06.24

12. Jahrgang
November 2024
Seiten 251–300

www.PinGdigital.de

PinG

Privacy in Germany

DATENSCHUTZ UND COMPLIANCE

ESV ERICH SCHMIDT VERLAG
100 Jahre

PinG-Podcast

Meldepflichten für Finanzunternehmen nach der DORA-Verordnung im Spannungsfeld zwischen DSGVO und NIS-2

Karina Filusch, LL.M., Frank Fünfstück und Dr. Aleksandra Sowa

Die Meldepflichten bei sicherheitsrelevanten Inzidenten sind in verschiedenen Rechtsgrundlagen geregelt. Wie, wann und an wen eine Meldung erfolgen muss, regeln u. a. die DORA-VO, das NIS-2-Umsetzungsgesetz, das KRITIS-Dachgesetz und die DSGVO. Wie das Spannungsverhältnis dieser Normen zueinander ist, wird im folgenden Beitrag am Beispiel von Unternehmen aus dem Finanzsektor beleuchtet und konstatiert, wie eine solche Meldung aussehen könnte, damit sie den zuvor genannten Rechtsnormen nicht widerspricht – sofern das bei der Fülle an Regelungen möglich ist.

Zusätzlich zu der Regulierung der Meldepflichten gemäß der DSGVO sowie dem aktuell als Regierungsentwurf vom 24.07.2024 vorliegenden NIS-2-Umsetzungsgesetz (NIS2UmsuCG) und dem KRITIS-Dachgesetz (KRITIS-DachG-E), die beide zahlreiche Überschneidungen im Bezug auf die Regelung der Meldepflichten für Sicherheitsvorfälle aufweisen, gilt für Finanzunternehmen[1] ab dem 17.01.2025 der Digital Operational Resilience Act (DORA-Verordnung, DORA-VO). Die zuständige Aufsichtsbehörde, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), regelt die Umsetzung der DORA-VO sowie das Vorfallsmeldewesen in Bezug auf schwerwiegende Informations- und Kommunikationstechnologie (IKT)[2]-bezogene Vorfälle.[3] Dass die Forderungen der DORA-VO zweckmäßig sind, zeigt der aktuelle Angriff auf den US-Finanzdienstleister MoneyGram.[4]

Während ein (nicht meldepflichtiger) IKT-bezogener Vorfall gemäß Art. 3 Nr. 8 DORA-VO als ein (1) nicht geplantes Ereignis oder eine Reihe verbundener Ereignisse definiert wird, das/die (2) die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und (3) nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf erbrachte Dienstleistungen hat, wird ein (meldepflichtiger) schwerwiegender IKT-bezogener Vorfall gemäß Art. 3 Nr. 10 DORA-VO als ein Vorfall definiert, der umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme hat, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen.[5]

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

Frank Fünfstück studiert Rechtswissenschaft an der Fernuniversität in Hagen.

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

I. Geltungsbereich, Ausnahmen und Besonderheiten: aggregierte Meldepflichten

Der Geltungsbereich der DORA-VO ist bewusst breit angelegt und umfasst neben Banken, Versicherungen, Zahlungs-

1 Als „Finanzunternehmen" oder „financial entities" werden gemäß Art. 2 Abs. 2 DORA-VO alle für die Zwecke der Verordnung in Abs. 1 lit. a bis t aufgeführten Unternehmen bezeichnet.

2 Art. 1 Abs. 1 lit. a röm. i) Verordnung (EU) 2022/2554.

3 Vgl. *Göddecke*, Referat GIT 2, BaFin. 2024. „IKT-Vorfallswesen". Vortrag auf der BaFin-Konferenz „IT-Aufsicht im Finanzsektor: Was bedeutet DORA in der Praxis?" (26.9.2024), abrufbar unter: https://www.bafin.de/SharedDocs/Veranstaltungen/DE/240926_BaFin_Konferenz.html; „Incident Reporting, Überwachung IT-MMDL und Krisenprävention, zum Incident-Meldewesen". Vortrag auf der BaFin-Veranstaltung „IT-Aufsicht im Finanzsektor" (5.12.2023), abrufbar unter: https://www.bafin.de/SharedDocs/Veranstaltungen/DE/2023_12_05_IT_Aufsicht.html und *Sowa*, 2023, Meldepflichten für Sicherheitsvorfälle für Finanzunternehmen (DORA) (9.12.2023).

4 Abrufbar unter: https://www.heise.de/news/Cyberangriff-auf-US-Finanzdienstleister-MoneyGram-9951507.html und https://www.it-markt.ch/news/2024-10-08/hacker-stehlen-persoenliche-daten-von-moneygram-kunden.

5 *Göddecke*, 2024, S. 5.

dienstleistern, Asset-Management-Gesellschaften, Börsen und Märkten auch Anbieter von Crypto-Assets-Services. Eine nationale Erweiterung des Anwendungsbereichs gemäß § 1a KWG erstreckt den Geltungsbereich außerdem auf Institute und Versicherungsholding-Gesellschaften.[6] Der Begriff „Finanzunternehmen", auf die sich die Meldepflichten beziehen, entspringt der Definition aus Art. 2 Abs. 2 DORA-VO und umfasst laut BaFin eine sehr große Bandbreite von Unternehmen. Darunter fallen gemäß Art. 2 Abs. 1 DORA-VO CRR-Kreditinstitute, Zahlungsinstitute (einschließlich registrierter Kontoinformationsdienstleister), E-Geld-Institute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen (MiCA), CSD, CCP, Handelsplätze, Transaktionsregister, Verwaltungsgesellschaften, AIFM, Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, EbAVs, Ratingagenturen, Administratoren kritischer Referenzwerte, Verbriefungsregister und Schwarmfinanzierungsdienstleister.[7]

1. Begleitende Gesetzgebung

Die Umsetzung der DORA-VO macht eine umfangreiche nationale Begleitgesetzgebung notwendig (Finanzmarktdigitalisierungsgesetz, FinmadiG), von der die nationalen Aufsichtsgesetze (u. a. KWG, VAG, ZAG, WpHG, WpIG, KAGB, BörsG, KMAG, GewO) betroffen sind. Das Gesetz zur Digitalisierung des Finanzmarktes soll das europäische DORA-Paket im FinmadiG zusammenfassen und umsetzen. Das Bundesministerium der Finanzen hat bereits den Regierungsentwurf des FinmadiG veröffentlicht. Die Beschlussempfehlung und der Bericht des Finanzausschusses liegen ebenfalls vor.[8]

Die BaFin betont dennoch das Prinzip der Proportionalität, dem man bei der Operationalisierung der Vorgaben folgt. Dies umfasst einerseits die Verhältnismäßigkeit der Anforderungen und andererseits die Ausnahmen und Vereinfachungen für bestimmte Unternehmen. Teilweise gelten die Vereinfachungen, etwa bei der Einhaltung von Meldefristen, nicht für die NIS-2-regulierten Finanzunternehmen.

2. Aggregierte Meldungen

IKT-Meldepflichten gelten nicht für IKT-Drittdienstleister – mit einer Ausnahme: Wenn es sich um aggregierte Meldungen gemäß Art. 7 der Draft Implementing Technical Standards, JC 2024 33 (ITS-E zur Festlegung von Standardformularen, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung)[9] handelt. Dabei geht es jedoch nicht explizit um eine Pflicht der Drittdienstleister, sondern vielmehr um eine zulässige Praxis, bei der – wenn mehrere Finanzunternehmen von dem Sicherheitsvorfall betroffen sind – die Meldung an die BaFin zentral bzw. aggregiert durch den Dienstleister, bei dem der Sicherheitsvorfall eingetreten ist, erfolgen kann[10]. Für diese Art von „aggregierten Meldungen" sind bestimmte Informationen zu den Finanzunternehmen erforderlich, die der Dienstleister mitmelden und vorab von den Finanzunternehmen erfahren muss. Hierfür sollten Kommunikationskanäle zwischen den Dienstleistern und den Finanzunternehmen etabliert sein.[11] Meldungen im Sinne von Art. 33 Abs. 2 DSGVO sind bei der Verletzung des Schutzes personenbezogener Daten durch die IKT-Drittdienstleister an die Verantwortlichen aufgrund der Geltung der DSGVO abzugeben.[12]

Von der Ausnahme für aggregierte Meldungen gibt es allerdings ebenfalls weitere Ausnahmen: Bedeutende Kreditinstitute, Betreiber von Handelsplätzen und zentrale Gegenparteien können gemäß Art. 7 ITS-E nicht in das aggregierte Meldewesen einbezogen werden. Die BaFin hat gleichwohl eine Generalerlaubnis für die von ihr beaufsichtigten Finanzunternehmen erteilt: Unter Berücksichtigung der Voraussetzungen von Art. 7 ITS-E und ohne zusätzlichen Antrag soll eine aggregierte Meldung erlaubt sein.

II. Schwerwiegende IKT-Vorfälle

Finanzunternehmen melden gemäß Art. 19 DORA-VO als schwerwiegend klassifizierte IKT-bezogene Vorfälle direkt an die BaFin. Geplant ist eine dreistufige Meldung für schwerwiegende Vorfälle: eine Erst-, eine Zwischen- und eine Abschlussmeldung.[13] Die Beurteilung, ob ein IKT-Vorfall als „schwerwiegend" eingestuft wird, erfolgt derzeit anhand von sieben Klassifizierungskriterien (Art. 1–7 der Delegierten Verordnung (EU) 2024/1772 der Kommission[14]). Die Kritikalität der betroffenen Dienste gemäß Art. 6 der Delegierten Verordnung (EU) 2024/1772 ist wesentlich für die Entstehung einer Meldepflicht. Darüber hinaus müssen entweder mindestens zwei weitere Klassifizierungskriterien erfüllt sein oder es muss ein „böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme"[15] stattgefunden haben. Zu den weiteren Kriterien gehören: Auswirkungen auf Kunden, finanzielle Gegenparteien und Transaktionen

6 *Fechler*, Referat GIT 3, BaFin, 2024, „DORA – Ein Update". Vortrag auf der BaFin-Konferenz „IT-Aufsicht im Finanzsektor: Was bedeutet DORA in der Praxis?" (26.9.2024), S. 3.

7 *Fechler*, Referat GIT 3, BaFin, 2023, DORA – Ein Überblick. Vortrag auf der BaFin-Veranstaltung „IT-Aufsicht im Finanzsektor" (5.12.2023), S. 2.

8 Abrufbar unter: https://dip.bundestag.de/vorgang/gesetz-%C3%BCber-die-digitalisierung-des-finanzmarktes-finanzmarktdigitalisierungsgesetz-finmadig/307253.

9 Abrufbar unter: https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf.

10 Sogenanntes „aggregated reporting" gemäß Art. 7 ITS-E ist ein Zugeständnis an Finanzunternehmen, die vom selben IKT-Vorfall betroffen sind, indem die Meldung des Vorfalls aggregiert und nur durch die Drittanbieter – in Abstimmung mit den betroffenen Unternehmen – erfolgt.

11 *Göddecke*, 2024, S. 11–13.

12 *Filusch/Sowa*, Meldepflichten bei Sicherheitsvorfällen und Datenpannen, PinG 1/2024, S. 1 ff.

13 Vgl. EBA, EIOPA, ESMA, Joint Committee of the European Supervising Authorities, Consultation Paper: Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards On the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat (JC 2023 83), Januar 2024.

14 Vgl. Delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle (24.6.2024), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R1772.

15 *Göddecke*, 2024, S. 5.

(Art. 1); Reputationsschaden (Art. 2); Dauer und Ausfallzeiten (Art. 3); geographische Ausbreitung (Art. 4); Verluste von Daten (Art. 5) sowie wirtschaftliche Auswirkungen (Art. 7).[16]

1. Erstmeldung: Inhalte und Fristen

Eine Erstmeldung (initial notification) sollte demnach auf die wesentlichen Informationen beschränkt sein[17] und gemäß Art. 3 RTS-E (Draft Regulatory Technical Standards, JC 2023 83), „mindestens die folgenden Informationen über den Vorfall bereitstellen“:[18]

1. Datum und Uhrzeit der Entdeckung und Klassifizierung des Vorfalls;
2. Beschreibung des Vorfalls;
3. Klassifizierungskriterien, die die Meldung des Vorfalls gemäß Art. 1 bis 7 der Delegierten Verordnung (EU) 2024/1772 ausgelöst haben;
4. Betroffene oder potenziell betroffene Mitgliedstaaten, sofern zutreffend;
5. Informationen darüber, wie der Vorfall entdeckt wurde;
6. Informationen über die Quelle des Vorfalls, sofern verfügbar;
7. Hinweis, ob es Auswirkungen oder potenzielle Auswirkungen auf andere Finanzinstitute und Dritte gibt, sofern zutreffend;
8. Informationen darüber, ob der Vorfall wiederkehrend ist oder in Zusammenhang mit einem früheren Vorfall steht, sofern zutreffend;
9. Hinweis, ob ein Notfallplan aktiviert wurde; und
10. weitere Informationen.

Die Erstmeldung an die BaFin soll zwecks Beschreibung des Vorfalls die folgenden Fragen beantworten:[19]

- Wer meldet, wer ist betroffen?
- Was ist passiert?
- Welche Services sind betroffen?
- Welche Auswirkungen hat der Vorfall auf Kundinnen und Kunden, Gegenparteien oder andere Finanzmarktakteure?
- Dauert der Vorfall noch an, und falls ja, wie lange wird er voraussichtlich noch andauern?
- Liegt dem Vorfall vermutlich eine böswillige Handlung zugrunde?
- Wie gravierend ist der Vorfall aus Sicht des Finanzinstituts zum Zeitpunkt der Meldungsabgabe? (Einschätzung des Schweregrades)
- Sind nachhaltige Auswirkungen auf das Finanzunternehmen, seine Kundschaft oder den Finanzmarkt zu erwarten – oder sind diese bereits sichtbar?
- Ist es wahrscheinlich, dass andere Finanzunternehmen von diesem Vorfall betroffen sind?

Für die Einreichung der Meldungen kann ab dem 17.01.2025 das MVP-Formular der BaFin genutzt werden. Es ist auch eine (verschlüsselte) Meldung via E-Mail oder telefonisch (z. B. bei Ausfall der IKT-Infrastruktur) möglich.[20]

Als Frist für die Abgabe der Erstmeldung gilt: vier Stunden nach der Klassifizierung des IKT-Vorfalls als „schwerwiegend“, jedoch spätestens 24 Stunden nach der Entdeckung des Vorfalls. Falls der Vorfall erst nach mehr als 24 Stunden nach der Entdeckung als „schwerwiegend“ klassifiziert wird, gilt die Vier-Stunden-Frist ab dem Zeitpunkt der Klassifizierung.[21]

2. Zwischenmeldung: Inhalte und Fristen

Inhalte der Erst-, Zwischen- und Abschlussmeldungen, Fristen zur Meldungsabgabe sowie Inhalte der freiwilligen Meldung von Cyberbedrohungen werden gemäß Art. 20 DORA-VO in den Regulatory Technical Standards (RTS) – aktuell im Kapitel III der Delegierten Verordnung (EU) 2024/1772 – geregelt. Formulare, Vorlagen und Meldeverfahren sind dagegen Gegenstand der Implementing Technical Standards (ITS).

Spätestens 72 Stunden nach der Erstmeldung, oder auch auf Wunsch der Aufsichtsbehörde, wird von der BaFin eine Zwischenmeldung erwartet. Darin sollten Informationen zum Ausmaß sowie eine detailliertere Analyse des Vorfalls enthalten sein. Änderungen des Status oder der Handhabung des Vorfalls müssen von den Finanzunternehmen angezeigt werden.[22]

3. Abschlussmeldung: Inhalte und Fristen

Die Abschlussmeldung ist einen Monat nach der letzten Zwischenmeldung fällig. Dies gilt auch dann, wenn der IKT-Vorfall nach einem Monat noch nicht abgeschlossen ist. In diesem Fall wird von der BaFin empfohlen, in der Abschlussmeldung die Ursachen des Vorfalls zu antizipieren, auch wenn sie noch nicht abschließend feststehen bzw. die Root-Cause-Analyse noch nicht abgeschlossen ist. In der Abschlussmeldung müssen unter anderem die Ursache des Vorfalls, getroffene Maßnahmen sowie entstandene Kosten und Verluste enthalten sein. Konkret müssen Finanzunternehmen gemäß Art. 5 RTS-E im Abschlussbericht folgende Informationen über den Vorfall bereitstellen:[23]

1. Informationen über die Hauptursache des Vorfalls;
2. Informationen über die Unfähigkeit, gesetzlichen Anforderungen zu entsprechen;
3. Informationen über die Verletzung von Vertragsvereinbarungen/Service-Level-Agreements (SLAs);
4. Datum und Uhrzeit, zu denen der Vorfall behoben wurde und die Hauptursache adressiert wurde;
5. Informationen über die vom Finanzunternehmen ergriffenen Maßnahmen zur Behebung des Vorfalls sowie zusätzliche Kontrollen zur Verhinderung ähnlicher Vorfälle in der Zukunft;

16 EK, 2024, Delegierte Verordnung (EU) 2024/1772 (13.3.2024).

17 EBA, EIOPA, ESMA, Joint Committee of the European Supervising Authorities, 2024, S. 16.

18 EBA, EIOPA, ESMA, Joint Committee of the European Supervising Authorities, 2024, S. 17.

19 *Queng/Göddecke*, BaFin-IT-Aufsicht, 2024, Transparenz dank Meldepflicht, in: BaFinJournal (18.6.2024), abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_0618_DORA.html;jsessionid=4AF042FED6AB35DAD8C11E2945E69FD6.internet011.

20 *Göddecke*, 2024, S. 15.

21 *Göddecke*, 2024, S. 7.

22 *Göddecke*, 2024, S. 7.

23 EBA, EIOPA, ESMA, Joint Committee of the European Supervising Authorities, 2024, S. 18.

6. Informationen über die Herabstufung eines schwerwiegenden Vorfalls zu einem nicht schwerwiegenden Vorfall, sofern zutreffend;
7. Informationen, die für Abwicklungsbehörden relevant sind; und
8. Informationen über direkte und indirekte Kosten und Verluste, die durch den Vorfall entstanden sind, sowie Angaben über finanzielle Erstattungen.

Das Konsultationspapier stellt im Annex I Templates und Tabellen zur Verfügung, mit denen die Datenfelder für die verschiedenen Meldungen sowie allgemeine Informationen erfasst und abgefragt werden können.[24]

III. Fristen gemäß DORA-VO und ITS-E

Eine Übereinstimmung der Fristen für die Meldepflichten mit der NIS-2-Richtlinie wäre wünschenswert, da einige Unternehmen, die unter die DORA-VO fallen, auch von der NIS-2-Richtlinie betroffen sind. Bewusst hat man sich bei der Formulierung von RTS und ITS jedoch für teilweise abweichende Vorgaben entschieden. Während gemäß NIS-2 die erste Meldung innerhalb von 24 Stunden nach Entdeckung erfolgen muss, gilt unter der DORA-VO die Frist für die Einreichung der Erstmeldung ab dem Zeitpunkt der Klassifizierung des Vorfalls als schwerwiegender IKT-bezogener Vorfall: vier Stunden Frist für die Erstmeldung ab dem Moment der Klassifizierung – jedoch nicht später als 24 Stunden nach der Entdeckung des Vorfalls. Der Abschlussbericht muss gemäß NIS-2 innerhalb von 20 Arbeitstagen eingereicht werden, während unter der DORA-VO eine Frist von einem Monat gilt.[25] Zur Vermeidung von Doppelmeldungen ist eine Meldung an die BaFin vorgesehen, die wiederum direkt (automatisiert) an das BSI, ESAs etc. sowie – insofern relevant – an „weitere" Institutionen wie die Deutsche Bundesbank, die EZB und so mittelbar auch an die European Union Agency for Cybersecurity (ENISA) weitergeleitet wird.[26] Die automatische Weiterleitung der Meldung an andere Behörden, wie das BSI, stellt eine effiziente, gemeinsame Lagebewertung sicher.

Da sich die Anforderungen aus der DORA-VO und NIS-2-Richtlinie teilweise überschneiden, greift die Lex-specialis-Regelung, wie die BaFin erläutert: „Finanzunternehmen, die unter die NIS-2-Richtlinie fallen, müssen [...] künftig nur eine Vorfallsmeldung gemäß DORA bei der BaFin einreichen. Die BaFin stellt die Meldung unverzüglich dem BSI zur Verfügung."[27]

IV. Pflichten nach der DORA-VO im Spannungsverhältnis mit der DSGVO

Art. 19 DORA-VO legt dem Finanzsektor umfangreiche Meldepflichten auf. Für die Erfüllung der Meldepflicht werden in Art. 17 DORA-VO im Finanzsektor interne und externe Prozesse etabliert, die ein umfangreiches Monitoring und Vorfalls-Auswertungen erfordern. Um diesen Anforderungen gerecht zu werden, sind erhebliche Anstrengungen für den Einsatz von Protokollierungssystemen und Angriffs- und Früherkennungssyteme einzusetzen. Zugleich ist es geboten, die vorhandenen Informationen so auszuwerten, dass heute übliche Angriffe, deren Entwicklung immer neuere Wege nimmt, möglichst zuverlässig erkannt werden. Die Angriffswege werden von den Akteuren so ausgebaut, dass eine möglichst geringe Entdeckungsgefahr vorhanden ist. Gerade bei Hochwertzielen wie großen Banken sind besondere Anstrengungen der Akteure erkennbar. Regelmäßig versuchen die Akteure die etablierten Erkennungsmethoden zu umgehen.[28] Die angewendeten Methoden sind dabei von höchster Professionalität, Geduld und Umgehung der Erkennbarkeit gekennzeichnet. Die Akteure setzen vielfach auf den Angriff von schlecht gesicherten Sekundärnetzen (z. B. Homeoffice, oder Dienstleister mit schlecht gesichertem System) über den Einsatz von Social-Engineering.[29] Diese Methoden werden regelmäßig in besonderen Situationen der Zielpersonen u. a. auf Geschäftsreisen eingesetzt.[30] Spear-Phishing-Angriffe werden nicht mehr direkt auf Primärziele durchgeführt. Es werden Sekundärziele aus dem sozialen Umfeld als Brücken zu den Primärzielen genutzt, um vertrauenswürdige Beziehungen auszunutzen.[31] Leicht erkennbare Brute-Force-Angriffe gehen dabei zurück, wobei der Einsatz von Passwort-Spraying[32] an Bedeutung gewinnt.

Diesen bekannten und erprobten Aktivitäten der Akteure setzt die DORA-VO durch rechtlich vorgeschriebene Maßnahmen zur Detektion, Analyse und Meldung eine Transparenz-Offensive entgegen. Zugleich hält die DORA-VO an der uneingeschränkten Gültigkeit der DSGVO in Art. 45 Abs. 1 lit. c DORA-VO und explizit in Art. 56 Abs. 1 DORA-VO fest. Damit befinden sich beide Verordnungen in einem Spannungsfeld zwischen wirksamer Detektion von Anomalien (Art. 10 Abs. 1 DORA-VO) und der Beachtung des Datenschutzes nach der DSGVO.

1. Mögliche Rechtsgrundlage bei Inzidenten mit DSGVO-Bezug

Als Befugnisnorm für die Datenverarbeitung durch das verantwortliche Geldinstitut zum Zwecke der Erkennung von IKT-Risiken könnten Art. 6 Abs. 1 S. 1 lit. a und f DSGVO in Betracht kommen.

24 Vgl. EBA, EIOPA, ESMA, Joint Committee of the European Supervising Authorities, 2024, S. 25–29.

25 EBA, EIOPA, ESMA, Joint Committee of the European Supervising Authorities, 2024, S. 8–9, 94.

26 *Göddecke*, 2024, S. 18.

27 *Queng/Göddecke*, 2024.

28 Abrufbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-02-bfv-cyber-brief.html.

29 Abrufbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-08-infoblatt-social-engineering-leitungsebene.pdf?__blob=publicationFile&v=2.

30 Abrufbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2022-05-24-infoblatt-geschaeftsreisen-allgemein.html.

31 Abrufbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-02-bfv-cyber-brief.pdf?__blob=publicationFile&v=6.

32 Abrufbar unter: https://www.computerweekly.com/de/meinung/So-funktioniert-Password-Spraying-und-so-schuetzt-man-sich.

a) Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO?

Eine Einwilligung als Rechtsgrundlage in die erforderliche Datenverarbeitung zum Zwecke der IKT-Sicherheit dürfte insbesondere bei älteren Verträgen mit den Kunden nicht in Betracht kommen, weil in den Alt-Verträgen eine solche Einwilligung höchstwahrscheinlich nicht vorgesehen war. Der EuGH hat im Urteil C-252/21[33] für die Einwilligung entschieden, dass eine Einwilligung nur dann wirksam ist, wenn die Zwecke der Datenverarbeitung – in enger Auslegung – bestimmt sind und die Einwilligung unmissverständlich und freiwillig vorliegt.[34] Eine fehlende Einwilligung in vollständiger Kenntnis der Zwecke der Datenverarbeitung führt zur Rechtswidrigkeit der Datenverarbeitung.[35] In diesem Zusammenhang sind die in Art. 6 Abs. 1 S. 1 lit. b bis f DSGVO vorgesehenen Rechtfertigungsgründe eng auszulegen.[36] Die Einwilligung muss dabei vor der Datenverarbeitung vorliegen. Die Datenschutzerklärung z. B. der DKB[37] nennt diese Zwecke nicht, sodass in eine Datenverarbeitung zu den zuvor genannten Zwecken nicht rechtswirksam eingewilligt werden kann.

b) Berechtigtes Interesse gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO?

In der Auslegung von Art. 6 Abs. 1 S. 1 lit. f DSGVO könnte im Zusammenspiel mit Erwägungsgrund 49 der DSGVO die Sicherheit der Informationsnetze ein berechtigtes Interesse darstellen und somit als Rechtsgrundlage der Datenverarbeitung gelten. Das berechtigte Interesse wäre für jeden einzelnen Fall und für jedes einzelne Datum abzuwägen. Das Ergebnis dieser Abwägung wirkt sich auf die Betroffenen aus, aber auch auf den Verantwortlichen, denn dieser muss dann nachweisen, dass die Datenverarbeitung wirklich erforderlich ist.[38] Zu beachten ist im Finanzsektor, dass es sich bei den Daten der Betroffenen um sensible Daten handelt.[39] Der Weg über Art. 6 Abs. 1 S. 1 lit. f DSGVO ist möglich, jedoch mit erheblichen Aufwendungen und Risiken für die Verantwortlichen verbunden. Art. 6 Abs. 1 S. 1 lit. f DSGVO steht einem Wirtschaftssubjekt dann nicht zur Verfügung, wenn dieses die Datenverarbeitung auf die Verfolgung oder Verhinderung von Straftaten stützt.[40]

c) Zur Erfüllung einer rechtlichen Verpflichtung gem. Art. 6 Abs. 1 S. 1 lit. c DSGVO?

In Betracht käme vorliegend allerdings Art. 6 Abs. 1 S. 1 lit. c DSGVO, um die Datenverarbeitung zu Zwecken der Protokollierung, Detektion und Anomalie-Erkennung durch Geldinstitute zu legitimieren. Art. 6 Abs. 1 S. 1 lit. c DSGVO legitimiert die Datenverarbeitung für die aus Rechtsvorschriften folgende Rechtspflicht.[41] Der Umfang der Regelung ist dabei umstritten. Keine Rechtspflichten sollen sich aus vertraglichen Pflichten ergeben.[42] Auch behördliche Anordnungen zur Datenverarbeitung und Datenweitergabe, sofern diese nicht unter die JI/RL fallen, sollen nicht unter Art. 6 S. 1 lit. c subsumierbar sein.[43] Diese Meinung ist jedoch umstritten, die Gegenauffassung wird in der Literatur vertreten.[44]

Ein konkretes Beispiel für eine rechtliche Verpflichtung zur Datenverarbeitung nach Art. 6 Abs. 1 S. 1 lit. c DSGVO gibt die DSGVO mit Art. 15 DSGVO selbst. Art. 15 DSGVO legt dem Verantwortlichen die Pflicht auf, die Daten im Sinne der Legaldefinition nach Art. 4 Nr. 2 DSGVO zu Zwecken der Auskunft an den Betroffenen herauszugeben.

Eine vorliegende rechtliche Verpflichtung für die Datenverarbeitung durch die verantwortlichen Kreditinstitute wäre jedoch der rechtssichere Weg und würde das Risiko für Sanktionen der Datenschutzbehörden und Schadensersatzklagen vermindern. Risikofrei wird die Datenverarbeitung jedoch nicht. Das Bundessozialgericht (BSG) vertritt die Auffassung, dass Gesetze und Verordnungen im Geltungsbereich der DSGVO dem Verantwortlichen zumindest Restrisiken hinsichtlich der vollständigen Umsetzung der DSGVO aufbürden.[45] Ob diese Wertung des BSG einer verfassungsrechtlichen Prüfung standhalten würde, darf durchaus bezweifelt werden. Das BSG argumentiert, dass nur ein geringes Risiko für Sanktionen bestehen würde, weil es schwierig sei, u. a. das Verschulden bei einem Datenschutzverstoß nachzuweisen. Diese Schlussfolgerung des BSG dürfte jedoch schwer mit dem Grundsatz der Normenklarheit und Normenwahrheit in Einklang zu bringen sein, da die Vorhersehbarkeit von Sanktionen für die Verantwortlichen nicht einschätzbar ist.[46]

Grundsätzlich stellen die Anforderungen der DORA-VO, nach der Rechtsansicht der Autorinnen und des Autors, im Sinne der DSGVO eine rechtliche Verpflichtung in Sinne des Art. 6 Abs. 1 S. 1 lit. c DSGVO dar, welcher die Verantwortlichen i. S. d. Art. 4 Nr. 7 DSGVO unterliegen.

2. Zu beachtende Prinzipien aus der DSGVO

Das Kriterium der Datenminimierung[47] ist zu beachten. Einen ähnlichen Schutzzweck erfüllt das Prinzip der Erforderlichkeit der Datenverarbeitung. Denn nur Daten, die unbedingt erforderlich sind, dürfen verarbeitet werden. Im Hinblick auf die Risikomanagementsysteme zur Anomalie-Erkennung und Zugriffsbeschränkungen z. B. durch Blacklisten stellt der EuGH für solche Daten, die nicht vom Verantwortlichen selbst erhoben wurden, sogenannte Off-Site-Daten – z. B. für Bekannte übernommene Endgeräte[48] – erhebliche Hürden für eine rechtmäßige Datenverarbeitung

33 EuGH, Urt. v. 04.07.2024, C-252/21 – Meta ./. Bundeskartellamt.
34 EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 92.
35 Generalanwalt Szpunar in EuGH, C-394/23, Rn. 35.
36 Wörtliches Zitat aus: EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 93.
37 Abrufbar unter: https://dok.dkb.de/pdf/Information_nach_Art13.pdf.
38 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO, 4. Aufl. 2024, Art. 6, Rn. 149.
39 *Britz/Indenhuck/Langerhans*, Die Verarbeitung „zufällig" sensibler Daten, ZD 2021, S. 559 ff.
40 EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 124.
41 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO, 4. Aufl. 2024, Art. 6, Rn. 76.
42 *Schulz*, in: Gola/Heckmann, DS-GVO, 3. Aufl. 2022, Art. 6, Rn. 46; so auch *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 3. Aufl. 2024, Art. 6, Rn. 30.
43 *Schulz*, in: Gola/Heckmann, DS-GVO, 3. Aufl. 2022, Art. 6, Rn. 46.
44 *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 3. Aufl. 2024, Art. 6, Rn. 29.
45 BSG, Urt. v. 06.03.2024 – B 6 KA 23/22 R, BeckRS 2024, 21615, Rn. 57.
46 *Eichberger*, in Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 2, Rn. 294; BVerfG, Urt. v. 19.5.2020 – 1 BvR 2835/17, BVerfGE 154, 152 (237 ff., Rn. 137 ff.).
47 Art. 5 Abs. 1 lit. c DSGVO.
48 Abrufbar unter: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-02-bfv-cyber-brief.pdf?__blob=publicationFile&v=6.

auf.[49] Eine Definition der Erforderlichkeit der Datenverarbeitung gibt der EuGH vor. Sinngemäß konstatiert er die Erforderlichkeit der Datenverarbeitung so, dass die Datenverarbeitung immer dann als erforderlich angesehen werden kann, wenn der Zweck der Datenverarbeitung ohne das einzelne Datum nicht oder nur mit unzumutbarem Aufwand erreicht werden kann.[50] Die Speicherung der Daten stellt einen dauerhaften Grundrechtseingriff in die Rechte der Betroffenen dar.[51] Zugleich kommt hinzu, dass auch die weitergehende Speicherung von Daten eine Datenverarbeitung ist, die erforderlich, verhältnismäßig und angemessen sein muss. Die zeitliche Beendigung der Datenverarbeitung muss erfolgen, sobald die Zweckerfüllung eingetreten ist.[52]

Das Spannungsverhältnis zwischen der Erforderlichkeit der Datenverarbeitung und der Datenminimierung zeigt sich nun in der DORA-VO an den auferlegten Protokollierungspflichten der Geldinstitute.[53] Das bekannte Verhalten von Akteuren ist insbesondere bei Hochwertzielen darauf ausgelegt, die Systeme langfristig und mit möglichst wenigen Spuren zu infiltrieren, aufzuklären und die Daten abfließen zu lassen. Die letzte Aktion der Akteure zur Beendigung der erkennbaren Infiltration ist, auch bei für die Akteure erkennbarer Entdeckung, die Verwischung von Spuren durch Verschlüsselung und eine damit zusammenhängend Erpressung.

Zeitlich angepasste Angriffsmuster, unter Ausnutzung von Social-Media-Informationen oder Abwesenheitsnachrichten außerhalb der Organisation für die An- und Abwesenheit relevanter personenbezogener Ziele, erfordern regelmäßig die langfristige Analyse von Protokolldaten. Gleiches gilt für Password-Spray-Attacken, die vermehrt in der Nähe von Ferienzeiten und Feiertagen zu erwarten sind. Hier gilt es bei besonderer Beachtung der Grundrechte aus Art. 7, 8 GRCh die Abwägung mit den Grundrechten aus Art. 15, 16, 17 GRCh in Einklang zu bringen. Diesen Spagat löst der Gesetzgeber, nach Meinung der Autorinnen und dem Autor, nicht detailliert auf und überlässt Restrisiken den Verantwortlichen. Der Gesetzgeber hätte in Kenntnis der tatsächlichen Bedrohungslage und des hochprofessionellen Agierens der Akteure klare zeitliche Mindestvorgaben für die Vorhaltung und Auswertung der Logfiles geben können. Mit klaren zeitlichen Mindestvorgaben, wie im aktuellen § 5 Abs. 2 BSIG geregelt, hätte der Gesetzgeber eine rechtliche Obliegenheit im Sinne von Art. 6 Abs. 1 S. 1 lit. c DSGVO geschaffen. Das BSG hat in der o. g. Rechtsprechung die Restrisiken schon dem Verantwortlichen aufgebürdet.

3. Informationspflichten nach der DSGVO

Der Verantwortliche hat auch bei der Ausführung der DORA-VO die betroffene Person über die Zweckänderung der Datenverarbeitung vor der Zweckänderung nach Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO zu informieren, um den Grundsatz der Transparenz zu wahren.

V. Fazit

Ob es um Meldepflichten für Sicherheitsvorfälle, Störungen oder „IKT-bezogene Vorfälle“ geht – eine Anpassung der Nomenklatur sowie eine klare Abgrenzung der Zuständigkeiten in den verschiedenen regulatorischen Vorgaben zur Cybersicherheit und Resilienz, wie der DORA-VO, dem KRITIS-DachG oder dem NIS2UmsuCG, wäre wünschenswert. Mit der zunehmenden begrifflichen Diversifizierung driftet auch der Modus Operandi für die Operationalisierung der Meldepflichten in den unterschiedlichen Regelwerken auseinander. Das ursprüngliche Ziel der DSGVO-Pioniere das Incident-Management in Unternehmen in einen effektiven und effizienten Prozess zu integrieren, rückt dadurch zunehmend in die Ferne.

Obwohl der Gesetzgeber mit dem NIS2UmsuCG mehr Transparenz und Bürokratieabbau versprach und nach der Verbändeanhörung im Juni 2024 in Aussicht stellte, „das Meldewesen klarer und leichter gestalten zu wollen“[54], wurde im Regierungsentwurf des NIS-2-Umsetzungsgesetzes vom 22.07.2024 die Chance nicht genutzt, die Vorgaben mit weiteren Regulatorien abzugleichen. Im Rahmen der Konsultation zur DORA-VO wurde auf die Überschneidung der Meldepflichten mit der NIS-2-Richtlinie hingewiesen. Dennoch entschied man sich – unionsweit – für eine abweichende Lösung.

Die bestehenden und etablierten Meldepflichten für Datenpannen gemäß der DSGVO wurden, nach aktuellem Stand, weder in den Konsultationen zur DORA-VO noch im Regierungsentwurf des NIS2UmsuCG berücksichtigt. Dies dürfte sich künftig infolge der Stellungnahme des Bundesrates zum NIS-2-Umsetzungsgesetz vom 27.9.2024 ändern.[55] Darin greift der Bundesrat den Gedanken aus dem Erwägungsgrund 106 der NIS-2-Richtlinie auf, in dem den Mitgliedstaaten nahegelegt wird, die zentrale Meldestelle für Sicherheitsvorfälle auch für die nach Art. 33 DSGVO erforderlichen Meldungen zu nutzen. Eine Bündelung sollte dem Zweck dienen, zusätzlichen Verwaltungs- bzw. Bürokratieaufwand zu verhindern. Hierzu ist es laut Bundesrat notwendig, den § 40 Abs. 3 Nr. 5 BSIG-E um die Pflicht zu ergänzen, „geeignete Online-Formulare“ für eine zeitgleiche Meldung nach Art. 33 DSGVO und § 32 BSIG-E zur Verfügung zu stellen.

Damit wäre zunächst eine Verknüpfung beider Meldepflichten auf der operativen Ebene möglich. Ein Blick auf bewährte Praktiken und Erfahrungen zu den Meldepflichten für Datenpannen würde dem Gesetzgeber möglicherweise die Aufgabe, das Vorfallsmeldewesen für die Sicherheitsvorfälle zu definieren, erleichtern und die beiden Themen – Datenschutz und Cybersicherheit – (wenigsten operationell) einander näherzubringen.

49 EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 120.
50 EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 108, 109, 121.
51 Art. 5 Abs. 1 lit. e DSGVO.
52 *Herbst*, in: Kühling/Buchner, DS-GVO, 4. Aufl. 2024, Art. 5, Rn. 64.
53 Art. 6 Abs. 2 DORA-VO.
54 *Stiebel*, NIS-2-Umsetzung dreht noch eine Runde. In: Tagesspiegel Background (6.6.2024), abrufbar unter: https://background.tagesspiegel.de/cybersecurity/nis-2-umsetzung-dreht-noch-eine-runde.
55 Vgl. Bundesrat, 2024, Stellungnahme v. 27.9.2024 (Drs. 380/24), abrufbar unter: https://www.bundesrat.de/SharedDocs/drucksachen/2024/0301-0400/380-24(B).pdf.