5/2024
97 – 120

FAQ
Datenschutzerklärung
Viktoria Haidinger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Transparenz

500 Auskünfte pro Tag!
Interview mit Gerhard Wagner, KSV1870 Information GmbH

Datenschutzinformation Gegenstand von Cyber Risk Ratings
Gregor König

Datenportabilität (DSGVO) und Datenzugang (Data Act) im Vergleich
Rainer Knyrim und Stephanie Briegl

Personenbezug statistischer Wahrscheinlichkeitswerte
Janos Böszörmenyi

Abwägung von Grundrechten bei KI-Anwendungen
Lisa Seidl

Checkliste DORA (Teil 1)
Hans-Jürgen Pollirer

ISSN 2313-5409
dako.manz.at
MANZ 175 Jahre

sonderer (europäischer wie nationaler) Rechtsvorschriften, die jedoch angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten müssen.[19]

Eine **vom Gesetzgeber geregelte Maßnahme** könnte zB eine Risikobewertung im Rahmen einer GRFA oder die Vorgabe der Einhaltung von nationalen wie internationalen Standards (wie ÖNormen, DIN, ISO usw) sein, die auch Risikoabschätzungen und grundrechtliche Mindestanforderungen beinhalten können.[20] Auch könnte die Judikatur oder die Lit – wie im Datenschutzrecht nicht ungewöhnlich – in Zukunft noch viel zur Auslegung unbestimmter Begriffe beitragen und Anforderungen an die Einhaltung von Grundrechten und -freiheiten konkretisieren.[21]

Conclusio

Somit lässt sich sagen, dass die Regelungen über die GRFA nach der letztlich in Kraft getretenen KI-VO nur eingeschränkt Anwendung finden, jedoch bestehen für risikoreiche Systeme trotzdem Vorgaben über Risikoabschätzungen, die das Kernstück einer GRFA – die Risikobeurteilung und die Maßnahmen zur Minderung der Grundrechtsrisiken – beinhalten müssen.

Dako 2024/51

[19] Nach ErwGr 140 KI-VO soll die KI-VO jedoch explizit keine solche Rechtsgrundlage bilden. [20] ZB Leitlinien für Risikomanagement (ISO/IEC 23894:2023). [21] Vgl *Jahnel*, Datenschutzrechtliche Grenzen des Einsatzes von KI-unterstützten Legal Tech Tools, ÖZW 2023, 117.

Zum Thema

Über die Autorin

Lisa Seidl, LL.M. (WU), ist Juristin mit Spezialisierung auf Grund- und Menschenrechte und Digitalisierung. Sie hat Erfahrung mit Grundrechtsabwägungen im Rahmen von Datenschutz-Folgenabschätzungen im Hinblick auf den Einsatz von künstlicher Intelligenz und ist im Bundeskanzleramt Sektion VII Digitalisierung und E-Government tätig.
E-Mail: lisa.seidl@bka.gv.at

Hinweis

Dieser Beitrag stellt die persönliche Meinung der Autorin und nicht ihres Arbeitgebers dar.

Links (Stand aller Links 30. 7. 2024)

- **Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html;**
- **EPRS, The impact of the General Data Protection Regulation (GDPR) on artificial intelligenc (2020), www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf;**
- **Ministry of the Interior and Kingdom Relations, Impact Assessment Fundamental rights and algorithms (2022), www.government.nl/documents/reports/2022/03/31/impact-assessment-fundamental-rights-and-algorithms;**
- ***EDPB*, Report of the work undertaken by the ChatGPT Taskforce (2024), www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf.**

Hans-Jürgen Pollirer
Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste DORA (Teil 1)

Anwendungsbereich; risikobasierter Ansatz; Dokumentation; Qualitätsmanagementsystem; Transparenzpflichten. Mit der Checkliste werden die wichtigsten Maßnahmen bei der Umsetzung der DORA-VO für Finanzunternehmen aufgezeigt. Sie kann eine eingehende Auseinandersetzung mit dieser Rechtsmaterie und mit den technischen Regulierungsstandards (RTS) und Durchführungsstandards (ITS) nicht ersetzen.

Entstehungsgeschichte DORA

Am 16. 1. 2023 ist die VO (EU) 2022/2554 des EP und des Rates vom 14. 12. 2022 über die Betriebsstabilität digitaler Systeme des Finanzsektors („Digital Operational Resilience Act"; DORA) in Kraft getreten[1] und von den betroffenen Unternehmen ab 17. 1. 2025 verpflichtend anzuwenden. Mit DORA sollen bestehende regulatorische Lücken für den gesamten europäischen Finanzsektor geschlossen und die Betriebsstabilität im Finanzsektor gestärkt werden. Mit gleichem Datum trat auch die RL (EU) 2022/2556 zur Änderung der RL 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EG, 2014/65/EG, (EU) 2015/2366 und (EU) 2016/2341 in Kraft,[2] die Bestimmungen zum Management von IKT-Risiken betreffen. Diese Änderungen sind deshalb

[1] https://kurzlinks.de/67uk. [2] https://kurzlinks.de/17oi.

notwendig geworden, weil viele Bestimmungen uneinheitlich und teilweise lückenhaft waren und die Kohärenz mit DORA hergestellt werden soll. Aufgrund der in DORA enthaltenen Ermächtigung für die EK wurden noch folgende Rechtsakte erlassen:

- Delegierte VO (EU) 2024/1502 der EK vom 22. 2. 2024[3] zur Ergänzung der VO (EU) 2022/2554 des EP und des Rates durch Festlegung der Kriterien für die Einstufung von IKT-Drittdienstleistern als für Finanzunternehmen kritisch;
- Delegierte VO (EU) 2024/1505 der EK vom 22. 2. 2024[4] zur Ergänzung der VO (EU) 2022/2554 des EP und des Rates durch Festlegung der Höhe der von der federführenden Überwachungsbehörde bei kritischen IKT-Drittdienstleistern zu erhebenden Überwachungsgebühren und der Art und Weise der Entrichtung dieser Gebühren.

Umsetzung in Österreich

Zum Wirksamwerden der DORA-VO wurde vom österr Gesetzgeber am 18. 4. 2024 ein Vollzugsgesetz (DORA-Vollzugsgesetz, DORA-VG) veröffentlicht, das im Finanzausschuss am 27. 6. 2024 die Stimmenmehrheit von ÖVP, SPÖ, Grünen und Neos erhielt und am 3. 7. 2024 im NR beschlossen wurde.[5] Das Gesetz soll insb den Anwendungsbereich der DORA-VO in Bezug auf die nationalen Institute klarstellen.

In Österreich ist die **Finanzmarktaufsicht** (FMA) für den Vollzug von DORA zuständig.

Durch die von den Unternehmen aufgrund der in DORA normierten Bestimmungen umzusetzenden Maßnahmen sollen folgende **Ziele** erreicht werden:

- IKT-Risikomanagement (Kapitel II, Art 5 bis 16);
- Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III, Art 17 bis 23);
- Testen der digitalen operationellen Resilienz einschließlich Threat-led Penetration Testing (TLPT) (Kapitel IV, Art 24 bis 27);
- Management des IKT-Drittparteienrisikos (Kapitel V, Abschnitt I, Art 28 bis 30);
- Überwachungsrahmen für kritische IKT-Drittdienstleister (Kapitel V, Abschnitt II, Art 31 bis 44);
- Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen (Kapitel VI, Art 45).

Abgrenzung NIS-2-RL und DORA

Grundsätzlich stellt sich die Frage, warum die EU zwei Rechtsvorschriften für Cybersicherheit, nämlich die NIS-2-RL und die DORA-VO, erlassen hat, die auf den ersten Blick ähnlich anmuten. Bei näherer Betrachtung dieser beiden Rechtsvorschriften zeigen sich jedoch einige **wesentliche Unterschiede:**

- Während NIS-2 als RL in nationales Recht umgesetzt werden muss,[6] handelt es sich bei DORA um eine VO, die zeitgleich für alle MS in Kraft tritt und unverändert in ihrer Gesamtheit durchgesetzt werden muss.
- Während die NIS-2 RL veröffentlicht wurde, um das allgemeine Niveau der Cybersicherheit in der EU zu vereinheitlichen, was durch NIS-1 nicht gelungen war, soll die Umsetzung der in der DORA-VO normierten Anforderungen im europäischen Finanzsektor sicherstellen und diesen in die Lage versetzen, Cyberangriffen standzuhalten und betriebsfähig zu bleiben. Der Fokus der DORA-VO liegt daher auf der Verfügbarkeit und Integrität von Finanzdienstleistungen.
- Auch in Bezug auf den Umsetzungszeitpunkt ergeben sich Unterschiede sowie in der Behördenzuständigkeit.
- Während die Bußgelder in der NIS-2-RL festgelegt sind, wird in der DORA-VO die Festlegung und Bewertung der Sanktionen den MS überlassen.

Die DORA-VO legt besonderen Wert auf die Sicherheit der Lieferkette und geht über die Anforderungen der NIS-2-RL weiter hinaus. So müssen Finanzunternehmen die Risiken über die **gesamte** Lieferkette hinaus identifizieren und in entsprechenden Verzeichnissen dokumentieren. Verträge mit IKT-Dienstleistungsunternehmen dürfen nur mit jenen abgeschlossen werden, die über einen hohen und aktuellen Informationssicherheitsstandard verfügen.

Anwendungsbereich

Die DORA-VO gilt – mit wenigen Ausnahmen – grundsätzlich für alle regulierten Finanzunternehmen in der EU und insb auch für IKT-Dienstleister, die von diesen Unternehmen eingesetzt werden. Als lex speciales geht die DORA-VO aber der NIS-2-RL vor. Nichtsdestotrotz kann es zu Mehrfachregulierungen kommen, und zwar für Unternehmen im IT- und TK-Sektor, die sowohl als NIS-2-Einrichtungen und als auch als kritische IKT-Dienstleister gem der DORA-VO gelten.

Im Einzelnen sind gem § 2 DORA-VG, der die in Art 2 DORA-VO angeführten Unternehmen um die geltenden nationalen und europäischen Rechtsgrundlagen ergänzt, folgende **Unternehmen des Finanzsektors** betroffen: Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Wertpapierfirmen, Anbieter von Kryptowerte-Dienstleistungen und Emittenten von vermögenswertreferenzierten Token, Zentralverwahrer, zentrale Gegenparteien über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, Handelsplätze, Datenbereitstellungsdienste, AIFM, Verwaltungsgesellschaften, Unternehmen gem § 1 Z 1 VAG, Pensionskassen, Administratoren kritischer Referenzwerte sowie Schwarmfinanzierungsdienstleister. Somit fallen so gut wie alle beaufsichtigten Unternehmen des europäischen Finanzsektors unter die Bestimmungen der DORA-VO. Darüber hinaus sind auch die kritischen IKT-Dienstleister, die für Finanzunternehmen tätig sind, von der DORA-VO betroffen, wobei die Einstufung als „kritisch" im Rahmen des europäischen Finanzaufsichtssystems erfolgt.

Regulierungs- und Durchführungsstandards

Die Anforderungen, die die DORA-VO an Finanzunternehmen mit Geschäftstätigkeit in der EU festlegt, werden in technischen Regulierungsstandards (regulatory technical standards, „RTS") und Durchführungsstandards (implementing technical standards, „ITS") konkretisiert. Die drei europäischen Aufsichtsbehörden European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) und die European Securities and Markets Authority (ESMA) haben am 17. 1. 2024 die ersten finalen Entwürfe der ersten Welle RTS und ITS der EK vorgelegt, die **folgende Bereiche betreffen:**[7]

- Final report on draft RTS on classification of major incidents and significant cyber threats;
- Final report on draft RTS to specify the policy on ICT services supporting critical or important function;
- Final report on draft RTS on ICT Risk Management Framework and on simp-

[3] https://kurzlinks.de/a87p [4] https://kurzlinks.de/tg5q
[5] https://kurzlinks.de/xvd8 [6] *Pollirer*, Checkliste NIS-2, Dako 2024/43. [7] https://kurzlinks.de/e3tk

lified ICT Risk Management Framework;
- Final report on draft ITS on Register of Information;
- Register of Information Templates in Excel format for illustration purposes.

Mit 17. 7. 2024[8] bzw 26. 7. 2024[9] wurden die finalen Entwürfe der **zweiten Welle der RTS und ITS** der EK vorgelegt, die folgende Bereiche betreffen:

- Final report on GL on oversight cooperation;
- Final report GL on costs and losses;
- Final Report RTS on JET;
- Final report on RTS on harmonisation of conditions for OVS conduct;
- Final report on the draft RTS and ITS on incident reporting;
- Final report DORA RTS on TLPT;
- Final report DORA RTS on subcontracting;

Mit der Checkliste werden die wichtigsten Maßnahmen bei der Umsetzung der DORA-VO für Finanzunternehmen aufgezeigt. Sie stellt jedoch keine umfassende und vollständige Dokumentation dar und kann für die betroffenen Finanzunternehmen eine eingehende Auseinandersetzung mit dieser komplexen und umfangreichen Rechtsmaterie und va mit den technischen Regulierungsstandards (RTS) und Durchführungsstandards (ITS) nicht ersetzen.

[8] https://kurzlinks.de/f01z [9] https://kurzlinks.de/dxlh

Prüffragen

Prüffragen	ja	nein
Governance		
Frage 1: Verfügt das Finanzunternehmen über eine Leitlinie zur internen Governance und einen entsprechenden Kontrollrahmen? ***Anmerkung:*** *Art 5 Abs 1 DORA-VO fordert vom Finanzunternehmen, dass es über einen internen Governance- und Kontrollrahmen verfügt, der ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet. Zielsetzung ist das Erreichen eines hohen Niveaus an digitaler operationaler Resilienz. Abs 2 enthält die detaillierten Verantwortlichkeiten und Pflichten des Leitungsorgans. Eine Definition des Begriffs „Leitungsorgan" findet sich in Art 3 Z 30 DORA-VO. Verantwortlich für die Definition, Genehmigung, Überwachung und Umsetzung ist das Leitungsorgan des Finanzunternehmens. Das Leitungsorgan muss Leitlinien einführen, die hohe Standards in Bezug auf die Verfügbarkeit, Authentizität und Vertraulichkeit von Daten gewährleisten.*		
Frage 2: Hat das Leitungsorgan klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen festgelegt? ***Anmerkung:*** *Gem Art 5 Abs 2 DORA-VO soll durch diese Maßnahme eine wirksame und rechtzeitige Kommunikation, Zusammenarbeit und Koordination zwischen diesen Funktionen erreicht werden.*		
Frage 3: Nimmt das Leitungsorgan seine Genehmigungs-, Überwachungs- und Prüfungsaufgaben wahr? ***Anmerkung:*** *Das Leitungsorgan ist für die Genehmigung, Überwachung und Prüfung der Umsetzung der IKT-Geschäftsfortführungsrichtlinie (Art 11 Abs 1 DORA-VO), der IKT-Reaktions- und -Wiederherstellungspläne (Art 11 Abs 3 DORA-VO) sowie für die internen IKT-Revisionspläne, die IKT-Revision und die Budgetmittel verantwortlich.*		
Frage 4: Werden die Mitarbeiter des Leitungsorgans regelmäßig in IKT-Risiken geschult? ***Anmerkung:*** *Im Finanzunternehmen sind Schulungsprogramme zur Sensibilisierung für IKT-Sicherheit sowie zur digitalen operationalen Resilienz und der IKT-Kompetenzen für alle Mitarbeiter gem Art 13 Abs 6 DORA-VO durchzuführen.*		
Frage 5: Verfügt das Finanzunternehmen über eine Leitlinie für die Nutzung von IKT-Dienstleistungen? ***Anmerkung:*** *Diese Leitlinie in Bezug auf Vereinbarungen über die Nutzung von IKT-Dienstleistungen ist vom Leitungsorgan regelmäßig zu überprüfen.*		
Frage 6: Wurden auf Unternehmensebene Meldekanäle in Bezug auf die IKT-Dienstleister eingerichtet? ***Anmerkung:*** *Diese Meldekanäle müssen das Leitungsorgan über die mit IKT-Dienstleistern abgeschlossenen Verträge sowie über alle geplanten wesentlichen Änderungen in Bezug auf diese Verträge informieren. Über die Auswirkungen dieser Änderungen ist eine Risikoanalyse durchzuführen.*		
IKT-Risikomanagement		
Frage 7: Verfügt das Finanzunternehmen über einen soliden, umfassenden und gut dokumentierten IKT-Risikorahmen? ***Anmerkung:*** *Zur Gewährleistung eines hohen Niveaus an digitaler operationaler Resilienz muss das Finanzunternehmen gem Art 6 Abs 1 DORA-VO über einen IKT-Risikorahmen als Teil des Gesamtrisikomanagementsystems verfügen.*		
Frage 8: Verfügt das Finanzunternehmen über das Management und die Überwachung des IKT-Risikos bei einer unabhängigen Stelle? ***Anmerkung:*** *Die Zuständigkeit für das Management und die IKT-Überwachung von IKT-Risiken ist gem Art 6 Abs 4 DORA-VO an eine unabhängige Kontrollfunktion zu übertragen. Weiters sind die IKT-Risikomanagementfunktionen, die Kontrollfunktionen und die internen Revisionsfunktionen zu trennen.*		
Frage 9: Enthält der IKT-Risikomanagementrahmen Maßnahmen, um alle eingesetzten IKT-Technologien ausreichend zu schützen? ***Anmerkung:*** *Der IKT-Risikomanagementrahmen muss gem Art 6 Abs 2 DORA-VO über Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools verfügen, um die IKT-Assets angemessen zu schützen. Weiters sind Auswirkungen von IKT-Risiken zu minimieren und gem Art 6 Abs 5 bis 7 DORA-VO ist der IKT-Risikomanagementrahmen mindestens jährlich zu überprüfen und kontinuierlich zu verbessern.*		
Frage 10: Umfasst der IKT-Risikomanagementrahmen eine Strategie für die digitale operationale Resilienz? ***Anmerkung:*** *Art 6 Abs 8 DORA-VO fordert, dass der IKT-Risikomanagementrahmen eine Strategie für die operationale Resilienz darlegt, und wie dieser Rahmen umgesetzt wird. Die Strategie hat die in Art 6 Abs 8 lit a bis h DORA-VO angeführten Maßnahmen zu enthalten.*		
Frage 11: Sind die eingesetzten IKT-Systeme, -protokolle, -Tools auf dem neuesten Stand? ***Anmerkung:*** *Art 7 lit a bis d DORA-VO fordert, dass die IKT-Systeme, -protokolle und -Tools zuverlässig, dem Umfang von Vorgängern, die für die Ausübung der Geschäftstätigkeit angemessen, über ausreichende Kapazitäten verfügen und technisch resilient sind.*		
Frage 12: Sind die Rollen und Verantwortlichkeiten risikobezogen analysiert und klassifiziert? ***Anmerkung:*** *Als Teil des IKT-Risikorahmens sind vom Finanzunternehmen gem Art 8 Abs 1 alle IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten sowie die Informations- und IKT-Assets zu ermitteln, zu klassifizieren und zu dokumentieren. Einmal jährlich ist zu prüfen, ob diese Klassifizierung und die Dokumentation angemessen sind.*		

Frage 13: Werden vom Finanzunternehmen kontinuierlich alle Quellen für IKT-Risiken ermittelt? ***Anmerkung:*** *Art 8 Abs 2 DORA-VO fordert vom Finanzunternehmen die kontinuierliche Ermittlung aller Quellen von IKT-Risiken, insb das Risiko gegenüber und von anderen Finanzunternehmen sowie eine Bewertung von Cyberbedrohungen und IKT-Schwachstellen. Diese Risikoszenarien sind jährlich zu überprüfen.*		
Frage 14: Wird für jede IKT-Infrastrukturänderung eine Risikobewertung durchgeführt? ***Anmerkung:*** *Art 8 Abs 3 DORA-VO fordert die Durchführung einer Risikobewertung bei jeder Änderung der Netzwerk- und Informationsinfrastruktur, der Prozesse oder Verfahren, die sich auf die Geschäftstätigkeit des Finanzunternehmens auswirken.*		
Frage 15: Werden alle Informations- und IKT-Assets ermittelt? ***Anmerkung:*** *Art 8 Abs 4 DORA-VO erfordert die Ermittlung aller Informations- und IKT-Assets sowie die Erfassung jener, die als kritisch gelten. Die Erfassung beschränkt sich nicht nur auf die Konfiguration, sondern auch auf die Interdependenzen.*		
Frage 16: Werden alle Prozesse, die von IKT-Dienstleistern abhängen, ermittelt und dokumentiert? ***Anmerkung:*** *Art 8 Abs 5 DORA-VO erfordert die Ermittlung und Dokumentation aller Prozesse, die von IKT-Dienstleistern abhängen, sowie die Vernetzungen von IKT-Dienstleistern, die Dienste zur Unterstützung kritischer oder wichtiger Funktionen bereitstellen.*		
Frage 17: Werden alle IKT-Altsysteme regelmäßig einer Risikobewertung unterzogen? ***Anmerkung:*** *Art 8 Abs 7 DORA-VO fordert regelmäßig, mindestens jedoch einmal jährlich, und jedenfalls vor und nach Anschluss von Technologien, Anwendungen oder Systemen, die Durchführung einer Risikobewertung.*		
Frage 18: Überwacht und kontrolliert das Finanzunternehmen kontinuierlich die Sicherheit und das Funktionieren der IKT-Systeme und -Tools? ***Anmerkung:*** *Gem Art 9 Abs 1 DORA-VO sind durch den Einsatz angemessener IKT-Sicherheitstools, -richtlinien und -verfahren die Auswirkungen von IKT-Risiken auf IKT-Systeme zu minimieren. Deren Wirksamkeit ist kontinuierlich zu überwachen und zu kontrollieren.*		
Frage 19: *Werden IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools implementiert, um die Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen aufrecht zu erhalten?* ***Anmerkung:*** *Durch diese Maßnahmen sollen gem Art 9 Abs 2 DORA-VO kritische und wichtige Funktionen gewährleistet und hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten sichergestellt werden.*		
Frage 20: Greift das Finanzunternehmen auf IKT-Lösungen und -Prozesse zurück, die gem Art 4 DORA-VO angemessen sind? ***Anmerkung:*** *Diese Lösungen entsprechen gem Art 9 Abs 3 lit a bis d DORA-VO den Anforderungen des Art 4 DORA-VO dann, wenn sie die Sicherheit der Datenübertragungsmittel gewährleisten, das Risiko des Datenverlustes oder der Datenkorruption minimieren sowie dem Mangel an Verfügbarkeit, die Beeinträchtigung der Authentizität und Integrität, Verletzungen der Vertraulichkeit und dem Datenverlust vorbeugen sowie Daten vor menschlichem Versagen schützen.*		
Frage 21: Wurde vom Finanzunternehmen eine Informationssicherheitsleitlinie erarbeitet und dokumentiert? ***Anmerkung****: Art 9 Abs 4 lit a DORA-VO fordert die Erarbeitung und Dokumentation einer Informationssicherheitsleitlinie, in der die Regeln zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und der Informations- und IKT-Assets – einschließlich für die Kunden Dritter – enthalten sind. Weitere Anforderungen an den Inhalt der Informationssicherheitsleitlinie sind in lit b bis f enthalten, wie ein angemessener risikobasierter Ansatz für das Netzwerk- und Infrastrukturmanagement, ein angemessenes Zugriffskontrollsystem auf IKT-Assets nach dem Need-to-Know-Prinzip, starke Authentisierungsmechanismen einschließlich Datenverschlüsselungsstrategien, Verfahren und Kontrollen für das IKT-Änderungsmanagement, Richtlinien für Patches und Updates.*		
Frage 22: Verfügt das Finanzunternehmen über Mechanismen, um anormale Aktivitäten umgehend zu erkennen? ***Anmerkung:*** *Art 10 Abs 1 DORA-VO fordert darüber hinaus, dass diese Erkennungsmechanismen gem Art 25 DORA-VO regelmäßig getestet werden. Abs 2 fordert die Festlegung mehrerer Kontrollebenen und Alarmschwellen und -kriterien, einschließlich automatischer Warnmechanismen, um die zuständigen Mitarbeiter zu benachrichtigen. Gem Abs 3 müssen Finanzunternehmen hiefür ausreichende Ressourcen und Kapazitäten zur Verfügung stellen. Abs 4 betrifft Datenbereitstellungsdienste und verpflichtet diese, Systeme einzurichten, damit deren Handelsauskünfte auf Vollständigkeit, Lücken und Fehler erkannt werden.*		
Frage 23: Verfügt das Finanzunternehmen im Rahmen des IKT-Risikomanagementrahmens über eine Geschäftsfortführungsrichtlinie? ***Anmerkung:*** *Art 11 Abs 1 DORA-VO fordert die Erstellung einer umfassenden IKT-Geschäftsfortführungsrichtlinie, die fester Bestandteil der allgemeinen Geschäftsfortführungsleitlinie ist, und die in Abs 2 lit a bis e enthaltenen Ziele, wie Sicherstellung der kritischen oder wichtigen Funktionen, rasche Reaktion auf alle IKT-bezogenen Vorfälle, unverzügliche Aktivierung der notwendigen Pläne zur Eindämmung der Vorfälle sowie der Wiederherstellung, Einschätzung der Auswirkungen von Schaden und Verlust sowie Festlegung von Kommunikations- und Krisenmanagementmaßnahmen einschließlich der Sicherstellung der Meldung an die zuständigen Behörden gem Art 19 DORA-VO enthält.*		
Frage 24: Wurden vom Finanzunternehmen IKT-Reaktions- und -Wiederherstellungspläne implementiert? ***Anmerkung:*** *Art 11 Abs 3 DORA-VO fordert als Teil des in Art 6 Abs 1 genannten IKT-Risikomanagementrahmens die Implementierung von IKT-Reaktions- und -Wiederherstellungsplänen und deren Prüfung durch eine unabhängige interne Revision.*		
Frage 25: Werden vom Finanzunternehmen angemessene IKT-Geschäftsfortführungspläne mit Fokus auf ausgelagerte oder vertragliche Vereinbarungen mit IKT-Dienstleistern erstellt, gepflegt und getestet? ***Anmerkung****: Art 11 Abs 4 DORA-VO fordert die Erstellung, Pflege und den Test dieser Pläne insb auf kritische oder wichtige Funktionen, die von IKT-Drittanbietern durchgeführt werden.*		

Dako 2024/52

Zum Thema

Über den Autor

Prof. KommR Hans-Jürgen Pollirer ist Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH und fachkundiger Laienrichter für Datenschutz am BVwG. E-Mail: hj.pollirer@secur-data.at

Hinweis

Teil 2 dieses Beitrags erscheint in Dako Heft 1/2025.