, 208.

[16] *Wolff*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 49. Edition, Rn. 73.

[17] Im Ergebnis ebenso: *Franzen*, in: Franzen/Gallner/Oetker, Kommentar zum europäischen Arbeitsrecht, 5. Auflage 2024, Rn.1.

b) Angemessenheit

Der in Artikel 5 DSGVO formulierte Grundsatzkatalog bietet eine klare und kohärente Basis für das Sicherheitsmanagement von personenbezogenen Daten, was in Gänze zu begrüßen ist. Insbesondere die Aufnahme der Schutzziele *Integrität und Vertraulichkeit* in die DSGVO als Kernpunkte des Sicherheitsmanagements stärkt die Verpflichtung adäquate TOM einzuführen.[18] Diese Anforderungen fördern die Schaffung einheitlicher Auslegung – und Entwicklungsstandards. Mit der ausdrücklichen Verankerung der Schutzziele wird zugleich ein konzeptioneller Anschluss an international etablierte Standards wie die ISO/IEC 27001 geschaffen. Zwar erfolgt kein expliziter Verweis, jedoch lässt sich ein mittelbarer Bezug herstellen, da die Norm zentrale Sicherheitsziele systematisch in die fortlaufenden Compliance-Anforderungen einbettet.[19]

Kritik könnte sich jedoch auf die hohe Anforderung der Rechenschaftspflicht beziehen, die insbesondere KMU vor administrative und finanzielle Herausforderungen stellt.

II. Art. 25 DSGVO: Privacy by Design und Privacy by Default

Bereits im Rahmen der langwierigen Verhandlungen, in denen sich die EU-Organe 2015 auf den heutigen Wortlaut, der durch die Streichung des Wortes „grundsätzlich“ (Art. 25 Abs. 2 S. 1) nochmals präzisiert und restriktiver gestaltet wurde, ging die Wichtigkeit der Norm im Kontext des Sicherheitsmanagements hervor.[20] Die Prinzipien Privacy by Design und Privacy by Default verlangen, dass der Datenschutz bereits bei der Entwicklung von Prozessen und Technologien sowie durch datenschutzfreundliche Voreinstellungen gewährleistet wird, im Sinne des Art. 25 DSGVO. Diese Grundsätze stehen in enger Verbindung zu den TOM, da beide darauf abzielen, Risiken für die Rechte und Freiheiten der betroffenen Personen durch angemessene Schutzvorkehrungen zu minimieren.

Der folgende Themenblock widmet sich der Analyse beider Grundpfeiler im Kontext des Sicherheitsmanagements. Dabei wird aufgezeigt, wie diese Prinzipien zur proaktiven Integration von Datenschutz in Entwicklungsprozessen, internen Verfahren beitragen und eine datenschutzfreundliche Ausgestaltung fördern. Die spezifischen Anforderungen an TOM werden in einem späteren Abschnitt detailliert behandelt.

---

[18] Die Begriffe *Integrität* und *Vertraulichkeit* waren in der Datenschutzrichtlinie 95/46/EG nicht explizit geregelt. Ihre Aufnahme in die DSGVO war notwendig, um den Anforderungen des digitalen Zeitalters gerecht zu werden. *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 46.

[19] Hinsichtlich der Zielsetzung sowie Struktur der ISO/IEC 27001 vgl. *Conrad/Streitz*, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 385.

[20] *Paulus*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 49. Edition, Rn. 1.

1. Privacy by Design

a) Auslegung der Norm

Im Rahmen von Eigenentwicklungen ist der Verantwortliche verpflichtet, bereits in der Konzeptionsphase datenschutzrechtliche Anforderungen durch geeignete Maßnahmen zu berücksichtigen, anstatt diese nachträglich zu integrieren.[21] Ziel ist es, den Datenschutz nicht erst während des Betriebs, sondern schon bei der Gestaltung und Planung technischer Systeme und Prozesse zu verankern. Als relevanter Zeitpunkt des finalen Sicherheitskonzeptes der Datenschutzmaßnahmen kann somit die verbindliche Festlegung der jeweiligen Mittel der Datenverarbeitung angesehen werden.[22] Nutzt der Verantwortliche die Angebote von Drittanbietern oder Herstellern, muss er die Vorgaben des Art. 25 Abs. 1 bei der Lieferantenauswahl und der Erstellung des Pflichtenhefts berücksichtigen - die Festlegung der Mittel der Verarbeitung erfolgt in diesem Fall durch die Auswahlentscheidung des Dienstleisters.[23] Die Verpflichtungen aus Art. 25 DSGVO zu Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen richten sich laut Wortlaut des Artikels ausschließlich an die Verantwortlichen und erfordern bei Hinzuziehen von Auftragsverarbeitern eine adäquate Geeignetheitsprüfung und einen damit einen einhergehenden TOM-Check des Lieferanten.[24]

b) Angemessenheit im Kontext des Sicherheitsmanagements

aa) Privacy by Design im Sicherheitsmanagement

Über die praktische Umsetzung des Privacy by Design Gebots wird in der Rechtsprechung häufig geurteilt, da es eine zentrale Grundlage für die Bewertung Technischer und Organisatorischer Maßnahmen zum Schutz personenbezogener Daten darstellt. So verdeutlichen Nationale Gerichtsentscheidungen, dass die aktuelle Bedrohung durch Scraping-Vorfälle die praktische Relevanz des Gebots in der heutigen Zeit unterstreicht. Die Entscheidungen der Gerichte zeigen unterschiedliche Ansätze hinsichtlich des immateriellen Schadensersatzes bei Scraping-Vorfällen. Während das OLG Oldenburg (Az. 13 U 108/23) dem Kläger einen Schadensersatz in Höhe von 250 Euro zusprach und dabei betonte, dass die unzureichende Umsetzung von Art. 25 DSGVO sowie die daraus resultierende Befürchtung einer missbräuchlichen Datennutzung einen immateriellen Schaden darstellen, entschied das

[21] *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 17.
[22] *Nolte/Werkmeister,* in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 4.
[23] *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 17.
[24] *Klingbeil/Kohm*, MMR 2021, 3.

OLG Hamm (Az. 7 U 154/23) anders.[25] Eine weitere misslungene Technikgestaltung wäre etwa eine vom Unternehmen intern entwickelte CRM-Software, die keine Features zur datenschutzkonformen Löschung von Kundendaten anbietet, da so etwaige Grundprinzipien (Zweckbindung, Datenminimierung), nicht umgesetzt werden können.[26]

Eine erfolgreiche Umsetzung des Privacy by Design Gebots erfordert folglich eine enge interdisziplinäre Zusammenarbeit zwischen Softwareentwicklern, IT sowie Compliance. Um sicherzustellen, dass die Technikgestaltung effektiv sowie fristgerecht umgesetzt werden kann, sollten das Organigramm und die internen Datenschutzrichtlinien so gestaltet werden, dass klare Verantwortlichkeiten und Reporting-Prozesse etabliert sind. Diese Maßnahmen sind nicht nur für die Erfüllung der datenschutzrechtlichen Anforderungen essenziell, sondern bilden auch einen integralen Bestandteil des übergreifenden Sicherheitsmanagements des Verantwortlichen.

bb) Angemessenheit

Art. 25 Abs. 1 DSGVO zeichnet sich durch einen gelungenen Wortlaut aus, da er die Implementierungskosten und den Stand der Technik ausdrücklich berücksichtigt. Diese Regelung ermöglicht es Unternehmen, Datenschutzmaßnahmen in finanziell verhältnismäßiger Weise umzusetzen. Damit wird ein Ausgleich zwischen der Notwendigkeit effektiver Datenschutzmaßnahmen und den wirtschaftlichen Rahmenbedingungen geschaffen, was die praktische Umsetzbarkeit der Vorschrift fördert. Die Berücksichtigung des Stands der Technik[27] verpflichtet Verantwortliche dazu, ihre Datenschutzmaßnahmen kontinuierlich an den technologischen Fortschritt anzupassen und so langfristig ein hohes Schutzniveau für personenbezogene Daten zu gewährleisten.

2. Privacy by Default

a) Auslegung der Norm

Privacy by Default verpflichtet den Verantwortlichen, bei der Gestaltung von Produkten, Diensten und Anwendungen sicherzustellen, dass standardmäßig datenschutzfreundliche Voreinstellungen implementiert werden. Der Europäische Datenschutzausschuss definiert eine Voreinstellung im Sinne der Informatik als den bereits bestehenden oder vorausgewählten Wert

[25] *OLG Oldenburg*, GRUR-RS 2024, 12097, Rn. 35. Das *OLG Hamm* verneinte einen Schadensersatzanspruch mit der Begründung, dass der bloße Kontrollverlust über personenbezogene Daten nicht ausreiche und eine konkret-individuelle Beeinträchtigung erforderlich sei. Vergleich hierzu: *OLG Hamm*, GRUR-RS 2024,16856, Rn. 44.

[26] *Conrad/Hausen*, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 210.

[27] So definiert das BSI regelmäßig branchenspezifische Sicherheitsstandards, vgl. *BSI,* „Stand der Technik" umsetzen.

einer konfigurierbaren Einstellung, der einer Anwendungssoftware, einem Computerprogramm oder einem Gerät zugewiesen wird.[28] Ziel ist es, Systeme so zu entwickeln, dass die Erhebung, Verarbeitung und Weitergabe personenbezogener Daten auf das unbedingt erforderliche Mindestmaß begrenzt wird.[29] Nutzende sollen keine manuellen Anpassungen vornehmen müssen, um datensparsame Verarbeitungsweisen zu erreichen, vielmehr dürfen Abweichungen von diesen Voreinstellungen nur durch ein bewusstes und aktives Tun der Nutzenden ermöglicht werden, wodurch die datenminimierende Systemarchitektur als Grundprinzip erhalten bleibt.[30] Diese Anforderungen erstrecken sich auf alle Aspekte der Verarbeitung personenbezogener Daten, wie die Menge, den Umfang, die Speicherdauer sowie den Zugang zu den Daten.[31]

b) Angemessenheit im Kontext des Sicherheitsmanagements

aa) Privacy by Default im Sicherheitsmanagement

Das Sicherheitsmanagement steht im Kontext des Privacy by Default Gebots vor der Hürde, datenschutzrechtliche Vorgaben mit den wirtschaftlichen Interessen des Unternehmens in einer ausgewogenen Weise zu verbinden. Der Unionsgesetzgeber verlangt hierbei, dass Verantwortliche ihre eigenen ökonomischen Interessen dem Prinzip der Datenminimierung unterordnen und technische Voreinstellungen als Instrument des Datenschutzes einsetzen.[32] Eine primäre Nutzung der Daten zur Maximierung ökonomischer Vorteile ist unzulässig. Gleichzeitig ist dies jedoch nicht uneingeschränkt gefordert, sondern unterliegt dem Grundsatz der Verhältnismäßigkeit.[33] Auch dies bedingt eine enge Zusammenarbeit der diversen Abteilungen im Unternehmen. Der Datenschutzbeauftragte spielt hierbei eine zentrale Rolle, indem er als neutrale Instanz agiert, die sicherstellt, dass die TOM zu Gunsten der Datenminimierung implementiert werden, im Sinne seiner legaldefinierten Aufgaben des Art. 39 DSGVO. Dies kann auch bedeuten, dass er, entgegen den wirtschaftlichen Interessen des Unternehmens, Entscheidungen trifft, um die Einhaltung der gesetzlichen Datenschutzvorgaben zu gewährleisten.[34]

---

[28] *European Data Protection Board*, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, 20. Oktober 2020, S. 12.
[29] *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 25.
[30] *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 25.
[31] *Guggenberger,* Handbuch Multimedia Recht, Werkstand: 62. EL Juni 2024, Rn. 89.
[32] *Martini*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 44a.
[33] *Martini*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 44a.
[34] Die Unabhängigkeit des Datenschutzbeauftragten erstreckt sich in weitem Umfang und umfasst auch das Verhältnis zu den Aufsichtsbehörden. Als eigenständiges Organ mit Unterrichtungs-, Beratungs- und Kontrollfunktion unterliegt er keinen Weisungen und orientiert sich ausschließlich an seiner fachlichen Bewertung der datenschutzrechtlichen Vorgaben. *Scheja*, in: Tager/Gabel, DSGVO – BDSG – TTDSG, 4. Auflag 2021, Rn. 1.

bb) Angemessenheit

Art. 25 Abs. 2 DSGVO wirft bei genauer Analyse Fragen hinsichtlich der Angemessenheit und seines eigenständigen Regelungsgehalts auf. Während Abs. 1 bereits umfassend die Verpflichtung zur Technikgestaltung, darunter mitunter auch die Standardeinstellung, regelt, könnte Abs. 2 als spezielle Ausführung zu Abs. 1 interpretiert werden, wodurch die Notwendigkeit einer separaten Erwähnung infrage gestellt wird.[35] Ein zentraler Kritikpunkt betrifft den Regelungsadressaten von Art. 25 Abs. 2 DSGVO. Obwohl die Wahl der standardmäßigen Voreinstellungen erheblich das Verhalten der Nutzer beeinflussen kann, liegt diese Entscheidung typischerweise beim Hersteller der zugrunde liegenden Technologie und nicht beim Verantwortlichen. Wie eine Stimme der Literatur hervorhebt, bestimmt der Hersteller, welche Optionen standardmäßig vorgegeben werden. Dennoch adressiert Art. 25 Abs. 2 DSGVO ausschließlich die Verantwortliche Stelle und nicht den Hersteller, was eine Regelungslücke darstellen und die Effektivität des Abs. 2 beeinträchtigen könnte.[36] Dieser Position ist jedoch nicht zu folgen, da die Weitsicht der Verantwortungs-Allokationen nicht vollumfänglich berücksichtigt wird. Nach den Regelungen der DSGVO ist ein Hersteller niemals nur Hersteller im engeren Sinne, sondern agiert in Abhängigkeit von seiner Rolle entweder selbst als Verantwortlicher oder als Auftragsverarbeiter. Insbesondere bei einer gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO oder bei der Auftragsverarbeitung im Sinne des Art. 28 DSGVO bleibt der Hersteller in den Geltungsbereich der DSGVO eingebunden und unterliegt entsprechenden datenschutzrechtlichen Verpflichtungen. Die Kritik an einer vermeintlichen Regelungslücke verkennt folglich, dass die DSGVO bereits einen umfassenden Rahmen bietet, um auch Hersteller in datenschutzrechtliche Verantwortlichkeiten einzubeziehen.[37]

III. Art. 32 DSGVO: Technisch-Organisatorische-Maßnahmen (TOM)

Die Technisch-Organisatorische Maßnahmen sind das Herzstück des Sicherheitsmanagements in der DSGVO. Sie verkörpern die praktischen Anforderungen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu Gunsten der Assets zu gewährleisten und so die Grundrechte der betroffenen Personen effektiv zu schützen. Die Relevanz der TOM zeigt sich eindrücklich an der Höhe drohender Bußgelder: So kündigte das britische Information Commissioner's Office (ICO) im Jahr 2019 ein Bußgeld von 183,39 Millionen GBP gegen British Airways an –

[35] *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 9.
[36] *Herfurth/Benner-Tischler*, ZD Aktuell 2017, 05901.
[37] Vgl. Erw. 88.

aufgrund schwerwiegender Verstöße gegen datensicherheitsrechtliche Vorgaben.[38] Ein weiterer aufsehenerregender Fall betrifft *Marriott International*: Nach umfangreichen Ermittlungen kündigte das ICO im Jahr 2019 ein Bußgeld in Höhe von 99,2 Millionen GBP an.[39]

Die intendierte Höhe der Bußgelder unterstreicht, dass der Schutz personenbezogener Daten weit über theoretische Anforderungen hinausgeht. TOM stehen im Zentrum des technischen Datenschutzes und bilden die Grundlage für ein robustes Sicherheitsmanagementsystem. In dieser Masterthesis nehmen die TOM einen zentralen Teil ein, da sowohl der Regelungsgehalt als auch die weitreichenden Auswirkungen des Sicherheitsmanagements auf Unternehmen umfassend beleuchtet werden. Ziel ist es, nicht nur die gesetzeskonforme Umsetzung zu analysieren, sondern auch darzustellen, wie TOM gestaltet werden können, um den Anforderungen des digitalen Zeitalters gerecht zu werden.

1. Auslegung der Norm

Art. 32 verpflichtet Verantwortliche und Auftragsverarbeiter, geeignete TOM umzusetzen, um die Rechte und Freiheiten betroffener Personen zu schützen sowie eine missbräuchliche Verarbeitung und Nutzung der Daten wirksam zu verhindern.[40] Diese Pflicht gilt in zeitlicher Hinsicht für alle Verarbeitungsphasen und erfordert Maßnahmen, die anhand von acht Kriterien – darunter Stand der Technik, Kosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen – ein angemessenes Schutzniveau gewährleisten sollen.[41]

a) Stand der Technik

Der Europäische Datenschutzausschuss betont die Notwendigkeit, den technischen Fortschritt zu kennen, sich regelmäßig zu informieren und Maßnahmen anzupassen, um ein adäquates Sicherheitslevel gewährleisten zu können.[42] Damit kann der Stand der Technik als die am Markt verfügbare, beste Lösung zur Erreichung der gesetzlich vorgegebenen IT-Sicherheitsziele verstanden werden.[43] Die Verpflichtung, den Stand der Technik bei der Festlegung von Maßnahmen zu berücksichtigen, macht deutlich, wie eng Datenschutz und technologische

[38] *EDPB*, ICO statement: Intention to fine British Airways £183.39m under GDPR for data breach, 8. Juli 2019.
[39] *EDPB*, ICO statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, 09. Juli. 2019.
[40] *Schläger*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Rn. 4.
[41] *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 9.
[42] *European Data Protection Board*, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, 20. Oktober 2020, S. 9.
[43] *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 6.

Entwicklungen miteinander verknüpft sind. Technikstandards sind unbestimmte Rechtsbegriffe, die in unterschiedlichem Maße auf Entwicklungen in Wissenschaft und Technik Bezug nehmen – die Einbindung in Rechtsvorschriften bietet dem Gesetzgeber den Vorteil, rechtliche Normen nicht ständig an den technischen Fortschritt anpassen zu müssen.[44] Im Zuge dessen wird es für Verantwortliche und Auftragsverarbeiter unabdingbar werden, sich kontinuierlich über aktuelle Entwicklungen zu informieren, sodass Best-Practice-Lösungen etabliert werden können.
Der Stand der Technik umfasst dabei nicht nur technische, sondern auch organisatorische Aspekte, die durch regelmäßige Schulungen und Fortbildungen gefördert werden können. Unterstützung liefert unter anderem vom BSI veröffentlichte Technikstandards, die Orientierung bei der Umsetzung bieten.[45]

b) Implementierungskosten

Die Implementierungskosten sind umfassend zu berücksichtigen. Damit sind nicht nur die initialen Planungskosten, sondern auch Aufwendungen für Personal, Schulungen sowie laufende Betriebs- und Folgekosten inkludiert.[46] Die zu tragenden Kosten müssen dem Grundsatz der Verhältnismäßigkeit entsprechen und dürfen nicht unverhältnismäßig hoch im Vergleich zum angestrebten Schutzniveau sein.[47]
Die Relevanz der Implementierungskosten geht insbesondere angesichts der stetig zunehmenden Menge der personenbezogenen Daten, die im Rahmen von SaaS-Einbindungen in der globalisierten Welt gehostet werden, hervor. Die historisch[48] hohe Verbreitung solcher Einbindungen führt zu einer gesteigerten Komplexität, die zusätzlich zu den Lizenzgebühren erhebliche Konfigurationskosten für die Erfüllung von Sicherheits- und Compliance-Anforderungen nach sich zieht.[49]
Die Einbindung der Implementierungskosten im Wortlaut der Regelung verdeutlicht die interdisziplinäre Natur des Sicherheitsmanagements. Verantwortliche und Auftragsverarbeiter müssen hierbei nicht nur Maßnahmen evaluieren, sondern auch wirtschaftliche Aspekte abwägen. Übersteigen die Implementierungskosten ein vertretbares Maß, kann es strategisch

[44] *Seibel*, NJW 2013, 3000.
[45] Vgl. *BSI*, „Stand der Technik" umsetzen.
[46] *Schläger*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Rn. 13.
[47] *Piltz,* in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 20.
[48] Der globale SaaS-Markt wurde 2024 auf 266,23 Mrd. USD geschätzt und soll bis 2032 auf über 1.131 Mrd. USD anwachsen, wobei Nordamerika mit einem Anteil von 47,85 % den Markt dominiert; *Fortune Business Insights*, Saas Market Size, 21. 07. 2025.
[49] Vor jeder SaaS-Einbindung muss eine sorgfältige Überprüfung des Auftragsverarbeiters erfolgen, im Sinne des Art. 28 DSGVO. Ferner werden regelmäßig Aufwendungen in Privacy by Design sowie by Default Settings budgetiert werden müssen. Im Ergebnis ebenso: *Pietzka/Wimmer/Kühle*, IRZ 2021, 473.

sinnvoll sein, ein kalkuliertes Risiko in Anbetracht der Eintrittswahrscheinlichkeit in Kauf zu nehmen.[50] Eine enge Einbindung der Finance-Abteilung in den betroffenen Einrichtungen ist essenziell, um sowohl regulatorische Anforderungen als auch wirtschaftliche Interessen miteinander zu harmonisieren.

c) Eintrittswahrscheinlichkeit und Schwere des Risikos

Die Integration von geeigneten TOM hängt maßgeblich von der potenziellen Eintrittswahrscheinlichkeit sowie dem Schweregrad des Risikos für die Rechte und Freiheiten der Betroffenen ab. Die Wahrscheinlichkeit stellt einen geschätzten Wert dar, der angibt, wie wahrscheinlich das Eintreten eines Ereignisses ist, das zur Realisierung eines Risikos führen kann.[51] Erwägungsgrund 75 zeigt die Bandbreite möglicher Schäden: physisch, materiell und immateriell. Das Risikomanagement wird im weiteren Verlauf der Ausarbeitung detailliert elaboriert werden. An dieser Stelle sei jedoch angemerkt, dass die Implementierung der TOM grundsätzlich einen prospektiven Ansatz erfordert, sodass diese den spezifischen Anforderungen gerecht werden kann. Eine fundierte Planung ist unentbehrlich, um nachhaltige Sicherheitsmaßnahmen zu gewährleisten. Aber auch die Berücksichtigung vergangener Datenschutzvorfälle ist sinnvoll für eine kontinuierliche Optimierung von TOM. Durch eine systematische Analyse solcher Vorfälle können potenzielle Schwachstellen identifiziert und nachhaltige Verbesserungen implementiert werden.

d) Art, Umfang, Umstände und Zweck der Verarbeitung

Effektive Sicherheitsmaßnahmen verfolgen keinen Selbstzweck, sondern richten sich strikt nach dem erforderlichen Schutzniveau der spezifischen Verarbeitungsvorgänge.[52] Der Europäische Datenschutzausschuss bekräftigt insbesondere, dass der Kontext der Verarbeitung durchgängig im Einklang mit ihrer Bedeutung in anderen Bestimmungen der DSGVO (Art. 24, 32 und 35) auszulegen ist, sodass Datenschutzgrundsätze in die Technikgestaltung eingebunden werden können.[53] Daraus ergibt sich für Verantwortliche und Auftragsverarbeiter die Notwendigkeit, eine fortlaufende Status-Quo-Auflistung bestehender Datenverarbeitungsprozesse zu haben. Das gesetzlich vorgeschriebene Verzeichnis von

[50] *Schläger*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Rn. 15.
[51] *Hense*, in: Taeger/Pohle, Computerrechts-Handbuch, Werkstand: 39. EL 2024, Rn. 123
[52] *Schläger*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Rn. 20.
[53] *European Data Protection Board*, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, 20. Oktober 2020, S. 10.

Verarbeitungstätigkeiten[54] (VVT) gemäß Art. 30 DSGVO kann hierbei als zentrale Grundlage dienen, da es ohnehin der granularen Beschreibung der Verarbeitungsvorgänge dient. Die im VVT dokumentierten Informationen zu Art, Umfang, Umständen und Zwecken der Verarbeitung ermöglichen eine strukturierte Analyse und erleichtern die Ableitung passender TOM. Der Wortlaut von Art. 30 fordert zudem die Angabe der verarbeiteten Datenkategorien, wodurch zumindest mittelbar auch die Sensibilität dieser Kategorien, beispielsweise ob es sich um besondere Kategorien personenbezogener Daten handelt, ersichtlich wird, was einen weiteren Anhaltspunkt für die Festlegung effektiver Sicherheitsmaßnahmen bietet.[55]Auf diese Weise zeigt sich, dass die DSGVO Synergien zwischen Dokumentationsanforderungen und Sicherheitsvorgaben schafft, die sowohl die Rechtssicherheit als auch die praktische Umsetzung der Datensicherheit unterstützen.

2. Regelungskatalog

Art. 32 Abs. 1 Hs. 2 nennt beispielhaft, aber nicht abschließend, mögliche Maßnahmen. Verantwortliche und Auftragsverarbeiter müssen weitere Maßnahmen ergreifen, sofern diese ein angemessenes Sicherheitsniveau gewährleisten. Verantwortliche, die im Rahmen des Outsourcings und der Anwendbarkeit des Art. 28 DSGVO weitere Auftragsverarbeiter involvieren, müssen eine detaillierte Due Diligence Prüfung der TOM der Auftragsverarbeiter durchführen, um deren Geeignetheit sicherzustellen. Verfügen Auftragsverarbeiter über eine ISO/IEC 27001-Zertifizierung, kann dies die Prüfung erleichtern, da diese Zertifizierung auf bereits implementierte und ausreichende Sicherheitsmaßnahmen hinweist.[56] Es ist jedoch unerlässlich, den spezifischen Anwendungsbereich der Zertifizierung zu berücksichtigen, da dieser gut begründet eingeschränkt werden kann und somit nicht alle relevanten Maßnahmen der ISO/IEC 27001 Normfamilie abdeckt. Die Klassifizierung der Maßnahmen kann anhand verschiedener Kategorien erfolgen, beispielsweise basierend auf den IT-Sicherheitszielen (Vertraulichkeit, Integrität, Verfügbarkeit) oder ihrer Einteilung in technische, organisatorische und physische Maßnahmen.[57] Diese Ausarbeitung folgt einem hybriden Ansatz: Zunächst wird

[54] Die Gesamtheit aller Datenverarbeitungen, die einem bestimmten Zweck oder mehreren miteinander verbundenen Zwecken dienen, kann als eine Verarbeitungstätigkeit betrachtet werden. *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 2.

[55] *Feiler/Forgó* vertreten hingegen die Ansicht, dass Verzeichnisse von Verarbeitungstätigkeiten in der Praxis mit sehr unterschiedlichem Detailgrad geführt werden. Es genüge, das Verzeichnis mit einem Detailgrad zu erstellen, der dem entspricht, wie er in der mittlerweile aufgehobenen Standard- und Musterverordnung 2004 vorgesehen war. Insbesondere sei es nicht erforderlich, die einzelnen Datenkategorien den jeweiligen Verarbeitungszwecken zuzuordnen. *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 4.

[56] Vgl. *Votteler*, MMR 2023, 403 (404).

[57] Hinsichtlich des letzteren Klassifizierens: *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 10.

die Grundstruktur gemäß Anhang A der ISO/IEC 27001:2022 herangezogen, da diese eine praxisbewährte und international anerkannte Grundlage zur Implementierung effektiver Sicherheitsmaßnahmen bietet. [58] Weiterhin werden die relevantesten Maßnahmen der Literatur den entsprechenden Gewährleistungszielen der DSGVO zugeordnet, die neben den IT-Sicherheitszielen auch weitere Compliance-Anforderungen umfassen.

a) Gewährleistungsziele der DSGVO

Eine Ableitung der TOM anhand der Gewährleistungsziele erscheint sinnvoll, um die Reichweite der DSGVO als Ankerpunkt zwischen Security und Compliance darzulegen. Einige der Gewährleistungsziele wurden bereits im Rahmen dieser Ausarbeitung herausgestellt, anbei eine Kurzübersicht, die sich an dem Standard-Datenschutzmodell orientiert:

- Transparenz - Art. 5 Abs. 1 lit. a) DSVGO
- Zweckbindung – Art. 5 Abs. 1 lit. c) DSGVO
- Datenminimierung – Art. 5 Abs. 1 lit. c) DSGVO
- Richtigkeit – Art. 5 Abs. 1 lit d) DSGVO
- Speicherbegrenzung – Art. 5 Abs. 1 lit. e) DSGVO
- Integrität – Art. 5 Abs. 1 lit. f) DSGVO
- Vertraulichkeit – Art. 5 Abs. 1 lit. f) DSGVO
- Rechenschafts- und Nachweispflichten – Art. 5 Abs. 2 DSGVO
- Umsetzung der Betroffenenrechte – Art. 15 bis 22 DSGVO
- Privacy by Design und Default – Art. 25 DSGVO
- Verfügbarkeit – Art. 5 Abs. 1 lit. e) DGVO, Art. 32 Abs. 1 lit. b) DSGVO
- Belastbarkeit – Art. 32 Abs. 1 lit. b) DSGVO
- Wiederherstellbarkeit – Art. 32 Abs. 1 lit. c) DSGVO
- Behebung und Abmilderung von Datenschutzverletzungen – Art. 33 Abs. 3 lit d, Art. 34 Abs. 2 DSGVO
- Angemessene Überwachung der Verarbeitung.[59]

b) Organisatorische Maßnahmen

Verantwortliche und Auftragsverarbeiter können Datenschutz-Compliance nur durch eine ganzheitliche Strategie erreichen, die die aktive Einbindung der Mitarbeitenden voraussetzt.[60] Im Zuge dessen ist die Einführung einer unternehmensweiten Datenschutzrichtlinie

[58] Organisatorische Maßnahmen, Maßnahmen in Verbindung mit Menschen, Physische Maßnahmen und Technische Maßnahmen; *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3.
[59] *Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder*, Das Standard-Datenschutzmodell, Version 3.1, S. 15.
[60] *Rath/Kuß*, Corporate Compliance Checklisten, 5. Auflage 2022, Rn. 34.

unabdingbar, die als Grundlage für ein einheitliches Datenschutzmanagement dient. Die Genehmigung durch das Top-Management sichert ihre Verbindlichkeit und Priorität im Unternehmen.[61] Die Richtlinie regelt Gewährleistungsziele wie Transparenz, IT-Sicherheitsziele (Integrität, Verfügbarkeit, Vertraulichkeit), die rechtmäßige Abhandlung der Betroffenenrechte sowie die interne und externe Kommunikation, etwa im Rahmen von Datenschutzvorfällen. In der Unternehmensrichtlinie Datenschutz sollte zudem der Umgang mit KI-Systemen geregelt werden, einschließlich Vorgaben zur datenschutzkonformen Nutzung der Technologie.[62] Eine weitere zentrale Maßnahme ist ein Rollen- und Berechtigungskonzept *(Int*egrität, Vertraulichkeit, Privacy by Design und by Default) das definiert, welche Tätigkeiten eine Authentifizierung erfordern und welche Zugriffsrechte den jeweiligen Systembetreuern zugewiesen werden.[63] Zudem können Auswertungsmöglichkeiten definiert und Zugriffsrechte vergeben werden, um eine forensische Nachvollziehbarkeit sicherzustellen (Angemessene Überwachung der Verarbeitung). [64] Das Berechtigungskonzept kann in der oben beschriebenen unternehmensweiten Datenschutzrichtlinie integriert werden oder Teil einer weitreichenderen IT-Richtlinie werden, sodass die dazugehörigen Technischen Maßnahmen entsprechend gelistet werden können.
Die Rechenschaftspflicht erfordert, dass Verantwortliche jederzeit nachweisen müssen, dass personenbezogene Daten rechtmäßig verarbeitet werden.[65] Dies hat die Dokumentationsanforderungen erheblich verschärft und stellt eine der größten bürokratischen Hürden dar, insbesondere im Rahmen eines Datenschutzmanagementsystems[66] *(*Transparenz, Rechenschafts – und Nachweispflicht). Die praktische Umsetzung dieser Anforderungen stellt mit großer Tendenz die wichtigste Organisatorische Maßnahmen dar, da in der Umsetzung alle einzelnen Compliance-Anforderungen inkludiert werden müssen.

[61] Analog zur Maßnahme A.5.1 der ISO/IEC 27001:2022 „Informationssicherheitsrichtlinie“; *Brenner*, Praxishandbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 4. Auflage, B. 3.
[62] Datenschutzverstöße sind laut Bitkom das größte Risiko beim KI-Einsatz: 70 % aller Unternehmen und 80 % der KI-Nutzer teilen diese Ansicht. Zudem glauben 62 % der Unternehmen, dass KI-Dienste in der Cloud nicht datenschutzkonform sind. *Hilmer*, BC 2024, 351.
[63] *Holthausen*, NZA 2023, 1489 (1493). Vgl. Maßnahme A.5.10 der ISO/IEC 27001:2022 „Informationssicherheitsrichtlinie“; *Brenner*, Praxishandbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 4. Auflage, B.3. Vgl. Maßnahme „Festlegung eines Berechtigungs- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle*“*; *Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder*, Das Standard-Datenschutzmodell, Version 3.1, S. 31.
[64] Im Ergebnis ebenso: *Stolper*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Rn. 119.
[65] *Jung*, ZD 2018, 208.
[66] Ein Datenschutzmanagementsystem umfasst organisatorische Maßnahmen, die den rechtskonformen Umgang mit personenbezogenen Daten sicherstellen; *Dendorfer-Ditges*, in: Moll/Eckhoff/Reufels, Münchener Anwaltshandbuch Arbeitsrecht, Rn. 6. Auflage 2025, Rn. 409.

c) Maßnahmen in Verbindung mit Menschen

Bereits vor Abschluss eines Arbeitsvertrags kann der Arbeitgeber mögliche Risiken im Zusammenhang mit potenziellen Arbeitnehmern prüfen, um spätere Risiken zu verhindern (*Pre-Employement-Screening*).[67] Im Zuge dessen können Recherchen durchgeführt werden - solche Maßnahmen unterliegen jedoch rechtlichen Grenzen, insbesondere durch das allgemeine Persönlichkeitsrecht des Bewerbers und den Datenschutz (Behebung und Abmilderung von Datenschutzverletzungen, Rechenschaft – und Nachweispflichten).[68] Zudem gelten in Deutschland die vom BAG entwickelten Grundsätze, wonach Fragen zu personenbezogenen Daten im Bewerbungsverfahren nur zulässig sind, wenn ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers an der Informationsbeschaffung besteht.[69] Das Screenen während des Arbeitsverhältnisses kann bereits durch einfache Maßnahmen wie das Vier-Augen-Prinzip, die Vermeidung von Kompetenzkonzentrationen und Interessenkonflikten sowie die Personal-Rotation in sensiblen Bereichen umgesetzt werden.[70] Die innerbetriebliche Weisungsgebundenheit und die daraus resultierenden Obliegenheiten der Beschäftigten wurden ebenfalls in den Wortlaut des Art. 32 Abs. 4 aufgenommen. Die Schulung der Mitarbeiter zu ihren Pflichten und Rechten nach der DSGVO sowie zur unternehmensinternen Datenschutzorganisation ist essenziell für eine wirksame DSGVO-Compliance, denn selbst die besten Richtlinien und Prozesse entfalten ihre Wirkung nur, wenn Mitarbeiter über ausreichendes Wissen und ein entsprechendes Bewusstsein (Awareness) verfügen (Integrität, Vertraulichkeit).[71] Nach Art. 39 Abs. 1 lit. b DSGVO ist der Datenschutzbeauftragte für die Sensibilisierung, Schulung und Überprüfung der an der Datenverarbeitung beteiligten Mitarbeiter verantwortlich - ist kein Datenschutzbeauftragter benannt, obliegt diese Aufgabe der verantwortlichen Stellen.[72] Nach Abschluss der Sensibilisierungsmaßnahmen, sollte eine Vertraulichkeitsvereinbarung ausgehändigt werden, die sie zur vertraulichen Behandlung personenbezogener Daten verpflichtet sowie die weisungsgebundene Datenverarbeitung der Beschäftigten definiert (Vertraulichkeit, Rechenschafts -und Nachweispflichten), im Sinne des Art. 32 Abs. 4.

[67] Vgl. Maßnahme A.6.1 der ISO/IEC 27001:2022, *Brenner*, Praxishandbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 4. Auflage, B.3, vgl. Maßnahme „Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal Seite 32 zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen (B1.7 Vertraulichkeit)“,Das Standard-Datenschutzmodell, Version 3.1, S. 31.
[68] *Schulze*, Zumkley, IT-Arbeitsrecht, 3. Auflage 2023, Rn. 1068.
[69] *Schulze,* Zumkley, IT-Arbeitsrecht, 3. Auflage 2023, Rn. 1069.
[70] *Pelz*, Corporate Compliance, 4. Auflage 2024, Rn. 2. Technische Maßnahmen zum Screening werden unter *Technische Maßnahmen* erläutert.
[71] *Mair/Müller/Schlepitzka*, Compliance Praxis 2019, S. 27.
[72] *Lapp*, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 39.

Im Gegensatz zu den Niederlanden besteht in Österreich und Deutschland grundsätzlich zwar kein gesetzlicher Anspruch auf Telearbeit (Home-Office), wird jedoch in der Post-Covid-Zeit ein unabdingbares Thema auf der Agenda der IT-Sicherheit sein.[73] Eine Home-Office-Richtlinie sollte insbesondere die Trennung von betrieblicher und privater Nutzung der Endgeräte regeln sowie Vorgaben zu Datenschutz, IT-Sicherheit und Aufbewahrung sensibler Unterlagen enthalten, darunter die Nutzung verschlüsselter Speichermedien, ein sicherer Remote-Zugang (z. B. VPN), Kennwortschutz, automatische Bildschirmsperre, das Verbot des Ausdrucks betrieblicher Dokumente und der Weiterleitung dienstlicher E-Mails auf private Accounts (Zweckbindung, Datenminimierung, Integrität, Vertraulichkeit, Angemessene Überwachung der Verarbeitung).[74]

d) Physische Maßnahmen

Im Rahmen der Etablierung physischer Maßnahmen ist eine unmittelbare Orientierung am Kontext der Datenverarbeitung und den äußeren Gegebenheiten unabdingbar. Während in einem eigenen Büro Zugangskontrollen, Alarmanlagen und abschließbare Schränke zentrale Sicherheitsmaßnahmen darstellen (Integrität, Vertraulichkeit, Angemessene Überwachung der Verarbeitung) erfordert ein Coworking Space zusätzliche Sicherheitsvorkehrungen wie abschließbare Container oder Datenschutzfolien auf den Bildschirmen, da auch Betriebsfremde in unmittelbarer Nähe des Arbeitnehmers sind.[75] Bei internen Servern sind Brandschutz, Klimatisierung und Zugangsbeschränkungen essenziell, während bei Outsourcing die Sicherheitsmaßnahmen des Dienstleisters geprüft werden müssen. Im Home-Office spielen Maßnahmen wie ein abschließbarer Arbeitsraum, sichere Aufbewahrung von Dokumenten und kontrollierter Zugang durch Dritte eine entscheidende Rolle. Dokumente, die personenbezogene Daten enthalten, sind gemäß der DIN 66399 mit einem Aktenvernichter der Sicherheitsstufe (ab) P-3 physisch zu vernichten, um eine rekonstruierbare Wiederherstellung der Informationen zu verhindern und die datenschutzrechtlichen Anforderungen der DSGVO zu erfüllen (Zweckbindung, Datenminimierung, Speicherbegrenzung).[76] Für die

[73] Vgl. *Imping*, in: Taeger/Pohle, Computerrechts-Handbuch, Werkstand: 39. EL 2024, Rn. 123

[74] Die Home-Office-Richtlinie beinhaltet bereits etwaige technische Maßnahmen – die Auflistung orientiert sich an *Dury/Leibold*, ZD-Aktuell 2020, 04405. Vgl. Maßnahme A.6.7 der ISO/IEC 27001:2022, *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3.

[75] Zu den datenschutzrechtlichen Risiken eines Coworking-Space vgl. *Oltmanns/Fuhlrott*, NZA 2018, 1225 (1230). Vgl. Maßnahme A.7.7 der ISO/IEC 27001:2022, *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3.

[76] *Meyer/Schmidt*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Rn. 95. Vgl. Maßnahme A.7.14 der ISO/IEC 27001:2022, *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3. Vgl. Maßnahme „*Festlegung und Umsetzung eines Löschkonzepts*“, Das Standard-Datenschutzmodell, Version 3.1, S. 35.

ordnungsgemäße Vernichtung der Hardware (Chipkarten, Festplatten etc.) enthält die DIN-Norm 66399 ebenfalls detaillierte Vorgaben.[77]

e) Technische Maßnahmen

Die Bandbreite der Maßnahmen technischer Natur lässt sich nahezu unbegrenzt erweitern, da fortlaufende Bedrohungen und neue Technologien entstehen. Im Rahmen dieser Ausarbeitung werden jedoch ausschließlich die wesentlichen Maßnahmen berücksichtigt, die in der Fachliteratur als grundlegende Sicherheitsvorkehrungen anerkannt sind und eine solide Basis für den Schutz personenbezogener Daten bieten. Der Unionsgesetzgeber hat mit der Pseudonymisierung (Vertraulichkeit, Integrität, Belastbarkeit, Abmilderung von Datenschutzverletzungen) und der Verschlüsselung (Vertraulichkeit, Integrität, Wiederherstellbarkeit in Backups, Behebung und Abmilderung von Datenschutzverletzungen) bereits zwei zentrale technische Maßnahmen in den Wortlaut aufgenommen.[78] Zum Schutzniveau und den Schwachstellen von Pseudonymisierungstechniken existieren umfangreiche Erläuterungen der Aufsichtsbehörden, die in der Praxis als Leitlinien herangezogen werden können. Dabei ist es essenziell, die jeweils aktuellen technischen Richtlinien des BSI zu berücksichtigen, um den Stand der Technik der Verschlüsselungsmethoden sicherzustellen.[79] Die Anonymisierung wird in Art. 32 nicht explizit erwähnt, ist jedoch de facto die effektivste Sicherheitsmaßnahme. Sie beendet die Anwendbarkeit der DSGVO und sollte in jedem Sicherheitsmanagement berücksichtigt werden.[80] Die Protokollierung (Integrität, Rechenschafts – und Nachweispflichten, angemessene Überwachung der Verarbeitung) dient sowohl der Dokumentation von Verarbeitungsvorgängen als auch der Sicherstellung der Nachweisbarkeit von Einwilligungen. Dabei reicht es nicht aus, lediglich auf eine ordnungsgemäße Ausgestaltung einer Webseite zu verweisen.[81] Vielmehr muss im Einzelfall der konkrete Nachweis der tatsächlichen Erteilung einer Einwilligung erbracht werden, wofür die Protokollierung eine zentrale Rolle spielt - dies umfasst insbesondere die Dokumentation relevanter Informationen, wie etwa den Zeitpunkt und

[77] *Meyer/Schmidt*, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Rn. 96.
[78] Art. 32 Abs. 1 lit. a) DSGVO. Vgl. Maßnahme „*Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten*“, Das Standard-Datenschutzmodell, Version 3.1, S. 35.
[79] *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 9.
[80] Der sachliche Anwendungsbereich ist folglich nicht anwendbar, da eine erfolgreiche Anonymisierung die Identifizierung der natürlichen Person verhindert. *Laue*, Recht der elektronischen Medien, 4. Auflage 2019, Rn. 10. Vgl. Maßnahme A.8.24 der ISO/IEC 27001:2022, *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3.
[81] *Scheja/Reibach/Reichert*, in: Leuopold/Wiebe/Glossner, IT-Recht, 4. Auflage 2021, Rn. 270.

die Identität der Person, den genauen Inhalt der Einwilligung, Sitzungsdaten, wie beispielsweise die IP-Adresse, der User-Agent oder die Sitzungs-ID.[82] Um Manipulationen oder unbefugten Zugriff auf Protokolldaten zu verhindern, müssen diese fälschungssicher gespeichert werden. Dies kann durch digitale Signaturen, unveränderliche Speichersysteme oder revisionssichere Logging-Verfahren erreicht werden. Zudem ist sicherzustellen, dass nur autorisierte Personen Zugriff auf die Protokolle erhalten.[83] In der Schnittstelle zu den Maßnahmen in Bezug zu Menschen werden die E-Mails der Beschäftigten durch verschiedene Schutzmechanismen gefiltert, um potenzielle Gefahren für die digitale Infrastruktur zu minimieren: Ein Virenschutzprogramm sorgt dafür, dass sowohl eingehende als auch ausgehende E-Mails kontinuierlich auf Schadsoftware geprüft werden, *Anti-Spam-Software* sortiert unerwünschte E-Mails raus und Anti-Phishing identifiziert schädliche Mails, die darauf abzielen, vertrauliche oder persönliche Daten durch täuschend echte Nachrichten zu erlangen (Transparenz, Integrität, Vertraulichkeit, Verfügbarkeit).[84] Eine Redundanz informationsverarbeitender Systeme intendiert, die Verfügbarkeit von IT-Systemen und deren Komponenten sicherzustellen. Dies wird durch die Implementierung von redundanten Systemen wie Spiegeldatenbanken, Datensicherungen, Vertretungsregelungen sowie durch Maßnahmen wie unterbrechungsfreie Stromversorgung erreicht (Verfügbarkeit, Belastbarkeit).[85]

3. Angemessenheit im Kontext des Sicherheitsmanagements

Die Sicherheitsanforderungen des Art. 32 DSGVO sind dahingehend zu begrüßen, da sie dem Verantwortlichen einen gewissen Spielraum bei der Auswahl und Implementierung dieser Maßnahmen lässt. Dies ermöglicht eine adaptive Sicherheitsstrategie, die sowohl den spezifischen Risiken des jeweiligen Unternehmens als auch den aktuellen Stand der Technik Rechnung trägt. Die Flexibilität von Art. 32 ermöglicht, je nach Kontext und Ressourcen die für sie passendsten Maßnahmen zu wählen. Dies fördert eine praxisnahe Umsetzung von Security und Compliance. Die Berücksichtigung der Implementierungskosten ist hierbei essenziell: Dieser Faktor ermöglicht eine ökonomische Bewertung, ob die Kosten der Maßnahmen im Verhältnis zu den Risiken für die Rechte und Freiheiten der betroffenen

[82] *Scheja/Reibach/Reichert*, in: Leuopold/Wiebe/Glossner, IT-Recht, 4. Auflage 2021, Rn. 270.
[83] Maßnahme A.8.15 der ISO/IEC 27001:2022, *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3.
[84] *Schmidt/Pruß, Handbuch IT- und Datenschutzrecht*, 3. Auflage 2019, Rn. 309.
[85] *Polenz*, in: Taeger/Pohle, Computerrechts-Handbuch, Werkstand: 39. EL 2024, Rn. 123. Vgl. Maßnahme A.8.14. der ISO/IEC 27001:2022, einsehbar bei: *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3.

Personen angemessen und geeignet sind.[86] Damit einhergehend kann der Spielraum zwar Flexibilität bieten, gleichzeitig jedoch auch zu Unsicherheit führen, da Verantwortliche und Auftragsverarbeiter kostengünstigere Lösungen wählen könnten, die den erforderlichen Schutz nicht gewährleisten. Die Berücksichtigung des Stands der Technik erfordert eine fortlaufende Weiterbildung des Sicherheitsteams, um den aktuellen Anforderungen gerecht zu werden und neue Maßnahmen zu evaluieren. Allein der Aufwand des Informationsersuchens zu Best-Practice-Lösungen stellt einen nicht unerheblichen Kostenfaktor dar. Weitere Kritikpunkte beziehen sich gebündelt auf die redaktionelle Dimension des Artikels: Besonders die fehlende Definition dessen, was als *angemessen* oder *wirksam* in Bezug auf Sicherheitsmaßnahmen gilt, führt zu Unsicherheiten hinsichtlich der Erforderlichkeit. Ferner wird in der deutschen Sprachfassung der DSGVO wird der Begriff „*Schutz"* fälschlicherweise als Synonym für „*Sicherheit"* verwendet - während die Überschrift von Art. 32 „*Sicherheit der Verarbeitung"* lautet, spricht Abs. 1 Satz 1 von einem „Schutzniveau", was zu einer terminologischen Verwirrung führen kann.[87] Die englische Version macht eine klare Unterscheidung zwischen „*Security*" und „*level of security*".[88] Zudem definiert die DSGVO „*Schutz*" oder „*Sicherheit*" nicht explizit, sondern mit Abs. 2 nur mittelbar in Anbetracht des Schutzes in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit.[89] Die redaktionelle Unschärfe des Art. 32 DSGVO erschwert die angestrebte Harmonisierung, da ein gleicher Wortlaut als Grundlage für eine harmonisierte Anwendung dient.

Die in Art. 5 Abs. 1 lit. f) eingangs beleuchteten Grundprinzipien der Informationssicherheit (*Integrität* und *Vertraulichkeit)* werden in Art. 32 Abs. 1 lit. b) mit dem Prinzip der *Verfügbarkeit* ergänzt, was ebenfalls eine Inkonsistenz darstellt. Eine Aufnahme der *Verfügbarkeit* in Art. 5 erscheint mithin sinnvoll.

Eine abgestufte Mindestanforderung – etwa für Unternehmen mit weniger als 250 Beschäftigten – könnte nicht nur die Effizienz steigern, sondern auch eine praxisnahe Umsetzung auf einem angemessenen Sicherheitsniveau ermöglichen. Durch eine solche Differenzierung ließen sich insbesondere KMU gezielter einbinden, was die Akzeptanz der Maßnahmen deutlich erhöhen würde. Gleichzeitig würde eine europaweit einheitliche Staffelung zu einer stärkeren Harmonisierung der Sicherheitsstandards beitragen.

[86] Analog zu *Privacy by Design* und *by Default* unter B. II. *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 5.
[87] *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 6.
[88] *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 6.
[89] *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 7.

IV. Art. 32 und 33 DSGVO: Melde – und Benachrichtigungspflichten

Die Melde- und Benachrichtigungspflichten nach den Artikeln 32 und 33 der DSGVO stellen exekutive Anforderungen dar, die im Falle von Datenpannen sicherstellen sollen, dass sowohl die Aufsichtsbehörden als auch die betroffenen Personen zeitnah und angemessen über die Verletzung des Schutzes personenbezogener Daten informiert werden, um die Risiken für die Rechte und Freiheiten der betroffenen Individuen zu screenen sowie einhergehend zu mitigieren.[90] So hat sich die Anzahl der gemeldeten Datenpannen bei der Aufsichtsbehörde NRW seit dem Inkrafttreten der DSGVO im Jahr 2018 bis 2024 nahezu verdoppelt.[91] Die tüchtige Meldepraxis der verantwortlichen Stellen könnte sich jedoch ändern, wenn die Datenschutzaufsichtsbehörden ihre Sanktionsbefugnisse verstärkt nutzen.[92]

1. Auslegung der Norm

a) Adressat

Nach Art. 33 Abs. 1 DSGVO ist der für die Datenverarbeitung Verantwortliche meldepflichtig und im Konzern meist die jeweilige Legaleinheit, bei der die Datenschutzverletzung auftritt.[93] Art. 33 Abs. 1 S. 1 lässt offen, welcher Verantwortliche im Rahmen einer gemeinsamen Verantwortung (Art. 26) die Meldepflicht trägt - Art. 26 Abs. 1 S. 2 regelt jedoch, dass die Meldepflicht denjenigen trifft, den die Verantwortlichen in ihrer Vereinbarung bestimmen, was eine ungewöhnliche Dispositionsfreiheit bei sicherheitsrelevanten Pflichten bedeutet.[94] Bei ausgelagerten Datenverarbeitungsprozessen, wie etwa einer Auftragsverarbeitung im Sinne des Art. 28 DSGVO, besteht die Meldepflicht des Auftragsverarbeiters gegenüber den Auftraggeber bereits qua Gesetz. Die weitere Abhandlung der Datenpanne muss vom Auftraggeber, der die Verantwortlichkeit der personenbezogenen Daten inne hat, vollzogen werden.

b) Verletzung

Nach § 42a BDSG a. F. betraf die Benachrichtigungspflicht nur bestimmte Risikodaten wie medizinische, strafrechtliche oder finanzielle Informationen - Die DSGVO hingegen erweitert

[90] Vgl. Erwägungsgrund 85.
[91] *LDI NRW*, Meldungen Nach Art. 33 DSGVO (sog. Datenpannen).
[92] Ein Bußgeldorientierter Ansatz der Aufsichtsbehörden im Rahmen von Datenpannen könnte die verantwortlichen Stellen daran hemmen, eine proaktive Meldung zu vollziehen. *Becker*, ZD 2020, 175.
[93] *Reif*, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 19.
[94] *Martini*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 14a. *Reif* allokiert die Meldepflicht im Außenverhältnis an alle beteiligten Verantwortlichen. *Reif*, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 19.

den Anwendungsbereich auf alle personenbezogenen Daten, was einen erheblichen Paradigmenwechsel darstellt.[95] Eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 33 DSGVO setzt, wie die Formulierungen „zur“ und „führt“ in Art. 4 Nr. 12 DSGVO nahelegen, kumulativ die Verletzung der Sicherheit sowie die kausale Beeinträchtigung eines Schutzziels (Verfügbarkeit, Integrität oder Vertraulichkeit) voraus.[96] Eine mögliche Beeinträchtigung kann folglich in drei Sicherheitskriterien kategorisiert werden: Die Verletzung der Vertraulichkeit, die die unbefugte oder unbeabsichtigte Offenlegung oder Einsichtnahme in personenbezogene Daten beschreibt, die Verletzung der Integrität, die sich auf die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten bezieht und die Verletzung der Verfügbarkeit, bei der es um den unbefugten oder unbeabsichtigten Verlust des Zugriffs auf personenbezogene Daten oder deren unbeabsichtigte oder unrechtmäßige Vernichtung geht.[97]
Eine vorübergehende Verletzung der Verfügbarkeit, wie etwa ein Serverausfall, stellt entgegen der vom EDSA im Mai 2018 geäußerten Rechtsansicht keine Datenschutzverletzung dar.[98]

c) Kenntnisnahme, Frist und Dokumentation

Die Meldung an die zuständige Aufsichtsbehörde muss innerhalb von 72 Stunden erfolgen, beginnend mit dem Zeitpunkt, an dem der Verantwortliche der Sicherheitsverletzung und der daraus resultierenden Gefahr für personenbezogene Daten Kenntnis erlangt.[99] Ein kurzer Zeitraum zur Prüfung des Sachverhalts ist erforderlich, jedoch kann eine umfassende rechtliche Prüfung nicht vorab erfolgen.[100] Stattdessen sind die Ermittlungsergebnisse gemäß Art. 33 Abs. 4 DSGVO schrittweise der Aufsichtsbehörde zu übermitteln.[101] In der digitalisierten Welt treten häufig Datenpannen bei Auftragsverarbeitern, wie etwa Cloud-Dienstleistern oder Anbietern von SaaS-Lösungen, auf. Da die Verantwortung beim Auftraggeber liegt und dieser das Risiko besser einschätzen kann, muss der Auftragsverarbeiter eine Datenpanne unverzüglich melden, damit der Auftraggeber seinen Meldepflichten nachkommen kann. Ergänzend zur Meldepflicht aus Art. 33 Abs. 1, verpflichtet Abs. 5, etwaige Verletzungen des Schutzes personenbezogener

[95] *Schultze-Melling*, in: Tager/Gabel, DSGVO – BDSG – TTDSG, 4. Auflage 2021, Rn. 10.
[96] *Becker*, ZD 2020, 175.
[97] *European Data Protection Board*, Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Version 2.0, S. 6.
[98] *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 2.
[99] *Maslewski*, ZD 2023, 251 (253).
[100] *Maslewski*, ZD 2023, 251 (253).
[101] *Maslewski*, ZD 2023, 251 (253).

Daten zu dokumentieren, wobei diese Dokumentationspflicht auch dann bestehen bleibt, wenn der Vorfall als risikoarm bewertet wird und mithin keine Meldepflicht besteht.

d) Inhalt der Meldung

Gemäß Art. 33 Abs. 3 DSGVO sind bei der Meldung einer Datenschutzverletzung vier Mindestangaben erforderlich: Zunächst muss eine Beschreibung der Art der Verletzung erfolgen, die, wenn möglich, auch die betroffenen Kategorien personenbezogener Daten und die ungefähre Zahl der betroffenen Personen umfasst (lit. a). Im Kontext des Sicherheitsmanagements sind hierbei auch die spezifischen Sicherheitslücken oder Angriffsvektoren zu benennen. Zudem sind die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Anlaufstelle für weiterführende Informationen bereitzustellen (lit. b). Eine Einschätzung der wahrscheinlichen Folgen der Verletzung, beispielsweise in Bezug auf mögliche finanzielle Schäden oder unbefugte Zugriffe, muss ebenfalls erfolgen (lit. c). Schließlich sind die ergriffenen oder geplanten Maßnahmen zur Behebung der Verletzung sowie zur Minderung möglicher nachteiliger Auswirkungen aufzuführen, wie etwa Sofortmaßnahmen zur Eindämmung der Bedrohung oder langfristige Sicherheitsverbesserungen (lit. d).
Die Angaben sollen der Aufsichtsbehörde ermöglichen, das Ausmaß des Datenschutzvorfalls dahingehend zu evaluieren, ob alle erforderlichen Maßnahmen ergriffen wurden, um den Vorfall zu beheben und mögliche negative Auswirkungen auf die betroffenen Personen zu verhindern oder zu mitigieren.[102]
Die Benachrichtigungspflicht nach Art. 34 Abs. 2 DSGVO inkludiert im Wesentlichen drei der vier Mindestanforderungen des Art. 33 Abs. 3 DSGVO. Diese Vorschrift spiegelt das in der gesamten DSGVO verankerte Leitbild eines schutzbedürftigen und informierten Bürgers wider, bei dem Transparenz im Mittelpunkt steht, sodass der Betroffene auf Grundlage der bereitgestellten Informationen geeignete Schutzvorkehrungen treffen kann.[103]

2. Angemessenheit im Kontext des Sicherheitsmanagements

a) Die Melde – und Benachrichtigungspflicht im Sicherheitsmanagement

Im Kontext des Sicherheitsmanagements stellt die Umsetzung der Anforderungen aus Art. 33 und 34 DSGVO das Datenschutzteam vor mehrere Herausforderungen. Ein zentrales Risiko ist die Gefahr von veralteten IT- und Datensicherheitsstrukturen, die, bei mangelnder

[102] *Reif*, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 64.
[103] *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 17.

Aktualisierung, zu Sicherheitslücken führen können. Das Sicherheitskonzept sowie die damit verbundenen TOM müssen bereits in präventiver Hinsicht individuell an das Geschäftsmodell und spezifische Risiken des Unternehmens angepasst werden, da Standardlösungen oft nicht ausreichen.[104] Fehlen klare Verantwortlichkeiten und ein effektiver Incident-Response-Plan, kann die Reaktionszeit bei einem Vorfall verzögert werden, was die rechtzeitige Meldung und Schadensbegrenzung erschwert.[105] *Reif* stellt eine prägnante konzeptionelle Anleitung für erfolgreiches Incident-Management zur Verfügung: Dazu gehören die Formulierung interner Richtlinien, die Definition von Datenschutzverletzungen, die Festlegung von Verantwortlichen und die Bildung eines Krisenteams. Ein Security-Incident-Response-System sollte IT-Systeme überwachen, Datenlecks schnell beheben und forensische Analysen ermöglichen. Ein Data-Breach-Notification-Management-System sorgt für klare Kommunikationswege, Kooperation mit Auftragsverarbeitern und die rechtzeitige Einbindung von Entscheidungsträgern sowie der Aufsichtsbehörde. Zusätzlich ist der Kontakt zur Strafverfolgungsbehörde notwendig, da mögliche Betroffenenmitteilungen die Strafverfolgung gefährden könnten.[106] Der Incident-Plan von *Reif* konzentriert sich vor allem auf Makroprozesse, die die übergeordneten Abläufe bei Datenschutzverletzungen regeln. Es ist jedoch von immenser Wichtigkeit, auch die mikroskopische Perspektive der konkreten Vorgehensweise bei einem Datenschutzvorfall zu berücksichtigen. Diese detaillierten Schritte sollten idealerweise in der Datenschutzrichtlinie, die unter *organisatorische Maßnahmen* eruiert wurde, festgelegt werden, die als operativer Leitfaden für den Umgang mit Datenschutzvorfällen dient. *Kinast/Stanonik* definieren einen fünftaktigen Ablauf aus der Mikroperspektive für den Umgang mit Datenschutzverletzungen. Der Prozess beginnt mit der Meldung seitens des zuständigen Mitarbeiters, der einen Vorfall erkennt und diesen umgehend dokumentiert und weiterleitet. Im nächsten Schritt folgt die Sachverhaltsermittlung, bei der der Vorfall genau analysiert wird, um Art, Umfang und mögliche Auswirkungen der Datenschutzverletzung zu bestimmen. Daraufhin werden Sofortmaßnahmen ergriffen, um den Vorfall zu begrenzen. In der vierten Phase erfolgt die Entscheidung über die Meldepflicht, bei der beurteilt wird, ob die Verletzung gemäß Art. 33 DSGVO an die Aufsichtsbehörde gemeldet werden muss. Schließlich werden weitere Maßnahmen definiert, die je nach Schwere des Vorfalls die Benachrichtigung der betroffenen Personen, die Durchführung von forensischen Analysen oder

[104] *Brams*, ZD 2023, 487 (485).
[105] *Brams*, ZD 2023, 487 (485).
[106] Der gesamte Krisenreaktionsplan orientiert sich an *Reif*, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 77.

die Anpassung der Sicherheitsvorkehrungen umfassen können.[107] Folglich stellt die abteilungsübergreifende Kommunikation eine große Herausforderung für das Sicherheitsmanagement dar. Zudem kann die Sorge vor arbeitsrechtlichen Konsequenzen die Bereitschaft der Mitarbeitenden zur Meldung von Vorfällen beeinträchtigen.[108] Eine gezielte Schulung könnte dazu beitragen, diese Hürden zu überwinden.
Eine weitere Hürde ist die einzuhaltende Frist von 72 Stunden zur Meldung einer Datenschutzverletzung an die zuständige Aufsichtsbehörde. Diese enge zeitliche Vorgabe erfordert eine effiziente und gut organisierte Prozessstruktur.
Das Lieferantenmanagement steht weiterhin vor der Herausforderung, die Anforderungen des Art. 28 DSGVO zu erfüllen. Eine sorgfältige Auswahl und vertragliche Absicherung der Dienstleister ist entscheidend, um Melde- und Informationspflichten ordnungsgemäß zu erfüllen. Eine zentrale und nachvollziehbare Dokumentation bildet dabei die Grundlage für ein wirksames Management von Datenschutzvorfällen und unterstützt die Umsetzung der Rechenschaftspflicht.

b) Angemessenheit der Norm

Vorauszuschicken ist, dass Geldbußen gemäß Art. 83 Abs. 1 DS-GVO *wirksam, verhältnismäßig und abschreckend* sein sollten, wobei die Aufsichtsbehörden diese Kriterien als Leitlinie bei der Berechnung der Bußgelder berücksichtigen müssen.[109] Im Zuge dessen liegt es nahe, die Angemessenheit (sowie die damit einhergehende Harmonisierungswirkung) der Artikel 33 und 34 DSGVO auch auf der Empfängerseite der Meldung, also bei den Aufsichtsbehörden, zu bewerten.
Bei direkten Verstößen gegen die Melde- und Benachrichtigungspflichten lässt sich eine gewisse Harmonisierung in der Rechtsdurchsetzung beobachten.
So verhängte die irische Aufsichtsbehörde ein Bußgeld von 450.000 EUR gegen die *Twitter International Company*, da sie feststellte, dass Twitter gegen Art. 33 Abs. 1 und Abs. 5 DSGVO verstoßen hatte, da die Datenschutzverletzung nicht fristgerecht gemeldet und nicht ordnungsgemäß dokumentiert wurde.[110] 2021 verhängte die Datenschutzbehörde der Niederlande eine Geldbuße von 475.000 EUR gegen das Online-Reisebüro *Booking.com*, da

[107] Der gesamte fünftaktige Plan orientiert sich an *Kinast/Stanonik*, Praxishandbuch Datenschutz für KMU, 1. Auflage 2019, S. 234.
[108] Im Ergebnis ebenso: *Hanloser*, CCZ 2010, 29 (25).
[109] *Brams*, ZD 2023, 487 (485).
[110] *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 27.

das Unternehmen eine Datenschutzverletzung nicht innerhalb von 72 Stunden nach deren Bekanntwerden gemeldet hatte.[111]

Diese zu beobachtende Harmonisierung steht jedoch im Schatten Rechtsdurchsetzung von größeren Fällen im unionsweiten Vergleich: Während die deutsche *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)* einen eher ausgewogenen Ansatz verfolgt, zeigt die französische *Commission Nationale de l'Informatique et des Libertés (CNIL)* eine öffentlichkeitswirksamere strengere Haltung, mit einem Fokus auf Transparenzvorgaben, rigoroser Durchsetzung und höheren Bußgeldern.[112] Diese Unterschiede verdeutlichen eine geringe Harmonisierungswirkung der DSGVO in der Rechtsdurchsetzung.

Weiterhin legt Art. 34 DSGVO fest, dass eine Benachrichtigung der betroffenen Personen nur dann erforderlich ist, wenn eine Verletzung des Datenschutzes *voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.*[113] Diese Formulierung ist kritikwürdig, da sie impliziert, dass nicht jede Datenschutzverletzung automatisch eine Benachrichtigungspflicht auslöst, sondern nur solche, die als hochrisikobehaftet eingestuft werden. In der Praxis führt dies zu einer erheblichen Einschränkung der Informationspflicht gegenüber den betroffenen Personen und lässt potenziell wichtige Benachrichtigungen aus.[114] Im gleichen Zuge bietet die DSGVO Flexibilität, da sie im Rahmen der Benachrichtigungspflichten technologieoffen ist und keine spezifische Methode vorgibt, wie die Benachrichtigung gegenüber den betroffenen Personen erfolgen muss. Dies ermöglicht es dem Verantwortlichen, auf verschiedene Kommunikationskanäle zurückzugreifen, etwa indem sie eine gebündelte Landingpage erstellt, Aushänge veröffentlicht oder Rundmails versendet.

V. Art. 35 DSGVO: Datenschutzfolgeabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) stellt ein zentrales Instrument im modernen Sicherheitsmanagement dar. Sie wurde durch die DSGVO eingeführt, um im Falle eines voraussichtlichen hohen Risikos für die Rechte und Freiheiten natürlicher Personen präventiv

---

[111] *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 31.

[112] Im Jahr 2019 verhängte die *CNIL* ein Bußgeld in Höhe von 50 Millionen Euro gegen Google LLC aufgrund einer unzureichenden Umsetzung der Transparenz – sowie informationspflichten, vgl. *European Data Protection Board*, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21. Januar. 2019. Im Jahr 2024 wurde ein Bußgeld in Höhe von 50 Millionen Euro an den französischen Telekommunikationsdienstleister ORANGE aufgrund rechtswidriger Werbeanzeigen verhängt, vgl. *CNIL*, Advertisements inserted among emails: ORANGE fined €50 million, 10. Dezember. 2024.

[113] *Martini*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Art. 34 Rn. 28.

[114] Es ist fraglich, inwieweit Aufsichtsbehörden bei einem mittleren Risiko dennoch die Auffassung vertreten könnten, dass eine Benachrichtigung der betroffenen Personen erforderlich ist. In diesen Fällen würde eine entsprechende Kommunikation mit weiteren Calls-to-Action erfolgen.

datenschutzrechtliche Risiken zu identifizieren, zu bewerten und gegebenenfalls durch geeignete Abhilfemaßnahmen zu minimieren.[115] Diese proaktive Herangehensweise ist besonders relevant in einem zunehmend digitalisierten Umfeld, in dem die Verarbeitung großer Mengen personenbezogener Daten allgegenwärtig ist. Im Zeitalter der Künstlichen Intelligenz, insbesondere bei der Nutzung von großen Sprachmodellen wie ChatGPT, gewinnt die DSFA stetig an Bedeutung. Die Verarbeitung personenbezogener Daten durch solche Technologien geht oft mit hohen Risiken einher, die durch eine umfassende Datenschutz-Folgenabschätzung systematisch adressiert werden müssen.

1. Auslegung der Norm

a) Voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen

Eine Verarbeitung erfordert eine Datenschutz-Folgenabschätzung, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Dies ist dann der Fall, wenn einer der in Absatz 3 genannten Fälle zutrifft, die Art der Verarbeitung auf einer schwarzen Liste der zuständigen Aufsichtsbehörde gemäß Absatz 4 aufgeführt ist oder nach einer ersten Einschätzung unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein hohes Risiko festgestellt wird.[116] Die Letztere kumulative Aufzählung der vier Attribute legt nahe, dass eine Spezifizierung und Bewertung der geplanten Datenverarbeitung in Bezug auf den Risikograd nur in der Gesamtschau der Attribute erfolgen kann.[117]

Risiken für die Rechte und Freiheiten betroffener Personen, die bei der Bewertung eines voraussichtlichen hohen Risikos berücksichtigt werden sollten, sind in den Erwägungsgründen 75, 83 und 85 beschrieben und spiegeln weitestgehend die Dimensionen einer Datenpanne wider.[118] Dies impliziert zugleich, dass nicht jede Datenverarbeitung mit einer DSFA abgesegnet werden muss.

Zur Bewertung eines hohen Risikos bei einer Verarbeitung ist eine Prognose des Verantwortlichen erforderlich, die im Rahmen einer Schwellenwertanalyse zeigt, ob ein bestimmter Risikograd überschritten wird.[119]

Ferner empfiehlt die europäische Datenschutzgruppe (WP29) auch dann eine DSFA durchzuführen, wenn Unsicherheit über ihre Notwendigkeit besteht, da dies den

[115] *Sedef/Steiner*, Datenschutz – Folgenabschätzung, 25.02.2025.
[116] *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Art. 35 DSGVO, Rn. 2.
[117] Im Ergebnis ebenso: *Jandt*, in: Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, Art. 35, Rn. 7.
[118] *Schwendemann*, in: Sydow/Marsch, DS-GVO | BDSG, 3. Auflage 2022, Art. 35, Rn. 9.
[119] *Schwendemann*, in: Sydow/Marsch, DS-GVO | BDSG, 3. Auflage 2022, Art. 35, Rn. 9.

Verantwortlichen ein wertvolles Instrument zur Sicherstellung der Einhaltung der Rechenschaftspflicht bietet.[120]

b) Inhalt der Folgenabschätzung

Vorab ist festzuhalten, dass nach dem Wortlaut der DSGVO ausschließlich der Verantwortliche unmittelbar zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist. Der Auftragsverarbeiter unterliegt hingegen keiner eigenständigen Verpflichtung zur Durchführung, sondern ist lediglich verpflichtet, den Verantwortlichen bei der Durchführung zu unterstützen.[121] Nichtsdestotrotz müssen auch Auftragsverarbeiter Weitsicht bewahren, denn es wird mit großer Wahrscheinlichkeit auch Datenverarbeitungsprozesse geben, in der sie, neben der Tätigkeit als Auftragsverarbeiter, als Verantwortliche agieren.
Ebenso ist der Datenschutzbeauftragte grundsätzlich nicht für die Durchführung der DSFA verantwortlich, sondern hat auf Anfrage in Bezug auf diese zu beraten.[122]
Das Hauptziel der Datenschutz-Folgenabschätzung ist es, die Auswirkungen geplanter Verarbeitungsvorgänge auf den Datenschutz zu ermitteln, wobei der Schutz personenbezogener Daten die Sicherheit der Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, Offenlegung oder Zugänglichmachung umfasst.[123]
Gemäß Artikel 35 Abs. 7 DSGVO muss eine DSFA mindestens eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, eine Einschätzung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie die vorgesehenen Maßnahmen zur Risikominderung enthalten.[124] Es liegt Nahe die letztere Anforderung unmittelbar mit den bereits vorhandenen TOM zu kombinieren und/oder zu ergänzen, sodass eine gesamtheitliche Konzeption erfolgen kann.
Eine Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO kann als Ultima Ratio betrachtet, wenn die geplanten Abhilfemaßnahmen nicht ausreichen, um ein hohes Risiko

[120] Der Ansicht ist in Gänze zuzustimmen – man bedenke die Anforderungen an die Rechenschaftspflicht, die eine proaktive Nachweisfähigkeit hinsichtlich der Einhaltung der Compliance-Anforderungen der DSGVO bedingen. *Datenschutzgruppe nach Artikel 29*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt, 4. April 2017, S. 9.

[121] „[..] So führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.“ – Art. 35 Abs. 1 DSGVO.

[122] Im Ergebnis ebenso: *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Art. 35 DSGVO, Rn. 5.

[123] *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Art. 35 Rn. 54.

[124] *Jandt*, in: Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, Art. 35 Rn. 32. *Schwendemann*, in: Sydow/Marsch, DS-GVO | BDSG, 3. Auflage 2022, Art. 35, Rn. 23.

für die Rechte und Freiheiten der betroffenen Personen zu verringern. Wie häufig diese Möglichkeit in der Praxis genutzt wird, ist jedoch unklar. Der Konsultationsweg hat einen Offenbarungscharakter, da der Verantwortliche gezwungen ist, umfassende Informationen über die geplante Verarbeitung und die identifizierten Risiken preiszugeben.

2. Angemessenheit im Kontext des Sicherheitsmanagements

a) Die DSFA im Sicherheitsmanagement

Die Durchführung einer Datenschutz-Folgenabschätzung erfordert vom Compliance- und Security-Team eine sorgfältige Planung, da die Anforderungen des Art. 35 DSGVO zwar normative Vorgaben zur Sicherstellung des Datenschutzes liefern, jedoch keine konkreten Verfahrensbeschreibungen oder praxisorientierte Anleitungen enthalten. Insbesondere ist es schwierig, die Risiken in Hinblick auf die personenbezogenen Daten und die Rechte der betroffenen Personen, angemessen zu bewerten, da die DSGVO vorwiegend auf die Notwendigkeit von Schutzmaßnahmen hinweist, ohne detaillierte Schritte zur Durchführung der DSFA vorzugeben. Folglich erfolgt die Abhandlung einer DSFA auf eigener Methodik sowie Expertise.[125]

Es wäre ratsam, dass Verantwortliche ein standardisiertes Muster zur Durchführung der Datenschutz-Folgenabschätzung erstellen, das in der gesamten Organisation einheitlich verwendet werden kann. Dies ermöglicht Synergien sowie Transfermechanismen in Bezug auf Risikomitigierungen.

Weiterhin empfiehlt *Schwendemann*, dass Organisationen die Anforderungen an Privacy by Design und Privacy by Default zusammen mit der Datenschutz-Folgenabschätzung in einem gemeinsamen Prozess abdecken sollten. Obwohl der Prüfungsmaßstab für beide Anforderungen nicht identisch ist, kann eine integrierte Herangehensweise die Effizienz steigern und die Einhaltung der Datenschutzvorgaben optimieren.[126]

Im Rahmen eines effektiven Sicherheitsmanagements ist eine standardisierte Vorgehensweise in diesem Zusammenhang ausdrücklich begrüßenswert, da sie eine rechtssichere und nachvollziehbare Entscheidung darüber ermöglicht, ob eine DSFA erforderlich ist. Zunächst ist zu prüfen, ob der konkrete Verarbeitungsvorgang unter einen der in der sogenannten „weißen Liste“ Fälle fällt. Ist dies der Fall, besteht keine Verpflichtung zur Durchführung einer DSFA. In einem zweiten Schritt ist zu klären, ob der Verarbeitungsvorgang von der „schwarzen Liste“ erfasst ist. Ist dies der Fall, so ist eine DSFA zwingend erforderlich. Drittens sind die in § 2 Abs

[125] *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 35 Rn. 71.
[126] *Schwendemann*, in: Sydow/Marsch, DS-GVO | BDSG, 3. Auflage 2022, Art. 35, Rn. 43.

3 DSFA-V genannten besonderen Fallkonstellationen zu prüfen, die durch mehrere unbestimmte Rechtsbegriffe gekennzeichnet sind und ebenfalls zur Pflicht einer DSFA führen können. Schließlich ist – unabhängig von den zuvor genannten Listen und Fallgruppen – im vierten Schritt zu bewerten, ob ein Verarbeitungsvorgang voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Diese Generalklausel des Art. 35 Abs. 1 DSGVO ist laut Europäischem Datenschutzausschuss anhand eines beweglichen Systems aus neun Risikokriterien zu beurteilen.[127]

b) Angemessenheit der Norm

Ein Kritikpunkt an Art. 35 DSGVO liegt in der unklaren Bestimmung dessen, was unter einem *hohen Risiko* zu verstehen ist. Wenig greifbar wird die Norm jedoch dadurch, dass es an einer Legaldefinition des hohen Risikos für die Rechte und Freiheiten der betroffenen Person oder zumindest an messbaren Kriterien fehlt.[128] In der Folge sind Verantwortliche auf die – rechtlich nicht bindenden – Leitlinien des EDSA angewiesen, um eine fundierte Einschätzung treffen zu können.

Problematisch ist zudem, dass die DSGVO zwar bestimmte Verfahrensschritte und Dokumentationspflichten im Rahmen der DSFA vorgibt (Art. 35 Abs. 2, 7 und 9 DSGVO), jedoch keine verbindliche Methodik für die Risikobewertung definiert. Art. 35 Abs. 1 DSGVO überlässt es vielmehr dem Verantwortlichen, wie diese im Einzelnen zu erfolgen hat.[129] Die Folge ist ein erheblicher Spielraum bei der Umsetzung, der nicht nur Unsicherheiten in der Praxis mit sich bringt, sondern auch die unionsweit angestrebte Harmonisierungswirkung der Verordnung beeinträchtigt.

Der Unionsgesetzgeber überträgt dem Verantwortlichen die Pflicht zur eigenständigen Risikobewertung. Wird im Zuge dessen festgestellt, dass trotz umgesetzter Maßnahmen zur Risikominderung, ein hohes Risiko für die Rechte und Freiheiten betroffener Personen bestehen bleibt, ist gemäß Art. 36 DSGVO eine vorherige Konsultation der Aufsichtsbehörde erforderlich. Diese Selbstverantwortung birgt jedoch die Gefahr eines strategischen Missbrauchs: Um eine Behördenkonsultation zu vermeiden, könnten Verantwortliche das Risiko proaktiv als geringer einstufen, als es tatsächlich ist. Damit wird das Ziel der DSGVO, ein hohes Schutzniveau für personenbezogene Daten und den natürlichen Personen zu gewährleisten, potenziell unterlaufen. Ein wesentlicher Vorteil der Datenschutz-Folgenabschätzung liegt darin, dass sich Verantwortliche – etwa beim Einsatz von KI-

[127] Der Vierschritt orientiert sich an *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Art. 35 DSGVO, Rn. 2.
[128] *Schwendemann*, in: Sydow/Marsch, DS-GVO | BDSG, 3. Auflage 2022, Art. 35, Rn. 43.
[129] *Reibach*, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, 4. Auflage 2022, Art. 35, Rn. 5.

Technologien – frühzeitig und strukturiert mit möglichen Risiken sowie geeigneten Sicherheitsmaßnahmen auseinandersetzen müssen.[130] Zur Bewältigung identifizierter Problemschwerpunkte sind insbesondere durch den gezielten Einsatz von TOM wirksame Abhilfemaßnahmen zu planen.

VI. Art. 37-39 DSGVO: Datenschutzbeauftragter (DSB)

1. Auslegung der Norm

Eine Benennungspflicht des DSB seitens der verantwortlichen Stelle oder des Auftragsverarbeiters besteht, wenn seine Verarbeitung in eine der Fallgruppen des Art. 37 Abs. 1 Buchst. a–c fällt oder eine nationale Benennungspflicht nach Abs. 4 S. 1 Hs. 2 besteht.[131] In Deutschland greift § 38 BDSG, wonach ab regelmäßig 20 mit der automatisierten Verarbeitung personenbezogener Daten betrauten Personen ein Datenschutzbeauftragter zu bestellen ist.[132] In Österreich besteht keine generelle Benennungspflicht ab einer bestimmten Mitarbeiterzahl für den privaten Sektor.[133]
Zu den legaldefinierten Kernkompetenzen des DSB gehört die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben, die Beratung der verantwortlichen Stelle (etwa im Rahmen der Durchführung von DSFA), der Beschäftigten und das Agieren als Ansprechpartner für Aufsichtsbehörden und Betroffene.[134] Daraus lässt sich ableiten, dass der DSB, ähnlich wie der Compliance-Officer, eine Selbstkontrollfunktion zur Sicherstellung der gesetzlichen und organisatorischen Pflichten des Unternehmens erfüllt.[135] Weiterhin ist anzumerken, dass seine Aufgaben unabhängig und ohne Weisungen des Verantwortlichen oder Auftragsverarbeiters erfüllen muss.[136]
Im Kontext des Sicherheitsmanagements ist hervorzuheben, dass nach Art. 37 Abs. 6 DSGVO die Benennung eines Datenschutzbeauftragten auch auf der Grundlage eines Dienstleistungsvertrags zulässig ist. Dies ermöglicht es, einen externen Datenschutzfachmann mit der Wahrnehmung der Aufgaben des Datenschutzbeauftragten zu betrauen.[137]

[130] Im Ergebnis ebenso: *Schürmann,* ZD 2022, 316 (321).
[131] *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 19.
[132] *Redeker*, IT-Recht, 8. Auflage 2023, Rn. 1103.
[133] Vgl. § 5 DSG.
[134] Art. 39 Abs. 1 DSGVO.
[135] *Thüsing/Granetzny*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 3. Auflage 2021, Rn. 1.
[136] Art. 38 Abs. 3 DSGVO.
[137] *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 54.

2. Angemessenheit im Kontext des Sicherheitsmanagement

a) Der Datenschutzbeauftragter im Sicherheitsmanagement

Zunächst wird von der Führungsriege entschieden werden müssen, ob der Datenschutzbeauftragte intern oder extern besetzt wird. Externe DSB bieten durch Spezialisierung und Erfahrung aus verschiedenen Sektoren hohe Fachkompetenz und einen breiten Überblick, sind jedoch nicht ständig vor Ort und werden teils später in relevante Prozesse eingebunden.[138]

Im Rahmen dieser Ausarbeitung wird weiterhin deutlich, dass ein ausschließlich juristischer Hintergrund des Datenschutzbeauftragten nicht ausreicht. Vielmehr ist ergänzendes informationsrechtliches und technisches Wissen erforderlich. Die zur Wissensaktualisierung gemäß Art. 38 Abs. 2 DSGVO notwendigen Ressourcen umfassen insbesondere Fachliteratur und Schulungen, bei internen Datenschutzbeauftragten zudem ausreichend Zeitressourcen zur kontinuierlichen Weiterbildung.[139]

Der Grundtenor dieser Ausarbeitung trifft auch explizit auf den DSB zu: Der Datenschutzbeauftragte hat eine zentrale Funktion in der übergeordneten Governance-Struktur inne.[140] Eine organisatorische Einbindung mit klar definierten Meldeprozessen in der IT-Richtlinie ist hierfür unerlässlich.

b) Angemessenheit

Durch die Kombination aus Überwachungs-, Beratungs- und Schnittstellenfunktion zu Aufsichtsbehörden sowie Betroffenen wird der DSB zu einer zentralen Instanz der internen Selbstkontrolle. Die Zulässigkeit der externen Bestellung gemäß Art. 37 Abs. 6 DSGVO ermöglicht zudem den flexiblen Einsatz spezialisierter Fachkompetenz, erfordert aber angepasste Abstimmungsmechanismen, um eine frühzeitige Einbindung in sicherheitsrelevante Entscheidungen sicherzustellen. Die in Art. 38 Abs. 3 DSGVO normierte Weisungsfreiheit stärkt seine Unabhängigkeit und ermöglicht eine objektive Bewertung sicherheitsrelevanter Prozesse. Während Art. 38 Abs. 3 DSGVO unionsweit – und damit auch in Österreich – sicherstellt, dass Datenschutzbeauftragte weder wegen der Erfüllung ihrer Aufgaben abberufen noch benachteiligt werden dürfen, besteht im österreichischen Recht kein darüberhinausgehender Sonderkündigungsschutz. In Deutschland hingegen wird die Unabhängigkeit des internen Datenschutzbeauftragten zusätzlich durch § 6 Abs. 4 BDSG abgesichert, der einen erweiterten Abberufungs- und Kündigungsschutz während der

[138] *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 55.
[139] *Feiler/Forgo*, EU-DSGVO, 2. Auflage, Rn. 3.
[140] Im Ergebnis ebenso: *Thüsing/Granetzny*, in: Thüsing, Beschäftigtendatenschutz und Compliance, 3. Auflage 2021, Rn. 1.

Amtszeit sowie für ein Jahr nach deren Beendigung vorsieht.[141]
Aus Perspektive der Harmonisierung zeigt sich ein eingeschränktes Bild: Während die DSGVO ein unionsweit einheitliches Grundgerüst vorgibt, führen nationale Sonderregelungen wie §§ 6 und 38 BDSG in Deutschland zu divergierenden Normen, die etwa in Österreich nicht bestehen. Dies kann zu unterschiedlichen Schutzniveaus und Implementierungspraktiken führen, was die angestrebte Einheitlichkeit teilweise konterkariert.

VII. Zwischenfazit

In Anbetracht der ersten Forschungsfrage, die die Sicherheitsanforderungen sowie die Angemessenheit dieser betrifft, lässt sich festhalten, dass die DSGVO ein umfassendes und mehrdimensionales Sicherheitsmanagement statuiert, das auf einem Zusammenwirken normativer Grundprinzipien (Art. 5), prozessualer Gestaltungsprinzipien (Art. 25), TOM (Art. 32) sowie exekutiver Pflichten (Art. 33, 34, 35) basiert. Die vorangehende Analyse zeigt, dass insbesondere der Grundsatz der Integrität und Vertraulichkeit in Art. 5 Abs. 1 lit. f) sowie die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO das Grundgerüst für ein datenschutzkonformes Sicherheitsmanagement darstellen. Diese Prinzipien greifen unmittelbar in die risikoorientierten Ansätze von TOM nach Art. 32 sowie die Pflicht zur technischen und datenschutzfreundlichen Systemarchitektur gemäß Art. 25 ein.
Hinsichtlich der Angemessenheit zeichnet sich die DSGVO durch eine flexible und risikobasierte Herangehensweise aus, welche sowohl den Stand der Technik als auch wirtschaftliche Aspekte berücksichtigt. Diese beschriebene Flexibilität erlaubt zwar eine differenzierte Umsetzung, kann jedoch bei fehlender Fachkenntnis zu Unsicherheiten und Überforderung für KMU führen. Eine explizite Definition des „angemessenen Schutzniveaus“ fehlt. Ferner bleibt die Harmonisierungswirkung in der Praxis, vor allem im Bereich der Aufsichtsmaßnahmen, bislang begrenzt.
Ungeachtet dessen zeigt sich insgesamt, dass die DSGVO durch die Integration etablierter Informationssicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit) in Verbindung mit Governance-Anforderungen ein geeignetes Fundament für ein zeitgemäßes Sicherheitsmanagement im Lichte des Datenschutzes bildet.

[141] *Henssler*, Münchener Kommentar zum BGB, 9. Auflage 2023, Rn. 30.

C. NIS-2-Richtlinie

Während sich der sachliche Anwendungsbereich der DSGVO vorrangig dem Schutz personenbezogener Daten widmet, verfolgt die NIS-2-Richtlinie einen umfassenderen Ansatz. Die Erwägungsgründe verdeutlichen, dass ihr Schwerpunkt insbesondere auf der Sicherheit von Netz- und Informationssystemen im Sinne der klassischen IT-Sicherheit liegt. In diesem Kontext lässt sich die NIS-2-Richtlinie als ein zentrales europäisches Regelwerk der Cybersicherheit einordnen. Sie verfolgt das Ziel, ein hohes gemeinsames Sicherheitsniveau für Netz- und Informationssysteme innerhalb der Union zu gewährleisten und dadurch das Funktionieren des Binnenmarkts zu stärken.[142]

Die Notwendigkeit einer umfassenderen Regulierung im Bereich der Cybersicherheit ergibt sich aus den stetig wachsenden Herausforderungen der IT-Sicherheitslage: Die Zunahme hochentwickelter, häufig KI-gestützter Angriffsformen – wie etwa Ransomware – verdeutlicht ebenso wie die sicherheitsrelevanten Schwachstellen im Zuge der pandemiebedingten Verlagerung ins Home-Office die Verwundbarkeit moderner IT-Strukturen.[143] Verstärkt wurde diese Entwicklung durch die geopolitischen Spannungen infolge des völkerrechtswidrigen Angriffskrieges Russlands gegen die Ukraine, der auch digitale Infrastrukturen zunehmend als strategisches Ziel adressiert.[144]

Vor diesem Hintergrund intendiert die NIS-2-Richtlinie eine Mindestharmonisierung[145] und reagiert auf die zunehmende Digitalisierung und Vernetzung, die zwar Chancen für Wirtschaft und Gesellschaft schafft, zugleich aber das Risiko von Cyberangriffen und Sicherheitsvorfällen erheblich erhöht.[146]

Sie verpflichtet die betroffenen Einrichtungen zu konkreten Maßnahmen im Bereich der Governance, des Risikomanagements und der Vorfallsbearbeitung.

Ziel dieses Themenblocks ist es, die Bedeutung der NIS-2-Richtlinie im Rahmen eines zeitgemäßen Sicherheitsmanagements herauszuarbeiten und ihre Angemessenheit kritisch zu hinterfragen. Im Fokus steht dabei die Frage, inwieweit die Richtlinie zu einer praxisnahen Verzahnung von Security und Compliance beiträgt.

---

[142] Vgl. Erwägungsgrund (1).
[143] *Degen/Emmert*, Elektronischer Rechtsverkehr, 3. Auflage 2025, § 9 IT- Sicherheit, Rn. 4.
[144] *Degen/Emmert*, Elektronischer Rechtsverkehr, 3. Auflage 2025, § 9 IT- Sicherheit, Rn. 4.
[145] Die Richtlinie steht dem Erlass oder der Aufrechterhaltung nationaler Vorschriften durch die Mitgliedstaaten nicht entgegen, sofern diese ein höheres Niveau an Cybersicherheit gewährleisten und mit den unionsrechtlichen Verpflichtungen der Mitgliedstaaten vereinbar sind, i.S.d. Art. 5 NIS-2-RL.
[146] Vgl. Erwägungsgründe (1), (3), (5) und (7). Für eine granulare Differenzierung der Begriffe *IT-Sicherheit* sowie *Cybersicherheit*: *Schallbruch*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Auflage 2024, § 5 IT-Sicherheit aus gesamtgesellschaftlicher Sicht, Rn. 6.

I. Art. 2 und Art. 3 NIS-2-RL: Betroffenheitsanalyse

1. Auslegung der Norm

Grundsätzlich fallen diejenigen Einrichtungen unter den Anwendungsbereich der NIS-2-Richtlinie, die gemäß Artikel 2 in Verbindung mit der Empfehlung 2003/361/EG (KMU-Definition) mindestens als mittlere Unternehmen einzustufen sind und Dienste erbringen, die in den Anhängen I und II der Richtlinie aufgeführt sind.[147] Ein besonderes Augenmerk liegt in der Einteilung in wesentliche und wichtige Einrichtungen: Als wesentliche Einrichtungen gelten große Unternehmen der in Anhang I der NIS-2-Richtlinie genannten Art sowie bisherige Betreiber wesentlicher Dienste. Einrichtungen der in Anhang I oder II aufgeführten Art, die diese Voraussetzungen nicht erfüllen, werden als wichtige Einrichtungen eingestuft.[148] Der Anwendungsbereich wird mithin weiter gefasst, indem zusätzliche Sektoren aufgenommen werden, die aufgrund ihres Digitalisierungsgrads, ihrer volkswirtschaftlichen sowie gesellschaftlichen Relevanz als kritisch eingestuft werden.

Zu den unter der NIS-2-Richtlinie neu aufgenommenen Sektoren zählen im Bereich der hochkritischen Sektoren Weltraum und Abwasserwirtschaft. Im Bereich der sonstigen kritischen Sektoren wurde die öffentliche Verwaltung, Post- und Kurierdienste, Abfallwirtschaft, Chemikalien, Lebensmittelversorgung, bestimmte Industriezweige (z. B. Maschinenbau), digitale Dienste sowie Forschung ergänzt.[149]

Artikel 3 führt zudem eine einheitliche Größenschwelle ein, nach der Kleinst- und kleine Unternehmen grundsätzlich vom Anwendungsbereich der Richtlinie ausgenommen sind.[150]

Ob eine Einrichtung dem Anwendungsbereich der Richtlinie unterfällt, richtet sich dabei ausschließlich nach der in den Anhängen enthaltenen Spalte zur Art der Einrichtung, in der konkrete Tätigkeiten und Dienste oft unter Verweis auf weitere europarechtliche Definitionen beschrieben sind. Die tabellarische Gliederung nach Sektor, Teilsektor und Einrichtungsart dient somit primär der strukturierten Einordnung, ist aber rechtlich nicht gleichrangig maßgeblich.[151]

[147] *Hessel/Schneider*, MMR 2025, 243.
[148] *Neuwirth*, jusIT, 2024/2, S.7.
[149] *Werry/Éles*, MMR 2024, 829 (830).
[150] *Werry/Éles*, MMR 2024, 829 (830).
[151] *Hessel/Schneider*, MMR 2025, 243.

2. Angemessenheit im Kontext des Sicherheitsmanagements

a) Betroffenheitsanalyse im Kontext des Sicherheitsmanagements

Ersten Einschätzungen zufolge werden in Deutschland voraussichtlich knapp 30.000 Unternehmen betroffen sein.[152] In Österreich wird der Anwendungsbereich der NIS-2-Richtlinie nach Schätzungen der Wirtschaftskammer Österreich rund 4.000 Unternehmen und Einrichtungen aus insgesamt 18 kritischen Sektoren erfassen.[153]

Die finale Entscheidungsfindung, ob eine Einrichtung unter den Anwendungsbereich der NIS-2-Richtlinie fällt, gestaltet sich in der Praxis wenig eindeutig. Ein Umstand, der sich bereits darin zeigt, dass das Bundesamt für Sicherheit in der Informationstechnik eine eigene Informationsseite samt interaktivem Fragebogen bereitstellt, um Einrichtungen im Rahmen der Selbstklassifizierung zu unterstützen.[154] Somit gewinnt eine sorgfältig dokumentierte Betroffenheitsanalyse im Rahmen des Sicherheitsmanagements zunehmend an Bedeutung, um sowohl regulatorischen Anforderungen gerecht zu werden als auch mögliche Bußgelder zu vermeiden.

b) Angemessenheit

Gleichwohl wirft der weit gefasste Anwendungsbereich der NIS-2-Richtlinie berechtigte Fragen hinsichtlich seiner Angemessenheit und praktischen Umsetzbarkeit auf. Aus dogmatischer Sicht stellt sich insbesondere die Frage, ob die damit verbundene pauschale Ausweitung noch in einem angemessenen Verhältnis zum intendierten Schutzzweck steht. Die Richtlinie orientiert sich vorrangig an der Größe und Zugehörigkeit zu bestimmten Sektoren, nicht mehr daran, ob tatsächlich ein wesentlicher Dienst im operativen Sinne erbracht wird.[155]

Ein dezidierte Unklarheit betrifft weiterhin die fehlende ausdrückliche Regelung für konzerninterne Strukturen im Anwendungsbereich der NIS-2-Richtlinie. Die Richtlinie selbst (noch der aktuelle österreichische Umsetzungsvorschlag) enthalten klare Vorgaben dazu, wie Unternehmensgruppen oder Konzernverbünde zu behandeln sind.[156] So würden, bei einer strengen Auslegung, konzerninterne Rechenzentren unter die NIS-2-RL fallen, was jedoch weder praxisgerecht erscheint noch dem mutmaßlichen Willen des Gesetzgebers entspricht.[157]

Darüber hinaus verzichtet die NIS-2-Richtlinie weitgehend auf Schwellenwerte für den Tätigkeitsumfang, wodurch selbst geringfügige Aktivitäten in einem relevanten Sektor zur

[152] *Weihe*, CCZ 2024, 85 (91).
[153] *WKO*, Cybersicherheits-Richtlinie NIS 2, 02.07.2025.
[154] Vgl. *BSI*, NIS-2 Betroffenheitsprüfung.
[155] Im Ergebnis ebenso: *Neuwirth*, jusIT, 2024/2, S.6.
[156] *Jung/Dirnbauer*, Compliance Praxis 2025, 10, Heft 1, S. 10.
[157] *Jung/Dirnbauer*, Compliance Praxis 2025, 10, Heft 1, S. 11.

Anwendung der Richtlinie führen können. Dieser Ansatz führt insbesondere bei Mischbetrieben zu unverhältnismäßigen Compliance und Security Anforderungen.[158] Abschließend bleibt festzuhalten, dass die angestrebte unionsweite Harmonisierung maßgeblich von einem einheitlich verstandenen und angewendeten Anwendungsbereich bedingt wird. Ein Ziel, das angesichts der zahlreichen Auslegungs- und Umsetzungsspielräume auf mitgliedstaatlicher Ebene nur eingeschränkt erreicht werden dürfte.

II. Art. 20 NIS-2-RL: Governance

1. Auslegung der Norm

Globale Entwicklungen und aktuelle Herausforderungen schlagen sich zunehmend in Governance-Themen nieder. [159] Vor diesem Hintergrund ist die in Art. 20 Abs. 1 verankerte Managerhaftung als Bestandteil moderner Governance-Strukturen im Bereich der Cybersicherheit zu verstehen.

Die Norm verpflichtet die Leitungsorgane wesentlicher und wichtiger Einrichtungen zur aktiven Mitwirkung an der Umsetzung von Risikomanagementmaßnahmen und verankert damit eine rechtlich verbindliche Führungsverantwortung. Die NIS-2-Richtlinie bringt somit eine Verschärfung der bisherigen Rechtslage einher, insbesondere im Hinblick auf die persönliche Verantwortlichkeit der Unternehmensführung.[160] Während die NIS-1-Richtlinie keine ausdrückliche Regelung zur Verantwortlichkeit von Führungspersonen enthielt, führt Art. 20 Abs. 1 NIS-2-RL eine direkte Pflichtenbindung an die Leitungsebene ein. Die Leitungsorgane sind nach dem Wortlaut verpflichtet, die im Rahmen von Art. 21 ergriffenen Maßnahmen zum Risikomanagement zu billigen und deren Umsetzung zu überwachen. Zu konstatieren ist ebenfalls, dass der deutsche Gesetzgeber in § 38 BSIG-E einen weiteren Ansatz wählt, indem er – abweichend von der NIS-2-Richtlinie – nicht nur die Billigung, sondern ausdrücklich die Umsetzung der Maßnahmen durch das Leitungsorgan einbezieht.[161] Für die ordnungsgemäße Wahrnehmung dieser Pflichten können Führungsmitglieder unmittelbar zur Verantwortung gezogen werden, was eine konkrete Ausprägung der Rechenschaftspflicht darstellt.

Artikel 20 Absatz 2 NIS-2-RL konkretisiert die Pflichten der Leitungsorgane im Bereich der organisatorischen Verantwortung. Danach sind die Mitglieder der Leitungsorgane verpflichtet, an einschlägigen Schulungen im Bereich Cybersicherheit und Risikomanagement

[158] *Hessel/Schneider*, MMR 2025, 243.
[159] Im Ergebnis ebenso: *Herdegen*, Internationales Wirtschaftsrecht, 13. Auflage 2023, 3. Corporate Governance, Rn. 21.
[160] Im Ergebnis ebenso: *Humer*, Die Geschäftsleiterhaftung unter der NIS-2-RL.
[161] *Schmidt*, RDi 2024, 550 (554).

teilzunehmen, um ein angemessenes Verständnis der Sicherheitsanforderungen und Risiken ihrer Einrichtung zu erhalten.

Darüber hinaus sieht die Richtlinie vor, dass alle Beschäftigte regelmäßig in diesen Themenbereichen geschult werden. Damit soll ein organisationsweites Sicherheitsbewusstsein geschafft und die Fähigkeiten der Mitarbeitenden zur Vermeidung, Erkennung und Reaktion auf sicherheitsrelevante Vorfälle kontinuierlich gestärkt werden. Die konkrete Frequenz der Schulungsmaßnahmen für die Geschäftsleitung sowie die Teilnahmeverpflichtung einzelner Positionen wird in dem Wortlaut der Richtlinie nicht weiter konkretisiert. [162]

2. Angemessenheit im Kontext des Sicherheitsmanagement

a) Governance im Sicherheitsmanagement

Die unmittelbar verankerte Verantwortlichkeit der Leitungsebene markiert einen Paradigmenwechsel im Sicherheitsmanagement betroffener Einrichtungen. Cybersicherheit wird folglich nicht länger primär als technische Aufgabe auf operativer Ebene verstanden, sondern als strategische Führungsaufgabe in der obersten Unternehmensebene etabliert.[163] Im Rahmen von Einstellungsverfahren auf C-Level-Ebene – insbesondere in Asset intensiven Unternehmen – gewinnt ein grundlegendes Verständnis für Cybersecurity zunehmend an Bedeutung, sodass auch Personalverantwortliche entsprechende Kompetenzen bereits im Auswahlprozess systematisch berücksichtigen müssen.

Die in Art. 20 Abs. 2 NIS-2 verankerte Schulungspflicht der Leitungsebene entfaltet ihre rechtliche Wirksamkeit nur dann vollständig, wenn deren Erfüllung im Sinne einer dokumentierten Rechenschaftspflicht nachgewiesen werden kann. [164] Im Zuge dessen gewinnen Compliance- und Security-Tools, die Schulungsteilnahmen und Inhalte revisionssicher erfassen können, eine zentrale Bedeutung für die praktische Umsetzung dieser Verpflichtung.

b) Angemessenheit der Norm

Die in Artikel 20 NIS-2-Richtlinie eingeführte persönliche Verantwortung der Geschäftsleitung ist grundsätzlich zu begrüßen, da sie eine lang geforderte rechtliche Klarstellung hinsichtlich der Führungsrolle im Bereich der Cybersicherheit schafft.[165] Mithin wird nicht nur eine wesentliche Governance-Anforderung der ISO-27000-Normfamilie hinsichtlich der Top-Level-Management-Verantwortlichkeit verbindlich adressiert, sondern zugleich ein wichtiger Schritt in Richtung einer Harmonisierung zwischen regulatorischen Vorgaben und

[162] *Schmidt*, RDi 2024, 550 (555), *BSI*, Fragen und Antworten zu NIS-2, Frage 22.
[163] Vgl. *BSI*, NIS-2- Was tun? 2. Übernehmen Sie als Leitung die Verantwortung.
[164] Im Ergebnis ebenso: *Neuwirth*, jusIT, 2024/2, S.8.
[165] Die Geschäftsleitung haftet mit dem Privatvermögen für Verstöße gegen die Überwachungspflicht, vgl. *Degen/Emmert*, Elektronischer Rechtsverkehr, 3. Auflage 2025, § 9 IT- Sicherheit, Rn. 16.

internationalen Best-Practices vollzogen.[166] Die Richtlinie fördert folglich eine rechtliche Unifizierung sicherheitsrelevanter Anforderungen an Führungskräfte.

Artikel 20 wirft insbesondere zwei wesentliche Fragen auf: Zum einen bleibt offen, in welchen Abständen Schulungen für Mitglieder der Leitungsorgane stattfinden sollen – einheitliche Vorgaben zur Häufigkeit und inhaltlichen Tiefe fehlen bislang. Zum anderen bleibt der Begriff des „Leitungsorgans" unscharf definiert, was vor allem in komplexeren Unternehmensstrukturen zu Auslegungsfragen führt. Ein Vergleich der nationalen Umsetzungen in Deutschland und Österreich zeigt allerdings eine weitgehende inhaltliche Annäherung. In Deutschland legt § 2 Nr. 13 BSIG-E fest, dass unter der Geschäftsleitung jede natürliche Person zu verstehen ist, „die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist."[167] Im Mittelpunkt der Definition stehen somit die geschäftsführenden Organe mit Befugnis zur Außenvertretung.

Demgegenüber formuliert der österreichische Gesetzgeber im NISG 2024 einen leicht weiter gefassten Begriff. Dort wird das „Leitungsorgan", als eine oder mehrere natürliche Personen oder Verwaltungsorgane beschrieben, „die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung oder innerhalb der Einrichtung zur Überwachung der Geschäftsführung berufen sind."[168] Diese Formulierung bezieht ausdrücklich auch überwachende Organe wie etwa Aufsichtsräte mit ein.

Trotz dieser terminologischen Unterschiede zeigt sich eine funktionale Konvergenz beider Regelungen: Beide Rechtsordnungen zielen darauf ab, Verantwortungsträger in geschäftsführenden oder überwachenden Schlüsselpositionen in die Pflichtenstruktur der NIS-2-Richtlinie einzubinden.

Nach der Begründung des deutschen Gesetzgebers gelten Schulungen der Geschäftsleitung jedoch dann als *regelmäßig*, wenn sie mindestens im Abstand von drei Jahren durchgeführt werden. [169]

Ferner kann sich die offene Ausgestaltung der Governance-Vorgaben in Artikel 20 auch als Vorteil erweisen, da sie technologieneutrale Handlungsspielräume eröffnet, die insbesondere

[166] Ohne die aktive Unterstützung und uneingeschränkte Rückendeckung des Top-Managements ist der Aufbau und nachhaltige Betrieb eines Informationssicherheits-Managementsystems kaum realisierbar – insbesondere im Hinblick auf die erforderlichen finanziellen und personellen Ressourcen. *Brenner*, Praxishandbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 4. Auflage, S. 43.
[167] *Heinelt/Dittrich/Basar*, CB 2025, 151 (154).
[168] § 3 Nr. 11 NISG 2024.
[169] *Schmidt*, RDi 2024, 550 (555), *BSI*, Fragen und Antworten zu NIS-2, Frage 22.

bei der Ausgestaltung von Schulungsmaßnahmen und der praktischen Umsetzung der Rechenschaftspflicht entscheidend genutzt werden können.

III. Art. 21 NIS-2-RL: Risikomaßnahmen im Bereich der Cybersicherheit

1. Auslegung der Norm

Das gemäß Artikel 21 NIS-2 verpflichtend einzuführende Risikomanagementsystem in wesentlichen und wichtigen Einrichtungen hat sich an mehreren Vorgaben zu orientieren. Artikel 21 NIS-2-Richtlinie enthält zentrale Mindestanforderungen[170] an TOM, die in ihrer Systematik und Zielrichtung an Artikel 32 DSGVO erinnern und gewissermaßen eine sektorspezifische Parallelvorschrift darstellen. Viele der in Artikel 21 NIS-2 aufgeführten Begrifflichkeiten – wie der Stand der Technik, Implementierungskosten oder Verhältnismäßigkeit – wurden bereits im Rahmen der Auslegung des Artikels 32 DSGVO eingehend diskutiert, sodass Doppelungen bei der nachfolgenden Eruierung möglichst vermieden werden sollen.

a) „gefahrenübergreifenden Ansatz“

Eine zentrale Neuerung von Artikel 21 Abs. 2 NIS-2-Richtlinie besteht in der unmittelbaren Verpflichtung zur Anwendung eines gefahrenübergreifenden Ansatzes, der nicht nur informationstechnische, sondern auch physische und organisatorische Gefahrenquellen einbezieht. Die Umsetzung dieses sogenannten *All-Hazards-Ansatzes* verpflichtet mithin dazu, IT-Systeme nicht nur gegen digitale Bedrohungen wie Hackerangriffe, sondern auch gegen physische Gefahren wie Diebstahl, Feuer, Stromausfälle oder Naturkatastrophen abzusichern (unter Einbeziehung sowohl interner als auch externer Risikofaktoren).[171] Folglich wird er als integraler Bestandteil bei der Bewertung der Angemessenheit von Schutzmaßnahmen zwingend zu berücksichtigen sein, da wirksame Vorkehrungen nur dann vorliegen, wenn sie, unter Einbeziehung des Stands der Technik sowie einschlägiger europäischer und internationaler Normen, ein ausreichendes Schutzniveau gegenüber allen relevanten Gefährdungen gewährleisten.[172]

Diese Erweiterung des Blickwinkels bietet die Chance, Informationssicherheit aus ihrer stark IT-fokussierten Nische herauszulösen und als unternehmensweites Querschnittsthema zu etablieren, im Einklang mit dem Grundverständnis internationaler Standards wie der ISO/IEC 27001, die Informationssicherheit stets im Kontext gesamthafter Geschäftsprozesse verortet.[173]

---

[170] „zumindest Folgendes umfassen“ – Art. 21 Abs. 2 NIS-2-RL.
[171] *Reiter/Heidinger/Gstrein*, Medien und Recht 2023/188, S. 191.
[172] Im Ergebnis ebenso: *Nink*, ZfPC 2025, 58 (65).
[173] *Neuwirth*, jusIT, 2024/2, S.8.

b) Regelungskatalog

Aus dem All-Hazard-Ansatz geht hervor, dass kein absolutes Sicherheitsniveau gefordert wird, sondern ein risikoadäquater Schutz, der auf einer vorgelagerten Risikoabschätzung basiert.[174] Diese Regelung trägt dem Umstand Rechnung, dass die Pflicht zum Risikomanagement keine Erfolgs-, sondern eine Bemühens-Verpflichtung darstellt, da das Stadium eines umfassenden Schutzniveaus kaum realisierbar erscheint.[175]
Die im Wortlaut gelisteten Maßnahmen sind im Sinne einer vollständig zu erfüllenden Checkliste zu verstehen.[176]
Angesichts des überschaubaren Maßnahmenkatalogs erscheint eine systematische Darstellung der einzelnen Vorgaben sachgerecht:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- Bewältigung von Sicherheitsvorfällen;
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement; Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.[177]

Obgleich in Fachliteratur und medialen Diskursen ein verschärftes Risikomanagement im Bereich der Cybersicherheit gefordert wird, ist der in Art. 21 Abs. 2 NIS 2-Richtlinie aufgeführte Maßnahmenkatalog in Summe eher als Grundgerüst einzuordnen. Viele der aufgeführten Vorgaben spiegeln grundlegende Sicherheitsmaßnahmen wider, die – gemessen an etablierten Standards – vor allem den Kern eines risikoorientierten Schutzkonzepts bilden. Vorkehrungen wie ein Back-Up-Management, Schulungen sowie Kryptografie wurden bereits im Rahmen der Ausdifferenzierung der DSGVO dargelegt und lassen sich ebenfalls unmittelbar

[174] Hessel/Callewaert/Schneider: RDi 2024, 208 (212).
[175] *Heinelt/Dittrich/Basar*, CB 2025, 151 (153).
[176] *Nink*, ZfPC 2025, 58 (64).
[177] Art. 21 Abs. 2 NIS-2-RL.

im Maßnahmenkatalog der ISO27001 Norm finden. Folglich werden zahlreiche Sicherheitsmaßnahmen bereits im Schutzportfolio der Adressaten zu finden sein. Ein besonderer Stellenwert kommt nun der Sicherheit der Lieferkette zu. Gemäß Art. 21 Abs. 2 lit. d) NIS-2-Richtlinie sind sicherheitsbezogene Aspekte der Beziehungen zwischen einer Einrichtung und ihren unmittelbaren Anbietern oder Diensteanbietern explizit in die Schutzmaßnahmen einzubeziehen. Die Richtlinie verweist damit auf die Notwendigkeit, auch externe Abhängigkeiten systematisch in die Risikoanalyse einzubeziehen. Allerdings bleibt offen, wie weitreichend diese Analysepflicht in Bezug auf mehrstufige Lieferketten zu verstehen ist.[178] Nach der Gesetzesbegründung, die zugleich den Wortlaut von Art. 21 Abs. 3 NIS-2-Richtlinie aufgreift, zählen etwa vertragliche Regelungen mit Zulieferern und Dienstleistern zu geeigneten Maßnahmen.[179] Diese sollen insbesondere Aspekte des Risikomanagements, der Bewältigung von Cybersicherheitsvorfällen, des Patchmanagements sowie die Berücksichtigung von Empfehlungen des BSI im Hinblick auf die eingesetzten Produkte und Dienstleistungen umfassen.[180] Darüber hinaus sieht Art. 21 Abs. 2 lit. j) NIS-2-Richtlinie vor, dass Einrichtungen bei der Umsetzung ihrer Sicherheitsmaßnahmen auch Lösungen zur Multi-Faktor-Authentifizierung, kontinuierlichen Authentifizierung sowie zur Absicherung von Notfallkommunikationssystemen in angemessener Weise berücksichtigen sollen.[181] Eine gewisse Inkonsistenz ergibt sich unmittelbar aus dem Wortlaut, da in der deutschen Sprachfassung der Zusatz „wo angemessen“ fehlt. Dies könnte zu der (möglicherweise unzutreffenden) Annahme führen, dass die Implementierung von Multi-Faktor-Authentifizierung künftig für die betroffenen Einrichtungen generell verpflichtend sei.[182]

Weiterhin ist unter dem Management von Anlagen vorrangig das Asset Management zu verstehen, also die systematische Erfassung und Verwaltung physischer sowie digitaler Werte, um Sicherheitsrisiken frühzeitig identifizieren und angemessen steuern zu können, im Sinne des Art. 21 Abs. 2 lit. i) NIS-2-RL.[183]

Ferner ist davon auszugehen, dass die Risikoexposition bei Betreibern kritischer Anlagen am höchsten ist und über besonders wichtige Einrichtungen bis hin zu wichtigen Einrichtungen

[178] *Neuwirth*, jusIT, 2024/2, S.8.
[179] *Schmidt*, RDi 2024, 550 (554).
[180] *Schmidt*, RDi 2024, 550 (554).
[181] *Hessel*, in: Marly, Praxishandbuch Softwarerecht, 8. Auflage 2024, Rn. 72.
[182] In der englischen Fassung findet sich die Risikoorientierung wieder („where appropriate“); *Schmidt*, RDi 2024, 550 (554).
[183] Vgl. A.8 „Verwaltung der Werte“ *Maseberg/Michael/Müller/Seidel*, in: Kipker, Cybersecurity, 2. Auflage 2023, Rn. 85. Im Ergebnis ebenso: jusIT, 2024/2, S.9.

sukzessive abnimmt, sodass ergänzende Sicherheitsmaßnahmen entsprechend abgestuft werden können.[184]

2. Angemessenheit im Kontext des Sicherheitsmanagement

a) Der Regelungskatalog im Sicherheitsmanagement

Erwägungsgrund 79 der NIS-2-Richtlinie betont die Notwendigkeit eines umfassenden Risikomanagementansatzes, der sowohl technische als auch physische Sicherheitsaspekte umfasst und ausdrücklich auf internationale Standards wie die Normenreihe ISO/IEC 27000 verweist. Vor diesem Hintergrund ist sich die Fachliteratur weitgehend einig, dass der Aufbau sowie die fortlaufende Aufrechterhaltung eines Informationssicherheitsmanagementsystems den zentralen ersten Schritt zur Umsetzung der Anforderungen aus Art. 21 NIS-2-RL darstellt.[185] Die ISO/IEC 27001 beschreibt ein systematisches Managementsystem zur Gewährleistung der Informationssicherheit. Das Sicherheitsmanagement wird sich mithin unabdingbar dem sogenannten PDCA-Zyklus (Plan – Do – Check – Act) bedienen müssen, der einen iterativen abbildet: Zunächst erfolgt die Planung und Initiierung des ISMS, anschließend die Umsetzung der definierten Maßnahmen, gefolgt von deren regelmäßiger Überprüfung und anschließender Optimierung.[186]

Sofern Governance-Strukturen und Sicherheitsmaßnahmen bereits etabliert sind, bietet sich alternativ die Durchführung einer Delta-Analyse an, um bestehende Abweichungen zu den Anforderungen der NIS-2-Richtlinie systematisch zu identifizieren.

Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt in diesem Zusammenhang auch die Durchführung des *CyberRisikoChecks*, bei dem Unternehmen in einem strukturierten Interview durch einen IT-Dienstleister hinsichtlich 27 Anforderungen aus sechs Themenbereichen bewertet werden, um eine fundierte Einschätzung ihres aktuellen IT-Sicherheitsniveaus zu erhalten sowie konkrete, nach Dringlichkeit priorisierte Handlungsempfehlungen inklusive möglicher staatlicher Fördermaßnahmen zu erhalten.[187]

Ein ganzheitlicher Ansatz ist auch im Kontext der NIS-2-Richtlinie unerlässlich, da deren Anforderungen nicht isoliert zu betrachten sind, sondern abteilungsübergreifende, personelle und rechtliche Schnittstellen betreffen – eine adäquate Kommunikation sowie gezielte

[184] Im Ergebnis ebenso: *Schmidt*, RDi 2024, 550 (554).
[185] *Schmidt*, RDi 2024, 550 (553), *Degen/Emmert*, Elektronischer Rechtsverkehr, 3. Auflage 2025, § 9 IT-Sicherheit, Rn. 14.
[186] *Maseberg/Michael/Müller/Seidel*, in: Kipker, Cybersecurity, 2. Auflage 2023, Kapitel 5. Rn. 70.
[187] *BSI*, CyberRisikoCheck, Durchführung des CyberRisikoChecks.

Schulungen sind daher entscheidend, um alle relevanten Stakeholder einzubinden und eine nachhaltige Sicherheitskultur im Unternehmen sicherzustellen.[188]

b) Angemessenheit der Norm

Die Etablierung eines klar formulierten Minimums an Maßnahmen in Art. 21 der NIS-2-Richtlinie ist positiv zu bewerten, da dadurch eine einheitlichere Auslegung und Umsetzung der Sicherheitsanforderungen im EU-Binnenmarkt gefördert wird. Durch die explizite Benennung technischer, operativer und organisatorischer Maßnahmen entsteht für betroffene Einrichtungen eine verbindlichere Orientierungshilfe, die nicht nur die Transparenz erhöht, sondern auch einen wichtigen Beitrag zur Harmonisierung des Cybersicherheitsniveaus innerhalb der Union leistet.

Trotz der begrüßenswerten Einführung bleibt die Natur der Richtlinie als solche nicht ohne Herausforderungen. Als europarechtliches Instrument bedarf eine Richtlinie der nationalen Umsetzung durch die Mitgliedstaaten, was zwangsläufig zu einem gewissen Maß an Interpretationsspielräumen und Verzögerungen führt. Diese Fragmentierung kann der intendierten Harmonisierung des Cybersicherheitsniveaus entgegenwirken.

Dies zeigt sich exemplarisch in der aktuellen Situation in Deutschland: Wie das BSI in seinen FAQ betont, kann es vor Abschluss des nationalen Gesetzgebungsverfahrens nur sehr eingeschränkt Auskünfte zu den künftigen Regelungen des neuen BSI-Gesetzes geben und verweist auf das Bundesministerium des Innern und für Heimat (BMI) als zuständige Behörde.[189] Unternehmen sind somit in einer Phase erhöhter Unsicherheit auf sich selbst gestellt und können sich allenfalls mit allgemeinen Fragen zur Cyber- und Informationssicherheit an das BSI wenden – eine individuelle rechtliche Beratung erfolgt nicht.[190] Trotz verzögerter nationaler Umsetzung in Deutschland und Österreich sollte laut einer Stimme aus der Literatur keine abwartende Haltung eingenommen werden: Die kommenden Cybersicherheitsgesetze werden sich weitgehend an der NIS-2-Richtlinie orientieren und nur wenige Überraschungen bereithalten.[191]

Weitere Kritikpunkte beziehen sich dezidiert auf die Schwächen der deutschen Fassung. So wird etwa „Asset Management“ unglücklich als „Management von Anlagen“ wiedergegeben – eine Formulierung, die dem etablierten Begriff der Informationssicherheit nicht gerecht wird.[192] Ebenso fehlt im Zusammenhang mit der Multi-Faktor-Authentifizierung der einschränkende

[188] *Schatzlmair*, Compliance Praxis 2025, Heft 1, S. 5.
[189] *BSI*, Fragen und Antworten zu NIS-2, Frage 4.
[190] *BSI*, Fragen und Antworten zu NIS-2, Frage 4.
[191] Vgl. § 30 BSIG-E, *Oberndorfer*, Compliance Praxis 2025, Heft 1, S. 5.
[192] *Neuwirth*, jusIT, 2024/2, S.8.

Zusatz „wo angemessen“, wodurch eine risikobasierte Auslegung der Maßnahme (wie in der englischen Fassung vorgesehen) in der deutschen Version nicht eindeutig erkennbar ist.[193]

IV. Art. 23 NIS-2-RL: Berichtspflichten

1. Auslegung der Norm

Ebenso wie die DSGVO sieht auch die NIS-2-Richtlinie verpflichtende Meldepflichten bei Sicherheitsvorfällen vor, um eine schnelle Reaktion und wirksame Schadensbegrenzung zu gewährleisten.

Art. 23 der NIS-2-Richtlinie verlangt bei erheblichen Sicherheitsvorfällen ein mehrstufiges Meldeverfahren: Eine Erstmeldung innerhalb von 24 Stunden, einen weiterführenden Bericht binnen 72 Stunden sowie einen Abschlussbericht nach einem Monat.[194] Erfolgen Rückfragen seitens der Aufsichtsbehörde oder ist der Vorfall nach einem Monat noch nicht abschließend geklärt, ist eine Zwischen- bzw. eine Fortschrittsmeldung statt des Abschlussberichts vorzulegen.[195] Eine Meldepflicht besteht gemäß Art. 23 Abs. 3 nur, wenn ein erheblicher Sicherheitsvorfall vorliegt, der entweder schwerwiegende Betriebsstörungen der betroffenen Dienste oder finanzielle Verluste für das Unternehmen verursachen kann oder wenn natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt werden könnten.[196] Für die NIS-2-Richtlinie lässt sich in Anlehnung an die Durchführungsverordnung der Kommission vom 17. Oktober 2024 festhalten, dass ein erheblicher Sicherheitsvorfall insbesondere dann anzunehmen ist, wenn dieser zu erheblichen finanziellen Verlusten über 500.000 EUR oder mehr als 5 % des Jahresumsatzes führen kann, die Gesundheit oder das Leben natürlicher Personen gefährdet oder eine wesentliche Beeinträchtigung der Verfügbarkeit erbrachter Dienste verursacht.[197]

Im Unterschied zur DSGVO folgt die Meldepflicht nach der NIS-2-Richtlinie somit einem gestuften Meldeverfahren mit deutlich differenzierteren Anforderungen an Inhalt und Frist.

2. Angemessenheit im Kontext des Sicherheitsmanagement

a) Die Berichtspflichten im Sicherheitsmanagement

Die im Kontext der DSGVO beschriebenen Herausforderungen und Handlungserfordernisse im Sicherheitsmanagement lassen sich im Grundverständnis analog auf die Meldepflichten nach

[193] *Neuwirth*, jusIT, 2024/2, S.8.
[194] *Grosmann/Michel*, ZD 2025, 250 (253).
[195] *Grosmann/Michel*, ZD 2025, 250 (253).
[196] *Steiner/Schmiedlechner*, Compliance Praxis 2025, 7, Heft 1, S. 8.
[197] Nur für ausgewählte Sektoren definiert, kann jedoch auch als Anhaltspunkt für andere Sektoren dienen; *Steiner/Schmiedlechner,* Compliance Praxis 2025, 7, Heft 1, S. 9.

der NIS-2-Richtlinie übertragen. Auch hier steht ein effektives und risikoorientiertes Incident-Management im Mittelpunkt, das durch klare Verantwortlichkeiten, technische Überwachungssysteme und abgestimmte Kommunikationsprozesse[198] getragen werden muss. Der Grundtenor bleibt dabei derselbe: Nur ein vorausschauendes, strukturiertes und abteilungsübergreifend koordiniertes Sicherheitsmanagement ermöglicht eine fristgerechte Meldung, wirksame Schadensbegrenzung und die Einhaltung regulatorischer Vorgaben.

Ein besonderes Augenmerk im Rahmen der NIS-2-Berichtspflichten liegt auf der eigenverantwortlichen Bewertung seitens der betroffenen Einrichtung, ob ein erheblicher Sicherheitsvorfall vorliegt und somit eine Meldepflicht besteht. Die Schwierigkeit beginnt bereits bei der Erkennung potenziell meldepflichtiger Vorfälle, da diese nicht immer klar identifizierbar sind und sich erst durch wiederholtes Auftreten als relevant erweisen.[199]

b) Angemessenheit

Die Einführung einer gestuften Meldepflicht im Rahmen der NIS-2-Richtlinie ist als eine positive Entwicklung zu bewerten. Während ein gestuftes Vorgehen bislang lediglich in Teilen der Literatur befürwortet wurde, erfolgt nun eine klare gesetzliche Verankerung.[200] Dies trägt dem berechtigten Interesse an schnellen Informationsflüssen Rechnung und schafft zugleich Transparenz.[201]

Wie bereits im Kontext der Datenschutz-Grundverordnung diskutiert, birgt auch die Verpflichtung zur Meldung nach NIS-2 das Risiko, dass Behörden auf Grundlage der offengelegten Informationen Ermittlungen aufnehmen oder Bußgeldverfahren einleiten. Das Verhältnis der Pflicht zur Meldung von erheblichen Vorfällen zum rechtsstaatlich verankerten Grundsatz der Selbstbelastungsfreiheit (nemo tenetur se ipsum accusare) ist bislang nicht abschließend geklärt. Im Zuge dessen besteht ein Spannungsverhältnis zwischen der Pflicht zur transparenten Berichterstattung einerseits und dem Schutz vor Selbstbelastung andererseits.[202]

In der praktischen Anwendung ist bislang offen, in welchem Umfang Meldungen unter NIS-2 tatsächlich privilegiert und vor behördlicher Verwertung geschützt sind, insbesondere dann, wenn sich aus der Meldung konkrete Hinweise auf Verstöße ergeben. [203]

Obwohl die NIS-2-Richtlinie auf eine Harmonisierung der Cybersicherheitsanforderungen abzielt, tritt gerade im Bereich der Meldepflichten eine Aufweichung dieses Vereinheitlichungsanspruchs zutage. Dies betrifft insbesondere die Definition des „erheblichen

[198] *Grosmann/Michel* plädieren für ausdifferenzierte Meldekanäle*; Grosmann/Michel*, ZD 2025, 250 (253).
[199] *Steiner/Schmiedlechner,* Compliance Praxis 2025, 7, Heft 1, S. 8.
[200] *Kipker/Dittrich,* MMR 2023, 481 (484).
[201] *Kipker/Dittrich,* MMR 2023, 481 (484).
[202] Im Ergebnis ebenso: *Hessel/Callewaert/Schneider*: RDi 2024, 208 (213).
[203] Im Ergebnis ebenso: *Hessel/Callewaert/Schneider*: RDi 2024, 208 (213).

Sicherheitsvorfalls“, welche den nationalen Gesetzgebern einen beträchtlichen Auslegungsspielraum überlässt. Die nationalen Umsetzungsgesetze differieren hinsichtlich der Voraussetzungen, unter denen ein Vorfall als erheblich zu qualifizieren ist. Der deutsche Gesetzgeber führt hierbei eine inhaltliche Erweiterung der Meldepflichten ein, insbesondere durch die ausdrückliche Einbeziehung immaterieller Schäden in die Kriterien der Erheblichkeit. Unklar bleibt jedoch, nach welchen Maßstäben diese Schwelle im Einzelfall zu bestimmen ist.[204] In Ungarn geht das bereits in Kraft getretene Umsetzungsgesetz ebenfalls weit: Dort kann bereits ein einzelnes unerwartetes Ereignis, das etwa einen vorübergehenden Verlust an Vertraulichkeit oder Funktionalität zur Folge hat, eine Meldepflicht auslösen. [205] Österreich wiederum wählt im Entwurf zum NISG 2024 eine breit gefasste, auslegungsbedürftige Definition des Begriffs „Erheblichkeit“. [206]

V. Informationssicherheitsbeauftragter (ISB)

Im Gegensatz zur DSGVO, die die Benennung eines Datenschutzbeauftragten vorsieht, enthält die NIS-2-Richtlinie keine ausdrückliche Pflicht zur Bestellung eines Informationssicherheitsbeauftragten. In den Entwürfen des deutschen NIS-2-UmsuCG ist die Bestellung eines ISB in §§ 45, 46 BSIG-E lediglich für Einrichtungen der Bundesverwaltung vorgesehen.[207] Gleichwohl ist davon auszugehen, dass die Funktion des ISB auch in der Unternehmenspraxis zunehmend an Bedeutung gewinnen wird. Spätestens im Kontext internationaler Standards wie der ISO/IEC 27001 gewinnt diese Funktion an zentraler Bedeutung: Die Norm sieht eine klare Allokation von Verantwortlichkeiten für Informationssicherheit vor und verlangt eine kontinuierliche Steuerung sowie Überprüfung der Sicherheitsmaßnahmen. [208]

VI. Zwischenfazit

Auch die die NIS-2-Richtlinie fordert, in Anbetracht der ersten Forschungsfrage, ein umfassendes und sektorspezifisches Sicherheitsmanagement, das über die Regelungstiefe ihrer Vorgängerrichtlinie deutlich hinausgeht. Im Zentrum stehen dabei die Ausweitung des Anwendungsbereichs, die verbindliche Führungsverantwortung sowie ein verbindlicher Maßnahmenkatalog zur Risikominimierung.

---

[204] *Kipker/Dittrich,* MMR 2023, 481 (484).
[205] *Steiner/Schmiedlechner*, Compliance Praxis 2025, 7, Heft 1, S. 8.
[206] Vgl. § 35 NISG 2024.
[207] *Grosmann/Michel*, ZD 2025, 250 (253).
[208] Im Ergebnis ebenso: *Schmidl*, Corporate Compliance, 4. Auflage 2024, Rn. 276.

Die Vernetzung mit internationalen Standards wie ISO/IEC 27001 zeigt den normativen Anspruch, Cybersicherheit ganzheitlich adressieren und Governance strukturell zu verankern. Insbesondere durch die Pflichtenbindung auf Leitungsebene (Art. 20) sowie durch spezifische Berichtspflichten (Art. 23) wird Sicherheitsmanagement zur strategischen Führungsaufgabe erhoben und durch Elemente der Rechenschaftspflicht flankiert.

Die Angemessenheit der Richtlinie ist differenziert zu bewerten. Positiv fällt insbesondere ins Gewicht, dass ein Katalog von Mindestanforderungen geschaffen wird, die als Grundlage eines Maßnahmenportfolios dient. Dies trägt zur Harmonisierung des Sicherheitsniveaus innerhalb der EU bei und bildet zugleich eine praxisnahe Orientierung für betroffene Einrichtungen. Die Etablierung einheitlicher Schutzstandards kann somit als Fortschritt im europäischen Cybersicherheitsrecht gewertet werden.

Gleichzeitig zeigen sich jedoch strukturelle Unschärfen: Der weite Anwendungsbereich, das Fehlen klarer Schwellenwerte sowie nationale Abweichungen (etwa bei der Definition erheblicher Vorfälle oder der Reichweite von Schulungspflichten) erschweren weitere Harmonisierungen. Die notwendige Konkretisierung durch nationale Gesetzgebungsakte verzögert zudem die Rechtssicherheit und schafft Rechtsunsicherheiten für die betroffenen Einrichtungen.

Insgesamt lässt sich jedoch festhalten, dass die NIS-2-Richtlinie einen paradigmatischen Wandel im Sicherheitsmanagement wesentlicher und wichtiger Einrichtungen markiert. Sie legt einen soliden, wenn auch noch nicht vollständig harmonisierten, Rahmen für Cybersicherheitsanforderungen im europäischen Binnenmarkt. Die Effektivität ihrer Umsetzung wird jedoch davon bedingt werden, inwiefern die Mitgliedstaaten etwaige Unklarheiten durch kohärente und praxisorientierte nationale Regelungen konkretisieren.

D. Synergien und Spannungsfelder zwischen DSGVO und NIS-2-RL

In diesem Abspann wird die zweite Forschungsfrage adressiert: Welche Synergien und potenziellen Spannungsfelder bestehen zwischen den Vorgaben der DSGVO und der NIS-2-RL? Ziel ist es, die Interdependenzen beider Regelungswerke systematisch zu analysieren, etwaige Überschneidungen sowie Divergenzen herauszuarbeiten und diese hinsichtlich ihrer praktischen Auswirkungen auf betroffene Einrichtungen zu bewerten.

I. Gemeinsamer Anwendungsbereich

Zunächst erscheint es unabdingbar, die regulatorische Schnittstelle im Anwendungsbereich beider Regelwerke für die betroffenen Einrichtungen zu identifizieren.

Unter Berücksichtigung der weiten Anwendbarkeit der DSGVO auf die Verarbeitung personenbezogener Daten sowie der sektoral breit gefassten Geltung der NIS-2-Richtlinie für zahlreiche systemrelevante Einrichtungen, ergibt sich eine substanzielle Schnittmenge beider Regime.[209]

Einrichtungen, die wesentliche oder wichtige Dienste erbringen und gleichzeitig personenbezogene Daten verarbeiten, fallen folglich regelmäßig in den Geltungsbereich beider Regelwerke. Folglich erfolgt eine exemplarische Auflistung:

- *Gesundheitseinrichtungen*: Sie verarbeiten besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) und sind zugleich als wesentliche Einrichtungen im Sinne der NIS-2-RL eingestuft.[210]
- Finanz- und Kreditinstitute: Diese unterliegen regelmäßig den datenschutzrechtlichen Pflichten bei der Verarbeitung von Kundendaten als auch den Cybersicherheitsanforderungen im Rahmen der NIS-2-RL.[211]
- Öffentliche Verwaltungen und Behörden: Sie verarbeiten personenbezogene Daten ihrer Bürger*innen und gelten je nach staatlicher Ebene und kritischer Relevanz ebenfalls als Einrichtungen im Sinne der NIS-2-RL.[212]
- Digitaldienstleister (z. B. Cloud-Provider, Rechenzentren, Domain-Registrare): Diese sind regelmäßig Auftragsverarbeiter im Sinne der DSGVO (Art. 28 DSGVO) und werden unter der NIS-2-Richtlinie ebenfalls reguliert.[213]

Eine isolierte Betrachtung von Datenschutz und Cybersicherheit ist für diese Akteure daher nicht zielführend. Vielmehr müssen Compliance- und Sicherheitsanforderungen stets integrativ berücksichtigt werden. Diese enge Kooperation schafft auch bedeutsame Synergieeffekte: Die Bündelung von Fachwissen und Ressourcen in den betroffenen Einrichtungen ermöglicht einen holistischen Ansatz und erhöht die Effizienz bei der Umsetzung gesetzlicher Anforderungen. Da in diesen Kontext auch mögliche Divergenzen kristallisiert werden sollen, ist die Size-Cap-Regelung zu nennen. Während die NIS-2-RL[214] einen pragmatischen Entlastungsansatz verfolgt, erscheint der Entlastungswille der DSGVO[215] eher theoretischer Natur, da die normierte Rückausnahme nach DSGVO den eigentlichen Schwellwert systematisch konterkariert.

---

[209] Anwendungsbereich der DSGVO: *Ernst*, in: Paal/Pauly, 3. Auflage 2021, Rn. 2-10. Anwendungsbereich der NIS-2-RL: *Hessel/Callewaert/Schneider*, RDi 2024, 208 (209).

[210] Anhang I NIS-2-RL (Sektoren hoher Kritikalität); *Gutbrunner*, Anwendungsbereich NIS-2-RL, Lexis Briefings.

[211] Anhang I NIS-2-RL (Sektoren hoher Kritikalität); *Gutbrunner*, Anwendungsbereich NIS-2-RL, Lexis Briefings.

[212] Anhang I NIS-2-RL (Sektoren hoher Kritikalität); *Gutbrunner*, Anwendungsbereich NIS-2-RL, Lexis Briefings.

[213] Anhang I und II NIS-2-RL (Sektoren hoher Kritikalität sowie sonstige kritische Sektoren); *Gutbrunner*, Anwendungsbereich NIS-2-RL, Lexis Briefings.

[214] Die NIS-2-Richtlinie erfasst Einrichtungen, die mindestens die Voraussetzungen für ein mittleres Unternehmen gemäß Artikel 2 des Anhangs der Empfehlung 2003/361/EG erfüllen; *Hessel/Schneider*, MMR 2025, 243.

[215] Die einzige Size-Cap-Regelung in der DSGVO betrifft eine mögliche Ausnahme zur Erstellung des VVT nach Art. 30 DSGVO. Es erscheint zweifelhaft, ob die von der Kommission intendierte Entlastung von KMU tatsächlich erreicht wird, da zwar die Rückausnahme für besondere Datenkategorien nachvollziehbar ist, die Beschränkung auf lediglich gelegentliche Verarbeitungen jedoch faktisch jede regelmäßige Verarbeitung – wie etwa die monatliche Lohn- und Gehaltsabrechnung ab dem ersten Beschäftigten – von der Ausnahme ausnimmt und damit den Entlastungsansatz weitgehend konterkariert; *Ehmann/Selmayr*, Datenschutz-Grundverordnung, Art. 30, 3. Auflage 2024, Rn. 6.

II. Governance

Ein zentrales Bindeglied zwischen der DSGVO und der NIS-2-Richtlinie stellt das Konzept der Governance dar.

Wie herausgearbeitet, verpflichtet Art. 20 NIS-2-RL die Leitungsorgane wesentlicher und wichtiger Einrichtungen zur Billigung und Überwachung der Maßnahmen gemäß Art. 21 NIS-2-RL. Diese Entwicklung steht im engen Zusammenspiel zur Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO. Beide Regulierungsansätze verlassen somit das klassische Muster behördlicher Steuerung („Command-and-Control") und verlangen vielmehr, dass die Einhaltung aktiv nachgewiesen wird.[216]

Mithin wird das Prinzip der „Accountability" in der obersten Unternehmensebene verankert sowie eine Governance-Struktur geschaffen, die Sicherheit und Compliance als integrale Managementverantwortung versteht. Im Zuge dessen wird jedoch auch ein deutlicher Unterschied klar: Während die DSGVO lediglich mittelbar über das Prinzip der Rechenschaftspflicht auf eine Beteiligung des Managements abzielt, etabliert Art. 20 NIS-2-RL eine explizite Rechtsverpflichtung der Leitungsgremien.

Auch im Rahmen der Schulungspflicht der relevanten Stakeholder ergibt sich eine inhaltliche Konvergenz. Zwar enthält die DSGVO keine ausdrücklich kodifizierte Verpflichtung des Verantwortlichen zur Durchführung von Schulungsmaßnahmen, jedoch ergibt sich diese indirekt aus verschiedenen Normen.[217]

So kann eine Schulungspflicht aus. Art. 32 Abs. 4 DSGVO sowie Art. 39 DSGVO (Pflichten des Datenschutzbeauftragten) indirekt entnommen werden.[218] Art. 20 Abs. 2 NIS-2-RL verpflichtet ausdrücklich die Mitglieder der Leitungsorgane zu einschlägigen Schulungen im Bereich Cybersicherheit. Diese gemeinsame Anforderung schafft die Grundlage für eine einheitliche Awareness-Kultur, die sowohl datenschutz- als auch cybersicherheitsbezogene Risiken adressiert.

Das Grundgerüst im operativen Sinne wird von einer die IT-Richtlinie abgebildet werden. Die Richtlinie bildet das organisatorische Fundament zur Umsetzung sowohl interner sowie externer Compliance Anforderungen an die IT-Sicherheit und den Datenschutz ab. Sie gewährleistet eine systematische Darlegung aller Assets – einschließlich Organisation, Technik, Personal und Infrastruktur.[219] Die IT-Richtlinie adressiert idealerweise ebenfalls

[216] Hinsichtlich der DSGVO: *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 52.
[217] *Grosmann/Michel*, ZD 2025, 250 (252).
[218] *Grosmann/Michel*, ZD 2025, 250 (252). Paal, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Rn. 5.
[219] *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, 40. EL März 2025, Rn. 411.

grundlegende Säulen der DSGVO, etwa Grundprinzipien der DSGVO, Meldeprozesse bei Datenpannen sowie die adäquate Abhandlung von Betroffenenanfragen.[220]

III. Sicherheitsmanagement

Trotz unterschiedlicher Zielrichtungen zeigen sich in der konkreten Ausgestaltung des Sicherheitsmanagements erhebliche inhaltliche Überschneidungen, aber auch unterschiedliche Akzentsetzungen.

1. Gemeinsame Grundstrukturen

Sowohl Art. 32 DSGVO als auch Art. 21 NIS-2-RL umfassen umfangreiche Anforderungen an die Implementierung von TOM, die sich an klassischen IT-Sicherheitszielen wie Vertraulichkeit, Integrität und Verfügbarkeit orientieren. Die Regelungssystematik beider Normen beruht auf einer kontextabhängigen Risikoabschätzung, unter Berücksichtigung des Stands der Technik, der Eintrittswahrscheinlichkeit und Schwere möglicher Schadensszenarien sowie ökonomischer Zumutbarkeit.[221]
Dies ermöglicht es betroffenen Einrichtungen, ein zentrales Maßnahmenportfolio aufzubauen, das gezielt internen, wie externen Compliance-Anforderungen zugeordnet werden kann. Weiterhin öffnen sich beide Regelwerke den international anerkannten Standards der Informationstechnik (ISO/IEC 27001), was die Grundlage für eine normative Unifizierung von Datenschutz und Cybersicherheit im Rahmen eines integrierten Sicherheitsmanagements schafft.[222] Folglich ergeben diese Entwicklungen, dass ein Sicherheitsmanagementsystem so etabliert werden muss, dass die kontinuierliche Überwachung, Anpassung und Dokumentation sichergestellt werden kann (im Sinne des international etablierten Plan – Do – Check – Act-Zyklus).[223] Die systematische Umsetzung dieses Zyklus wird damit zu einem konvergenten Erfüllungsinstrument beider Regime.
Trotz inhaltlicher Parallelen bei den TOM, zeigt sich ein grundlegender Unterschied in der Schutzlogik: Während die DSGVO bereits bei jeder Verarbeitung personenbezogener Daten risikoadäquate Maßnahmen fordert, greift die NIS-2-Richtlinie erst ab einer erhöhten

---

[221] *Grosmann/Michel*, ZD 2025, 250 (252).
[222] Art. 5 Abs. 1 lit. f) DSGVO normiert mit dem Gebot der Integrität und Vertraulichkeit zentrale Schutzziele, wie sie auch dem Informationssicherheitsmanagement nach ISO/IEC 27001 zugrunde liegen; dabei handelt es sich jedoch nicht um eine zusätzliche materielle Schutzdimension im Sinne des vom BVerfG entwickelten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sondern um formelle Anforderungen an die datenschutzkonforme Ausgestaltung der Verarbeitung – mit Fokus auf das „Wie" der Datenverarbeitung, nicht auf deren „Ob"; *Pötters*, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 39. Vgl. Erw. 17 und 79 NIS-2-RL.
[223] Im Ergebnis ebenso: *Reichert/Schweda/Shaha*, ZD 2023, 141 (143); *Oberndorfer*, Compliance Praxis 2025, Heft 1 v. 3.3.2025, S. 5.

Gefahrenschwelle - konkret bei als wesentlich oder wichtig eingestuften Einrichtungen.[224] Dadurch verlangt die NIS-2-Richtlinie bereits auf Basisebene ein umfangreicheres Risikomanagement.[225]

2. Asset Management und Verzeichnis von Verarbeitungstätigkeiten (VVT)

Eine fundierte Risikoanalyse sowie die darauf aufbauende Auswahl und Umsetzung geeigneter Sicherheitsmaßnahmen setzen zwingend eine vorgelagerte Analyse der relevanten Schutzgüter voraus. Sowohl im Anwendungsbereich der DSGVO als auch im Rahmen der NIS-2-Richtlinie bildet die systematische Identifikation und Bewertung schützenswerter Assets das notwendige Fundament für ein wirksames Sicherheitsmanagement. Das VVT nach Art. 30 DSGVO wird im Kapitel B. zur DSGVO nicht vertieft behandelt, da es primär als Compliance-Instrument einzuordnen ist, jedoch zugleich eine fundamentale Grundlage für ein Asset-Management in der Security Dimension fungiert. Das VVT verlangt von Verantwortlichen die Dokumentation zentraler Verarbeitungsparameter, einschließlich der Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten, der Verarbeitungszwecke, Kategorien betroffener Personen und Daten, Empfänger (einschließlich Drittländern und internationalen Organisationen), etwaiger Übermittlungen in unsichere Drittstaaten samt Garantien, Löschfristen sowie einer allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.[226] Folglich kann das VVT nach Art. 30 DSGVO als ein Asset-Management im Sinne der DSGVO angesehen werden. Im direkten Vergleich legt Art. 21 Abs. 2 lit. i NIS-2-RL den Fokus auf ein strukturiertes Asset Management als integralen Bestandteil des Risikomanagements im Bereich der Cybersicherheit.

Beiden Ansätzen ist gemein, dass sie auf eine transparente Bewertung der Kritikalität der Assets nach den jeweiligen Anwendungsbereichen abzielen und dadurch die Grundlage für risikobasierte Schutzmaßnahmen schaffen. Für betroffene Einrichtungen ergibt sich hieraus die Möglichkeit, durch eine adäquate Dokumentationspraxis sowohl datenschutzrechtliche als auch sicherheitsbezogene Anforderungen kohärent zu erfüllen, um somit Redundanzen zu vermeiden.

[224] *Grosmann/Michel*, ZD 2025, 250 (252).
[225] *Grosmann/Michel*, ZD 2025, 250 (252).
[226] *Klug*, in: Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Rn. 4-9.

3. Operative Umsetzung der Sicherheitsmaßnahmen

Das bereits beschriebene Portfolio an Sicherheitsmaßnahmen wird diverse Überschneidungen haben. Zugangskontrollen, Verschlüsselung, Multi-Faktor-Authentifizierung, Schulungsprogramme, Protokollierung, physische Sicherungsmaßnahmen oder Business Continuity Management werden von beiden Regelwerken entweder ausdrücklich gefordert oder implizit vorausgesetzt. Diese Parallelen bieten erhebliche Synergiepotenziale: Ein einmal implementiertes Rollen- und Berechtigungskonzept, ein standardisiertes Awareness-Programm oder ein unternehmensweites Notfallmanagement können gleichzeitig Anforderungen aus beiden Regimen erfüllen.[227] Besonders deutlich wird dies in der datenschutzkonformen Ausgestaltung von IT-Systemen nach Art. 25 DSGVO (Privacy by Design), die methodisch mit den Vorgaben zur sicheren Systementwicklung und Schwachstellenmanagement gemäß Art. 21 Abs. 2 lit. e) NIS-2-RL harmoniert. Langfristig wird für Einrichtungen, die sowohl der DSGVO als auch der NIS-2-Richtlinie unterliegen, die Einführung und Aufrechterhaltung eines dokumentierten Informationssicherheitsmanagementsystems nach ISO/IEC 27001 unabdingbar, da diese Norm organisationsübergreifend verbindliche Anforderungen an Aufbau, Betrieb und kontinuierliche Verbesserung eines risikobasierten Sicherheitsmanagements stellt.[228] Ein unmittelbarer Beleg für diese normative Annäherung findet sich in der aktuellen Handreichung der *Europäischen Agentur für Cybersicherheit* (ENISA), in der die einzelnen Maßnahmenanforderungen des Art. 21 NIS-2-RL systematisch den Controls des Anhangs A der ISO/IEC 27001:2022 zugeordnet werden.[229] Ein mögliches Spannungsfeld in der operativen Umsetzung von Sicherheitsmaßnahmen ergibt sich aus den Grundsätzen der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO), die mit den Anforderungen an die technische Nachvollziehbarkeit in sicherheitsrelevanten Systemen kollidieren können. Die NIS-2-Richtlinie sieht in Art. 21 Abs. 2 – in lit. b (Bewältigung von Sicherheitsvorfällen) und lit. f (Wirksamkeitsbewertung) – eine umfassende Protokollierung und Überwachung sicherheitsrelevanter Vorgänge vor. Diese Erfordernisse können den datenschutzrechtlichen Geboten konterkarieren.[230]

---

[227] Vgl. Maßnahmen des Anhangs A. ISO/IEC 27001:2022, *Brenner*, Praxishandbuch ISO/IEC 27001, 4. Auflage, B.3.

[228] Vgl. *Conrad/Streitz*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn. 385-387.

[229] Vgl. *ENISA*, NIS2 Technical Implementation Guidance, 26. Juni 2025.

[230] Sicherheitsmaßnahmen nach NIS-2 müssen im Lichte der DSGVO geplant und technisch so gestaltet werden, dass sie mit dem Minimierungsprinzip vereinbar sind. Im Ergebnis ebenso: *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage 2024, Rn. 31.

4. Meldeprozesse

Trotz unterschiedlicher Schutzgüter kann es in der Praxis zur Anwendbarkeit beider Meldepflichten kommen, sofern ein Vorfall eine erhebliche Beeinträchtigung von Informationssystemen als auch eine Verletzung des Schutzes personenbezogener Daten verursacht. In solchen Fällen bestehen parallele Meldepflichten gegenüber verschiedenen Behörden mit teils abweichenden inhaltlichen Anforderungen und Fristen. Dies kann zu erheblichen Koordinationsaufwänden führen. Um den teils parallel geltenden Meldepflichten nach DSGVO und NIS-2-Richtlinie gerecht zu werden, müssen in der Praxis differenzierte Meldeprozesse etabliert werden, die sowohl die unterschiedlichen Fristen und Inhalte als auch die getrennten Meldekanäle berücksichtigen.[231] Betroffenen Einrichtungen ist mithin zu empfehlen, ein übergeordnetes Incident-Response-Management zu implementieren, welches in der IT-Richtlinie definiert wird.

Im Unterschied zur DSGVO, die in Art. 34 eine Benachrichtigungspflicht gegenüber betroffenen Personen vorsieht, richtet sich die Unterrichtungspflicht nach der NIS-2-Richtlinie vorrangig an Kunden des betroffenen Unternehmens (B2B).[232] Darüber hinaus kann die zuständige Behörde nach Art. 23 Abs. 7 NIS-2-RL im öffentlichen Interesse sogar eine Information der allgemeinen Öffentlichkeit anordnen oder selbst vornehmen, womit der Anwendungsbereich über die DSGVO hinausgeht.[233] Ein harmonisiertes, europaweites Meldeportal der Aufsichtsbehörden könnte die Einhaltung der Compliance-Anforderungen erleichtern.[234]

5. DSFA und Risikoanalyse

Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und die Risikoanalyse gemäß Art. 21 Abs. 2 lit. a) NIS-2-Richtlinie verfolgen jeweils einen risikobasierten Ansatz.[235] Während Art. 35 DSGVO bei Verarbeitungsvorgängen mit voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen greift und eine vorhergehende Bewertung datenschutzrechtlicher Risiken verlangt, zielt Art. 21 Abs. 2 lit. a) NIS-2-RL auf die fortlaufende Bewertung von Risiken für Netz- und Informationssysteme ab. Letztere Risikoanalyse stellt eine generelle Pflicht für alle wesentlichen und wichtigen Einrichtungen dar, unabhängig von einer personenbezogenen Risikoprognose. Beide Normen verlangen die Ableitung geeigneter TOM, wobei sich die DSFA stärker an individuellen Grundrechten

[231] *Grosmann/Michel*, ZD 2025, 250 (253).
[232] *Grosmann/Michel*, ZD 2025, 250 (253).
[233] *Grosmann/Michel*, ZD 2025, 250 (253).
[234] *Hessel/Callewaert/Schneider*: RDi 2024, 208 (213).
[235] Wie in Kapitel B. V. sowie in C. III. dargelegt.

orientiert und die NIS-2-Richtlinie eine ganzheitliche Absicherung kritischer Infrastrukturen bezweckt.[236] Trotz dieser unterschiedlichen Schutzgüter ergeben sich methodische Parallelen. Das BSI schlägt in diesem Zusammenhang einen (für diese Ausarbeitung vereinfachten) Siebenschritt vor: Vom Verständnis des Kontexts über die Identifikation relevanter Assets und Bedrohungen bis hin zur Risikobewertung, Maßnahmenableitung, Dokumentation und regelmäßigen Überprüfung.[237] In ihrer Struktur weist sie deutliche Parallelen zur Datenschutz-Folgenabschätzung nach Art. 35 DSGVO auf. Auch dort steht die Beschreibung der Verarbeitung, die Bewertung potenzieller Risiken für die Rechte und Freiheiten betroffener Personen sowie die Auswahl und Dokumentation geeigneter technischer und organisatorischer Maßnahmen im Mittelpunkt.[238]

6. DSB und ISB

Angesichts der funktionalen Nähe ist es grundsätzlich möglich, die Aufgaben von DSB und ISB in einer Person zu bündeln, sofern die dezidiert benannte Person ausreichende Fachkompetenz in beiden Bereichen aufweist.[239] Gerade in Bezug auf die geforderten Meldepflichten würde eine Bündelung der Positionen in einer Person zu Effizienzen und Klarheiten in den internen Meldeprozessen führen. Konflikte entstehen, wenn sicherheitstechnische Maßnahmen zwar der Optimierung der Informationssicherheit dienen, zugleich aber datenschutzrechtlich problematisch oder unterschiedlich zu bewerten sind.[240] Aufgrund der unterschiedlichen Schutzrichtungen von Datenschutz und Informationssicherheit führt eine Doppelfunktion von DSB und ISB langfristig zu Interessenkonflikten, weshalb sich in der Praxis eine Trennung der Rollen durchgesetzt hat.[241]

IV. Zwischenfazit

In Bezug auf die zweite Forschungsfrage ergibt sich, dass sich die DSGVO und die NIS-2-Richtlinie in ihrer Zielsetzung zwar unterscheiden, jedoch in zahlreichen normativen und operativen Aspekten eine enge Verzahnung aufweisen. Die beiden Regelwerke adressieren unterschiedliche Schutzgüter, werden jedoch für viele Einrichtungen gleichermaßen anwendbar sein.

---

[236] Erw. (1), (2), (4), (76), (78) und (83) DSGVO; Erw. (16), (42), (79) NIS-2-RL.
[237] *BSI*, #nis2know: NIS-2 Risikoanalyse.
[238] Wie in Kapitel B.V. beschrieben.
[239] Ein Verbot ist per se nicht gegeben; in der Praxis wird dies eher eine Frage der Ressourcen der betroffenen Einrichtung sein.
[240] *Schmidl*, Corporate Compliance, 4. Auflage 2024, Rn. 294.
[241] Im Ergebnis ebenso: *Grosmann/Michel*, ZD 2025, 250 (253). *Schmidl*, Corporate Compliance, 4. Auflage 2024, Rn. 294.

Zentrale Synergien zeigen sich in der Governance-Verankerung von Sicherheits- und Compliance-Pflichten, der risikobasierten Implementierung der TOM sowie im gemeinsamen Bezug auf internationale Standards wie ISO/IEC 27001. Beide Regime verlangen (direkt oder indirekt) die Implementierung von Managementsystemen, die kontinuierliche Risikoanalysen, Schulungen, Dokumentationen sowie Reaktionsmechanismen auf Sicherheitsvorfälle im Sinne der jeweiligen Normen. Besonders hervorzuheben ist die zunehmende Bedeutung einer integrierten IT-Richtlinie, die als organisationsinterne Brücke zwischen Datenschutz und Cybersicherheit fungiert.
Zugleich treten auch divergente Regelungsansätze zutage, etwa hinsichtlich der Schutzlogik (personenbezogen vs. systembasiert), der Schwellenwerte für die Anwendung (Size-Cap-Ausnahme vs. universelle Anwendbarkeit bei der Verarbeitung personenbezogener Daten) sowie bei der operativen Umsetzung (etwa im Spannungsverhältnis zwischen Datenschutzprinzipien und Anforderungen an technische Nachvollziehbarkeit). Die getrennten Meldepflichten und Adressaten im Falle von Sicherheitsvorfällen verdeutlichen zudem bestehende Koordinationsherausforderungen.
Insgesamt lässt sich festhalten, dass die gleichzeitige Anwendung beider Regime für betroffene Einrichtungen nicht nur Anforderungen kumuliert, sondern - bei kohärenter Umsetzung – auch signifikante Synergieeffekte ermöglicht. Um diese Potenziale auszuschöpfen und zugleich etwaigen Spannungsfeldern wirksam zu begegnen, ist ein integrierter Ansatz erforderlich, der die Anforderungen holistisch umsetzt.

D. Resümee

I. Zusammenfassung der Forschungsergebnisse

Die vorhergehende Analyse zeigt, dass sowohl die Datenschutz-Grundverordnung als auch die NIS-2-Richtlinie eigenständige, jedoch in wesentlichen Teilen komplementäre Regelungsansätze für ein zeitgemäßes Sicherheitsmanagement verfolgen.
In Bezug auf die erste Forschungsfrage wurde herausgearbeitet, dass die DSGVO ein vielschichtiges Sicherheitsmanagement etabliert, das normative Grundprinzipien (Art. 5), Gestaltungsprinzipien (Art. 25), Technische und Organisatorische Maßnahmen (Art. 32) sowie exekutive Pflichten (Art. 33, 34, 35, 37, 38, 39) integriert. Die Angemessenheit dieser Anforderungen beruht auf einem risikobasierten, flexiblen Ansatz, der den Stand der Technik und wirtschaftliche Zumutbarkeit berücksichtigt, jedoch an terminologischen Unschärfen und der fehlenden Definition eines „angemessenen Schutzniveaus“ leidet. Die NIS-2-Richtlinie verfolgt hingegen einen sektorübergreifenden Ansatz, der durch verbindliche

Führungsverantwortung (Art. 20), ein klar umrissenes Maßnahmenportfolio (Art. 21) und gestufte Berichtspflichten (Art. 23) ergänzt wird. Positiv hervorzuheben ist die Anlehnung an internationale Standards wie ISO/IEC 27001, während die weite Fassung des Anwendungsbereichs, nationale Umsetzungsspielräume und unklare Schwellenwerte weiterhin Herausforderungen darstellen.
Die Ausarbeitungen hinsichtlich der zweiten Forschungsfrage verdeutlichen, dass beide Regelwerke zwar unterschiedliche Schutzgüter adressieren, in der operativen Umsetzung jedoch erhebliche Schnittmengen bestehen. Gemeinsamkeiten finden sich insbesondere in der Governance-Verankerung von Sicherheits- und Compliance-Pflichten, der risikobasierten Implementierung von TOM, der Orientierung an internationalen Normen sowie in der Notwendigkeit fortlaufender Risikoanalysen, Schulungen und Dokumentation.
Spannungsfelder ergeben sich vor allem aus unterschiedlichen Schwellenwerten, divergierenden Schutzlogiken sowie potenziellen Konflikten zwischen Datenschutzprinzipien und Anforderungen an die technische Nachvollziehbarkeit.
Insgesamt lässt sich festhalten, dass die gleichzeitige Anwendung beider Regime zwar Mehrfachanforderungen erzeugt, bei kohärenter Anwendung jedoch erhebliche Synergieeffekte ermöglicht. Entscheidend für die Praxis wird sein, ein strategisch integriertes Sicherheits- und Compliance-Management zu etablieren, das die Anforderungen beider Rechtsinstrumente in einem harmonisierten Rahmen umsetzt und so sowohl rechtliche als auch sicherheitstechnische Zielsetzungen erfüllt. Compliance wird nie isoliert von Security betrachtet werden können. Diese unvermeidbare Realität wird Hebel für Tools

II. Ausblick

Es lassen sich deutliche regulatorische Entwicklungen erkennen. Neben den in dieser Arbeit behandelten Rechtsakten adressiert der europäische Gesetzgeber mit der KI-Verordnung sowie dem Cyber Resilience Act weitere zentrale Bereiche moderner Technologien.
Mit dem Inkrafttreten der KI-VO am 1. August 2024 wurde ein risikobasiertes Regulierungssystem etabliert, das schrittweise über mehrere Jahre zur Anwendung gelangt. Die Legaldefinition des KI-Systems in Art. 3 Ziff. 1 KI-VO verdeutlicht dabei, dass regulatorische Maßnahmen im Bereich der Künstlichen Intelligenz eng mit dem technologischen Fortschritt verflochten sind. [242]
Mit dem Cyber Resilience Act werden zudem erstmals europaweit verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen eingeführt, die

[242] *Becker/Feuerstack*, KIR 2024, 62 (63).

Hersteller verpflichten, grundlegende Sicherheitsstandards über den gesamten Lebenszyklus hinweg zu gewährleisten.[243]

Diese Dynamik lässt erkennen, dass die EU-Regulierung sich stark integrierend weiterentwickelt. Datenschutz, Cybersicherheit und KI-Sicherheit verschmelzen zunehmend zu einem einheitlichen Governance-System. Zudem werden sich zukünftige vermutlich stärker an gemeinsamen Standards und Managementsystemen (z. B. ISO/IEC 27001) orientieren. Gleichzeitig verspricht die Kommission Unterstützungsmaßnahmen für Unternehmen – insbesondere KMU. So werden gezielte Anpassungen der DSGVO vorgeschlagen, darunter die Ausweitung der Befreiung von der Pflicht zum Führen eines VVT auf Unternehmen mit bis zu 750 Beschäftigten sowie die stärkere Einbindung von KMU und Small Mid Caps in Codes of Conduct und Zertifizierungen.[244]

Ein spannender Aspekt betrifft die rechtliche Natur der NIS-2-Richtlinie als Richtlinie. In Hinblick auf die wachsende Bedeutung von Cybersicherheit stellt sich die Frage, ob dieser Rechtsakt auf Dauer bestehen bleibt oder ob das ähnliche Schicksal der Datenschutzrichtlinie droht, die durch die DSGVO abgelöst wurde und in absehbarer Zeit eine unmittelbar geltende Verordnung folgen könnte. Eine solche Entwicklung würde den Harmonisierungsgrad innerhalb der Europäischen Union erheblich steigern und die derzeit bestehenden Umsetzungsspielräume der Mitgliedstaaten verringern.

Abschließend lässt sich festhalten: Die EU-Gesetzgebung befindet sich in einer Phase der erhöhten Integration. Die Kombination aus DSGVO, NIS-2, AI-Act und CRA bildet ein vernetztes Regelwerk, das technische Standards, Governance-Anforderungen und Produkt-Lebenszyklus-Verantwortungen zusammenführt.

[243] *Schöttle*, MMR 2024, 741.

[244] *EDPB*, Targeted modifications of the GDPR: EDPB & EDPS welcome simplification of record keeping obligations and request further clarifications, 09. Juli. 2025.

Literaturverzeichnis

Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019.

Becker/Feuerstack, Die KI-Verordnung, KIR 2024, 62.

Brams, Bußgeldrisiken nach Datenschutzvorfällen, ZD 2023, 484.

Brenner, Michael/ Gentschen Felde, Nils/ Hommel, Wolfgang/ Metzger, Stefan/ Reiser, Helmut/ Schaaf, Thomas, Praxisbuch ISO/IEC 27001, 4. Auflage, München 2022.

BSI, „Stand der Technik“ umsetzen, abrufbar im Internet: <https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html> (Stand 16.12.2024).

BSI, Die Lage der IT-Sicherheit in Deutschland 2024, abrufbar im Internet https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (Stand: 23.11.2024).

BSI, Fragen und Antworten zu NIS-2, abrufbar im Internet < https://www.bsi.bund.de/dok/nis-2-fa> (Stand 17.05.2025).

BSI, CyberRisikoCheck, abrufbar im Internet < https://www.bsi.bund.de/dok/crc> (Stand 20. Mai 2024).

BSI, NIS-2-Betroffenheitsprüfung, abrufbar im Internet < https://betroffenheitspruefung-nis-2.bsi.de/> (Stand 19.07.2025).

BSI, #nis2kno: NIS-2 Risikoanalyse, abrufbar im Internet < https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Risikoanalyse/NIS-2-Risikoanalyse_node.html> (Stand 07. 08. 2025).

CNIL, Advertisements inserted among emails: ORANGE fined €50 million, 10. Dezember. 2024, abrufbar im Internet: <https://www.cnil.fr/en/advertisements-inserted-among-emails-orange-fined-eu50-million> (Stand 03.04.2025).

Datenschutzgruppe Nach Artikel 29, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt, 04. April. 2017, abrufbar im Internet: < https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_de> (Stand 01. April. 2025).

Degen/Emmert, Elektronischer Rechtsverkehr, 3. Auflage, München 2025.

Dury/Leibold „Home Office“ und Datenschutz, ZD-Aktuell 2020, 04405.

Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Auflage, München 2024.

ENIS, NIS2 Technical Implementation Guidance, abrufbar im Internet: < https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance> (Stand 05.08.2025).

European Data Protection Board, The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21.01.2019, abrufbar im Internet: < https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en> (Stand: 23.03.2025).

European Data Protection Board, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, abrufbar im Internet: <https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf> (Stand 15.12.2024).

European Data Protection Board, Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Version 2.0, abrufbar im Internet: < https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_de.pdf> (Stand 03.02.2025),

European Data Protection Board, ICO statement: Intention to fine British Airways £183.39m under GDPR for data breach, 08. Juli. 2019, abrufbar im internet unter: < https://www.edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-british-airways-ps18339m-under-gdpr-data_en< (Stand 01.08.2025).

European Data Protection Board, ICO statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, 09. Juli 2019, abrufbar im Internet unter: <https://www.edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en> (Stand 01.08.2025).

European Data Protection Board, Targeted modifications of the GDPR: EDPB & EDPS welcome simplification of record keeping obligations and request further clarifications, 09. Juli. 2025, abrufbar im Internet: https://www.edpb.europa.eu/news/news/2025/targeted-modifications-gdpr-edpb-edps-welcome-simplification-record-keeping_en (Stand 26. August. 2025).

Franzen/Gallner/Oetker, Kommentar zum europäischen Arbeitsrecht, 5. Auflage, München 2024.

Feiler/Forgo, EU-DSGVO, 2. Auflage, Wien 2022.

Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage, München 2022.

Fortune Business Insights, SAAS MARKET SIZE, 21.07.2025, abrufbar im Internet unter: < https://www.fortunebusinessinsights.com/software-as-a-service-saas-market-102222> (Stand 01.08.2025).

Grosmann/Michel, Datenschutz trifft IT-Sicherheit, ZD 2025, 253.

Gutbrunner, Anwendungsbereich NIS-2-RL, Lexis Briefings Wirtschaftsrecht, Februar 2025.

Hanloser, Datenschutz-Compliance: Security Breach Notification bei Datenpannen, CCZ 2010, 25.

Henssler, Münchener Kommentar zum BGB, 9. Auflage, München 2023.

Herdegen, Internationales Wirtschaftsrecht, 13. Auflage, München 2023.

Hessel/Callewaert/Schneider, Die NIS-2-Richtlinie aus Unternehmensperspektive, RDI 2024, 208.

Hilmer, Hans-Jürgen, Datenschutz als KI-Bremse: Richtlinien und Checklisten helfen beim Wechsel aug das Gaspedal, BC 2024, 351.

Holthausen, Überlegungen und Gestaltungshinweise zu IT-Betriebsvereinbarungen, NZA 2023, 1489.

Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Auflage, München 2024.

Hötzel/Völkel, Vermeidung von Haftungsfällen mittels IT-CMS, BC 2024 (402).

Humer, Die Geschäftsleiterhaftung unter der NIS-2-RL, abrufbar im Internet: < https://360.lexisnexis.at/d/lexisbriefings/die_geschaftsleiterhaftung_unter_der_nis_2_rl/h_80004_2758271828530131775_cdd0f38cca?origin=gs&searchid=20250510100644376&rlclick=graph%2Btitle> (Stand 02.05.2025).

Kipker/Birreck/Niewöhner/Schnorr, NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie, MMR 2021, 214.

Kipker, Cybersecurity, 2. Auflage, München 2023.

Kipker/Dittrich, Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, MMR 2023, 481.

Jung, Datenschutz – (Compliance-) Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018.

Jung/ Dirnbauer, Konzerninterne Rechenzentrumsdienste im Anwendungsbereich der NIS-2-Richtlinie? Compliance Praxis 2025, 10, Heft 1 v. 03.03.2025.

Kinast/Stanonik, Praxishandbuch Datenschutz für KMU, 1. Auflage, München 2019.

Klingbeil/Kohm, Datenschutzfreundliche Technikgestaltung und ihre vertraglichen Implikationen, MMR 2021 (3).
Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder, Das Standard-Datenschutzmodell, Version 3.1, Kiel 2024.
Kramer, IT-Arbeitsrecht, 3. Auflage, München 2023
Kühlin/Buchner, DS-GVO BDSG, 4. Auflage, München 2024.
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Meldungen nach Art. 33 DSGVO (sog. Datenpannen), 2025, abrufbar im Internet: https://www.ldi.nrw.de/zahlen-und-daten (Stand 01.03.2025).
Leupold/Wiebe/Glossner, IT-Recht, 4. Auflage, München 2021.
Marly, Praxishandbuch Softwarerecht, 8. Auflage, München 2024.
Moosmayer/Lösler, Corporate Compliance, 4. Auflage, München 2024.
Moll/Eckhoff/Reufels, Münchener Anwaltshandbuch Arbeitsrecht, 6. Auflage, München 2025
Mair/Müller/Schlepitzka, Lessons Learned – 1 Jahr DSGVO – Compliance, Compliance Praxis 2019, S. 27.
Maslewski, Datenpannen-Management in der Unternehmenspraxis, ZD 2023, 251
Neuwirth, Vom "wesentlichen Dienst" zur "wesentlichen" beziehungsweise "wichtigen" Einrichtung - und weitere ausgewählte Aspekte zur NIS-2-Richtlinie, jusIT 2024/2, Heft 1 v. 29.2.2024.
Oltmanns/Fuhlrott, Desk-Sharing & Coworking-Spaces: Arbeitsrechtliche Besonderheiten zweier „moderner Arbeitsformen“, NZA 2018, 1225.
Paal/Pauly, DS-GVO BDSG, 3. Auflage, München 2021.
Pietzka/Wimmer/Kühle: Zur Bilanzierung von Implementierungskosten im Rahmen von SaaS-Verträgen, IRZ 2021, 473.
Redeker, IT-Recht, 8. Auflage, München 2023.
Reichert/Schwada/Shaha, Datenschutzmanagement messbar machen und steuern, ZD 2023, 151.
Reiter/Heidinger/Gstrein, Die NIS2-Richtlinie: Von Cybersicherheit und Haftung, Medien und Recht 2023, 188, Heft 4 v. 15.09.2023
Schatzlmaier, NIS-2-RL – Wunderwaffe gegen den Cyber-Supergau? Compliance Praxis 2025, Heft 1 v. 03.03.2025.
Seibel, Abgrenzung der „allgemeinen anerkannten Regeln der Technik“ vom „Stand der Technik“, NJW 2013, 3000.
Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage, München 2019.

Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 2. Auflage, Berlin 2021.
Schmidt, Der Regierungsentwurf zur NIS-2-Richtlinie - Richtliniengetreue Umsetzung oder deutscher Sonderweg? RDi 2024, 550.
Schürmann, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz, ZD 2022, 316.
Steiner/Schmiedlechner, NIS-2-RL – Was bei der Meldung zählt, Compliance Praxis 2025, 7, Heft 1 v. 03.03.2025.
Sydow/Marsch, DS-GVO | BDSG, 3. Auflage, München 2022.
Taeger/Gabel, DSGVO – BDSG -TTDSG, 3. Auflage, München 2021.
Taeger/Gabel, DSGVO – BDSG – TTDSG, 4. Auflage, München 2022.
Unmuß, Corporate Compliance Checklisten, 5. Auflage, München 2022.
Votteler, Die ISO/IEC-Norm 27002:2017 „Leitfaden für Informationssicherheitsmaßnahmen, MMR 2023 (403).
Wirtschaftskammer Österreich, Cybersicherheits-Richtlinie NIS 2, 02.07.2025, abrufbar im Internet unter: < https://www.wko.at/it-sicherheit/nis2-uebersicht> (Stand 11.08.2025).
Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 49. Edition, München 2021.
Weihe, Compliance 2024: Was Verantwortliche im Mittelstand wissen müssen, CCZ 2024, 85.
Werry/Éles, Umsetzung der NIS2-Richtlinie: Harmonisierung oder Heterogenität, MMR 2024, 829.