1/2025
1 – 24

10 Jahre Dako!

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Überwachung und Datenschutz

Bei der Überwachung von Messengern sind wir vom Ausland abhängig

Interview mit Hagen Nordmeyer, OGH

Überlegungen zum Verbot automatisierter Entscheidungen

Wolfgang Goricnik

Hohe Hürden für berechtigte Interessen

Martin Bauman und Felix Mikolasch

Checkliste Datenportabilität – Data Act vs DSGVO

Rainer Knyrim und Stephanie Briegl

Folgen der Datenschutzverletzung einer Gemeinde

Daniel Lehner

Checkliste DORA (Teil 2)

Hans-Jürgen Pollirer

ISSN 2313-5409

dako.manz.at

MANZ

Recht auf Datenportabilität gem Data Act	Recht auf Datenportabilität gem DSGVO
– Bestimmtheit des Inhalts eines Datensatzes, Nutzungsbeschränkungen, Lizenzen, Methodik der Datenerhebung und Datenqualität, damit der Datenempfänger die Daten unkompliziert finden, darauf zugreifen und nutzen kann. – Beschreibung von Datenstrukturen, Datenformaten, Vokabular, Klassifikationsschemata, Taxonomien und Codelisten in einer öffentlich zugänglichen und konsistenten Weise. – Beschreibung der technischen Mittel für den Datenzugriff (zB Programmierschnittstellen und deren Nutzungsbedingungen), um den automatischen Zugang und die automatische Übermittlung von Daten zu ermöglichen. – Bereitstellung der Mittel, um Interoperabilität von „smart contracts" innerhalb ihrer Dienste und Tätigkeiten zu ermöglichen. ■ Erfüllung der Anforderungen für Datenverarbeitungsdienste (Art 35 Data Act); Interoperabilitätsspezifikationen und Normen müssen: – Leistungsorientiert sein, um Interoperabilität zwischen Datenverarbeitungsdiensten desselben Typs zu erreichen; – die Übertragbarkeit digitaler Vermögenswerte zwischen verschiedenen Datenverarbeitungsdiensten desselben Typs verbessern und – die Funktionsäquivalenz zwischen verschiedenen Datenverarbeitungsdiensten desselben Typs sicherstellen, soweit dies technisch machbar ist. ■ Darüber hinaus technische Anforderungen an Smart Contracts (Art 36 Data Act) diverse Anforderungen wie Manipulationssicherheit, Nachvollziehbarkeit, Zugangskontrolle.	
Frage 13: Ist für die Bereitstellung ein Entgelt zu leisten?	
■ Im B2C-Bereich unentgeltlich; ■ im B2B-Bereich kann ein Entgelt verlangt werden (Art 9 Data Act).	Der Datenzugang hat unentgeltlich zu erfolgen (Art 12 Abs 5 DSGVO).
Frage 14: Besteht eine Beschwerdemöglichkeit bei Verletzung?	
Beschwerdemöglichkeit bei zuständiger Behörde gem Art 38 Data Act.	Beschwerdemöglichkeit binnen eines Jahrs ab Kenntnis des Ereignisses gem Art 77 DSGVO iVm § 24 Abs 1 iVm Abs 4 DSG.

Zum Thema

Über den Autor und die Autorin

RA Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte OG: E-Mail: kt@kt.at

Mag.ª Stephanie Briegl, BA, ist Juristin.

Hans-Jürgen Pollirer

Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste DORA (Teil 2)

Anwendungsbereich; risikobasierter Ansatz; Dokumentation; Qualitätsmanagementsystem; Transparenzpflichten. Mit der Checkliste werden die wichtigsten Maßnahmen bei der Umsetzung der DORA-VO für Finanzunternehmen aufgezeigt. Teil 1 dieser Checkliste ist in Dako 5/2024 erschienen (Dako 2024/52).

Prüffragen	ja	nein
IKT-Risikomanagement		
Frage 26: Führt das Finanzunternehmen eine Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen durch? ***Anmerkung:*** *Art 11 Abs 5 DORA-VO fordert die Durchführung einer BIA für schwerwiegende Betriebsstörungen, im Rahmen derer die Auswirkungen anhand quantitativer und qualitativer Kriterien bewertet werden.*		
Frage 27: Werden vom Finanzunternehmen entsprechende Tests durchgeführt? ***Anmerkung:*** *Art 11 Abs 6 lit a und b DORA-VO fordern die Durchführung von Tests von IKT-Systemen, IKT-Geschäftsfortführungsplänen, IKT-Reaktions- und Wiederherstellungsplänen, Krisenkommunikationsplänen sowie der IKT-Geschäftsfortführungsleitlinie.*		

Frage 28: Können die Aufzeichnungen über die Tätigkeiten vor und während der Störungen jederzeit eingesehen werden? ***Anmerkung:*** *Gem Art 11 Abs 8 DORA-VO hat das Finanzunternehmen dafür Sorge zu tragen, dass bei Aktivierung seiner IKT- und Geschäftsfortführungspläne oder seiner IKT-Reaktions- und -Wiederherstellungspläne die Aufzeichnungen über die Tätigkeiten vor und während der Störung jederzeit eingesehen werden können.*		
Frage 29: Ist das Finanzunternehmen in der Lage, den zuständigen Behörden auf Anfrage die geschätzten aggregierten Kosten und Verluste, die durch schwerwiegende IKT-Vorfälle verursacht wurden, zu melden? ***Anmerkung:*** *Diese Forderung ergibt sich aus den Bestimmungen des Art 11 Abs 10 DORA-VO, wobei gem Abs 11 die am 17. 7. 2024 vorgelegten* ***„Guidelines on Costs and Losses“***[1] *zu beachten sind.*		
Frage 30: Verfügt das Finanzunternehmen über Richtlinien und Verfahren zur Datensicherung? ***Anmerkung:*** *Art 12 Abs 1 lit a und b DORA-VO fordert die Erstellung von Richtlinien und Verfahren für die Datensicherung mit Angabe des Umfangs der Daten, die der Sicherung unterliegen, des Sicherungszyklus sowie der Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden.*		
Frage 31: Verfügt das Finanzunternehmen über Datensicherungssysteme, die in Übereinstimmung mit den Richtlinien und Verfahren zur Datensicherung sowie den Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung aktiviert werden können? ***Anmerkung:*** *Art 12 Abs 2 DORA-VO fordert darüber hinaus, dass die Aktivierung der Datensicherungssysteme, die Sicherung der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten nicht gefährden darf, sowie den regelmäßigen Test dieser Systeme.*		
Frage 32: Werden für die Wiedergewinnung gesicherter Daten IKT-Systeme verwendet, die von ihrem Quellsystem physisch und logisch getrennt sind? ***Anmerkung:*** *Darüber hinaus fordert Art 12 Abs 3 DORA-VO, dass die IKT-Systeme vor unbefugtem Zugriff oder IKT-Manipulationen geschützt sind, und die rechtzeitige Wiederherstellung von Diensten ermöglichen.*		
Frage 33: Verfügt das Finanzunternehmen über redundante IKT-Kapazitäten, Fähigkeiten und Funktionen? ***Anmerkung:*** *Art 12 Abs 4 DORA-VO fordert, dass diese redundanten IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen ausgestattet sind, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind.*		
Frage 34: Wird bei der Festlegung der Wiederherstellungszeit berücksichtigt, ob es sich um eine kritische oder wichtige Funktion handelt? ***Anmerkung:*** *Art 12 Abs 6 DORA-VO fordert die Berücksichtigung der Relevanz der einzelnen Funktionen sowie der potenziellen Gesamtauswirkungen auf die Markteffizienz.*		
Frage 35: Wird bei der Wiederherstellung nach IKT-bezogenen Vorfällen die Datenintegrität geprüft? ***Anmerkung:*** *Gem Art 12 Abs 7 DORA-VO sind Mehrfachprüfungen und Abgleiche durchzuführen, dies auch bei der Rekonstruktion von Daten externer Interessenträger.*		
Frage 36: Verfügt das Finanzunternehmen über ausreichende Kapazitäten und Personal, um IKT-bezogene Vorfälle, insb Cyberangriffe, zu analysieren? ***Anmerkung:*** *Art 13 Abs 1 DORA-VO fordert, dass diese Vorfälle auf ihre digitale Resilienz untersucht werden.*		
Frage 37: Erfolgt nach Störungen der Haupttätigkeit des Finanzunternehmens eine Analyse über die erforderlichen Verbesserungen von IKT-Vorgängen? ***Anmerkung:*** *Art 13 Abs 2 DORA-VO fordert in diesem Fall eine nachträgliche Prüfung über die Ursachen der Störungen und die erforderlichen Verbesserungen an IKT-Vorgängen oder der in Art 11 DORA-VO genannten IKT-Geschäftsfortführungsleitlinie. Diese nachträgliche Prüfung in Bezug auf die Wirksamkeit der ergriffenen Maßnahmen umfasst die Schnelligkeit bei der Reaktion auf Sicherheitswarnungen, die Qualität und Schnelligkeit bei der Durchführung forensischer Analysen, die Wirksamkeit der Eskalation von Vorfällen sowie der Wirksamkeit interner und externer Kommunikation.*		
Frage 38: Werden Erkenntnisse aus TLPT (s Art 26 und 27 DORA-VO) in den Risikobewertungsprozess einbezogen? ***Anmerkung:*** *Art 13 Abs 3 DORA-VO fordert die Einbeziehung der gem den Art 26 und 27 DORA-VO definierten „bedrohungsorientierten Penetrationstests“ (TLPT – Thread-Led Penetration Testing) der digitalen Resilienz und der aus realen IKT-bezogenen Vorfällen in den IKT-Risikobewertungsprozess. Die leitenden Mitarbeiter haben gem Abs 5 dem Leitungsorgan einmal jährlich über die in Art 13 Abs 3 genannten Feststellungen zu berichten und Empfehlungen abzugeben.*		
Frage 39: Überwacht das Finanzunternehmen die Wirksamkeit der Umsetzung seiner Strategie für die digitale operationale Resilienz? ***Anmerkung:*** *Zielsetzung dieser Überwachung ist gem Art 13 Abs 4 DORA-VO die Cyberreife und die Abwehrbereitschaft des Finanzunternehmens zu verbessern.*		
Frage 40: Führt das Finanzunternehmen Schulungen zur digitalen operationalen Resilienz für die Mitarbeiter durch? ***Anmerkung:*** *Art 13 Abs 6 DORA-VO fordert die Entwicklung von Schulungsprogrammen zur Sensibilisierung für die IKT-Sicherheit und zur digitalen Resilienz, deren Besuch für alle Mitarbeiter – einschließlich der Geschäftsleitung – obligatorisch ist.*		
Frage 41: Überwacht das Finanzunternehmen fortlaufend die einschlägigen technologischen Entwicklungen? ***Anmerkung:*** *Gem Art 13 Abs 7 DORA-VO muss sich das Finanzunternehmen fortlaufend über die einschlägige technologische Entwicklung informieren, um die möglichen Auswirkungen dieser auf die Anforderungen an die IKT-Sicherheit und digitale operationale Resilienz zu verstehen.*		
Frage 42: Verfügt das Finanzunternehmen über Kommunikationspläne, die eine verantwortungsbewusste Offenlegung von schwerwiegenden IKT-bezogenen Vorfällen oder Schwachstellen ermöglichen? ***Anmerkung:*** *Gem Art 14 Abs 1 DORA-VO müssen diese Kommunikationspläne – je nach Sachlage – die Offenlegung von Vorfällen oder Schwachstellen gegenüber Kunden und anderen Finanzunternehmen sowie der Öffentlichkeit ermöglichen. Gem Abs 2 ist bei den Kommunikationsplänen zwischen dem Personal, das am IKT-Management beteiligt ist und dem zu informierenden Personal zu differenzieren. Abs 3 fordert, dass mindestens eine Person im Finanzunternehmen mit der Umsetzung der Kommunikationsstrategie beauftragt ist und diese Aufgabe auch gegenüber der Öffentlichkeit und den Medien wahrnimmt.* *Genauere Spezifikationen enthält der* ***„Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework“.***[2]		
Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle		
Frage 43: Existiert im Finanzunternehmen ein Prozess für die Behandlung IKT-bezogener Vorfälle? ***Anmerkung:*** *Gem Art 17 Abs 1 DORA-VO ist dieser Prozess anzuwenden, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden. Dieser Prozess hat die in Abs 3 lit a bis h angeführten Merkmale zu gewährleisten, wie Einsatz von Frühwarnindikatoren, Verfahren zur Ermittlung, Nachverfolgung, Protokollierung, Kategorisierung und Klassifizierung IKT-bezogener Vorfälle entsprechend ihrer Priorität und Schwere und entsprechend der Kritikalität der betroffenen Dienste. Weiters ist die Benachrichtigung der Führungsebene sicherzustellen, um Verfahren für Reaktionsmaßnahmen einzurichten, um die zeitnahe Verfügbarkeit der Dienste sicherzustellen.*		
Frage 44: Erfolgt durch das Finanzunternehmen eine Klassifizierung IKT-bezogener Vorfälle und Cyberbedrohungen? ***Anmerkung:*** *Art 18 Abs 1 lit a bis f DORA-VO fordert eine Klassifizierung IKT-bezogener Vorfälle und Cyberbedrohungen nach Anzahl und/oder Relevanz der Kunden, Dauer des IKT-bezogenen Vorfalls einschließlich der Ausfallzeiten, geografische Ausbreitung des Vorfalls, die mit dem Vorfall verbundenen Verfügbarkeits-, Authentizitäts-, Integritäts- oder Vertraulichkeitsverluste von Daten, die Kritikalität der betroffenen Dienste und die wirtschaftlichen Auswirkungen.* *Eine genaue Spezifikation der Klassifizierung enthält der* ***„Final report on draft RTS on classification of major incidents and significant cyber threats“.***		

[1] https://kurzelinks.de/f01z [2] https://kurzelinks.de/e3tk

Frage 45: Werden durch das Finanzunternehmen schwerwiegende IKT-bezogene Vorfälle an die zuständige Behörde gemeldet? ***Anmerkung:*** *Für die in Österreich tätigen Finanzunternehmen ist die FMA die zuständige Behörde. Diese leitet gem Art 19 Abs 1 DORA-VO die von den Finanzunternehmen erhaltenen Meldungen an die jeweilige Europäische Aufsichtsbehörde und gegebenenfalls an die EZB weiter. Das Meldewesen umfasst nach den Bestimmungen des Art 19 Abs 4 lit a bis c DORA-VO eine Erstmeldung, bei Änderung des Vorfalls eine Zwischenmeldung sowie eine Abschlussmeldung, wenn die Ursachenanalyse abgeschlossen ist.*		
Frage 46: Informiert das Finanzunternehmen seine Kunden bei einem schwerwiegenden IKT-bezogenen Vorfall unverzüglich? ***Anmerkung:*** *Art 19 Abs 3 DORA-VO fordert eine unverzügliche Information der Kunden des Finanzunternehmens, um die nachfolgenden Folgen zu mildern.*		
Frage 47: Lagert das Finanzunternehmen seine Meldepflichten an einen Dienstleister aus? ***Anmerkung:*** *Auch bei einer Auslagerung des Meldewesens trägt das Finanzunternehmen gem Art 19 Abs 5 DORA-VO die volle Verantwortung.*		
Testen der digitalen operationalen Resilienz		
Frage 48: Verfügt das Finanzunternehmen über ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz? ***Anmerkung:*** *Gem Art 24 Abs 1 DORA-VO ist dieses Programm integraler Bestandteil des Risikomanagementrahmens. Gem Abs 2 hat dieses Programm eine Reihe von Bewertungen, Tests, Methoden, Verfahren und Tools zu umfassen. Abs 3 fordert einen risikobasierten Ansatz des Programms und Abs 4 die Durchführung der Tests durch eine unabhängige Stelle. Weiters sind gem Abs 5 Verfahren und Leitlinien festzulegen, um die Feststellungen zu priorisieren, damit sichergestellt ist, dass alle ermittelten Schwächen, Mängel oder Lücken vollständig beseitigt werden. Bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, sind mindestes einmal jährlich angemessene Tests durchzuführen.*		
Frage 49: Werden vom Finanzunternehmen angemessene Tests durchgeführt? ***Anmerkung:*** *Art 25 Abs 1 DORA-VO fordert die Durchführung von angemessenen Tests der digitalen operationalen Resilienz und zählt verschiedene Testarten auf, wie etwa die Schwachstellenbewertung und -scans, Open Source Analysen, Netzwerksicherheitsbewertungen, Penetrationstests usw.*		
Frage 50: Werden auf Aufforderung der FMA mindestens alle drei Jahre erweiterte Tests (TLPT) durchgeführt? ***Anmerkung:*** *Diese Bestimmung des Art 26 Abs 1 DORA-VO gilt für die von der FMA ermittelten Finanzunternehmen, die sich dabei auf die in Abs 8 lit a bis c angeführten Kriterien stützt.*		
Frage 51: Werden vom Finanzunternehmen gem Art 8 Abs 2 die bedrohungsorientierten Penetrationstests an mehreren kritischen oder wichtigen Funktionen am Live-Produktionssystem durchgeführt? ***Anmerkung:*** *Um diese Forderung des Art 26 Abs 2 DORA-VO erfüllen zu können, muss das Finanzunternehmen die zu testenden kritischen und wichtigen Funktionen und IKT-Dienstleistungen nachvollziehbar ermitteln.*		
Frage 52: Werden vom Finanzunternehmen die IKT-Dienstleister in das Spektrum der TLPT einbezogen? ***Anmerkung:*** *Gem Art 26 Abs 3 DORA-VO muss das Finanzunternehmen diese Maßnahme sicherstellen, wobei Abs 4 die Möglichkeit vorsieht, einen gebündelten Test der Systeme der IKT-Dienstleister durch einen externen Tester zu vereinbaren und durchzuführen.*		
Frage 53 Werden bei den Tests wirksame Risikomanagementkontrollen angewendet? ***Anmerkung:*** *Art 26 Abs 5 DORA-VO fordert diese Maßnahme, um die Gefahr von negativen Auswirkungen auf Daten, Vermögensschäden und Unterbrechung kritischer oder wichtiger Funktionen zu vermeiden.*		
Frage 54: Werden vom Finanzunternehmen nach Abschluss der Tests die Berichte und Pläne mit Abhilfemaßnahmen der FMA vorgelegt? ***Anmerkung:*** *Diese Forderung ergibt sich aus den Bestimmungen des Art 26 Abs 6 DORA-VO und soll belegen, dass der TLPT ordnungsgemäß durchgeführt wurde.*		
Frage 55: Wurden vom Finanzunternehmen interne Tester eingesetzt? ***Anmerkung:*** *In diesem Fall fordert Art 26 Abs 8 DORA-VO, dass das Finanzunternehmen für jeden dritten Test einen externen Tester beauftragen muss. Kreditinstitute, die als bedeutend eingestuft wurden, dürfen allerdings nur externe Tester heranziehen.*		
Frage 56: Verfügt das Finanzunternehmen über besonders qualifizierte Tester? ***Anmerkung:*** *Gem Art 27 Abs 1 dürfen Finanzunternehmen nur Tester für die Durchführung von TLPT heranziehen, die die Anforderungen von lit a bis e erfüllen. Zu diesen Kriterien zählen höchste Eignung und Ansehen, technische und organisatorische Fähigkeiten, Zertifikate einer Akkreditierungsstelle, Unabhängigkeit und Vorliegen einer einschlägigen Berufshaftpflichtversicherung.* *Der „**Final report_DORA RTS on TLPT**“ enthält umfangreiche Informationen zu TLPT.*		
Management des IKT-Drittparteienrisikos		
Frage 57: Ist sich das Finanzunternehmen bewusst, dass es auch für die Nutzung von IKT-Dienstleistungen verantwortlich ist? ***Anmerkung:*** *Diese in Art 28 Abs 1 lit a DORA-VO normierte Forderung bedingt gem lit b, dass das Finanzunternehmen dem Grundsatz der Verhältnismäßigkeit Rechnung trägt, indem es die Art des Ausmaßes sowie die Kritikalität oder Relevanz der jeweiligen Dienstleistung berücksichtigt.*		
Frage 58: Existiert im Rahmen des IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko? ***Anmerkung:*** *Diese Strategie fordert gem Art 28 Abs 2 DORA-VO die Erstellung von Leitlinien zur Nutzung von IKT-Drittdienstleistungen für kritische oder wichtige Funktionen.*		
Frage 59: Führt das Finanzunternehmen ein zentrales Informationsregister über die vertraglichen Vereinbarungen mit den IKT-Dienstleistern? ***Anmerkung:*** *Diese Forderung erhebt Art 28 Abs 3 DORA-VO, der darüber hinaus die Vorlage eines jährlichen Berichts über die Nutzung von IKT-Dienstleistern an die zuständige Behörde (FMA) fordert. Des Weiteren ist die Behörde zeitnah über jede neue IKT-Dienstleistung zu informieren.* *Der **„Final report on draft ITS on Register of Information“** sowie das **„Register of Information Templates in Excel format for illustration purposes“** enthalten umfangreiche Informationen.*		
Frage 60: Werden vom Finanzunternehmen vor Abschluss einer Dienstleister-Vereinbarung die in Art 28 Abs 4 DORA-VO festgelegten Maßnahmen eingehalten? ***Anmerkung:*** *Art 28 Abs 4 lit a bis d DORA-VO fordert, dass das Finanzunternehmen beurteilt, ob sich die Dienstleister-Vereinbarung auf kritische oder wichtige Funktionen bezieht, ob die aufsichtsrechtlichen Bedingungen erfüllt sind, alle relevanten Risiken, die mit dem Vertragsabschluss verbunden sein könnten, ermittelt und bewertet werden, sowie, ob die potenziellen IKT-Dienstleister der gebotenen Sorgfaltspflicht nachkommen und geeignet sind. Weiters sind mögliche Interessenkonflikte zu ermitteln und zu bewerten.*		
Frage 61: Halten für die Erbringung der IKT-Dienstleistung die ausgewählten IKT-Dienstleister angemessene Standards für die Informationssicherheit ein? ***Anmerkung:*** *Falls diese vertraglichen Vereinbarungen kritische oder wichtige Funktionen betreffen, muss das Finanzunternehmen gem Art 28 Abs 5 DORA-VO prüfen, ob die IKT-Dienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit einhalten.*		
Frage 62: Erstellt das Finanzunternehmen einen angemessenen Audit-Plan in Bezug auf die IKT-Dienstleister? ***Anmerkung:*** *Art 28 Abs 6 DORA-VO fordert die Erstellung eines Audit-Plans auf der Grundlage eines risikobasierten Ansatzes in Bezug auf die Häufigkeit von Audits sowie die Einhaltung allgemein anerkannter Audit-Standards.*		

Frage 63 Hat das Finanzunternehmen sichergestellt, dass Vereinbarungen mit IKT-Dienstleistern unter bestimmten Umständen auch gekündigt werden können? ***Anmerkung:*** *Art 28 Abs 7 DORA-VO fordert die Sicherstellung einer Kündigungsmöglichkeit von IKT-Dienstleistern, zB bei einem Verstoß des IKT-Dienstleisters gegen Gesetze, Vorschriften oder Vertragsbedingungen, bei Beeinträchtigung der Wahrnehmung der vereinbarten Dienstleistung, bei festgestellten Schwächen im Risikomanagement oder wenn die Behörde in Folge der vertraglichen Vereinbarung das Finanzunternehmen nicht mehr wirksam beaufsichtigen kann.*		
Frage 64: Hat das Finanzunternehmen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, entsprechende Ausstiegsszenarien eingerichtet? ***Anmerkung:*** *Art 28 Abs 8 DORA-VO fordert die Festlegung von Ausstiegsszenarien, ohne dass die Geschäftstätigkeit unterbrochen wird, die Einhaltung regulatorischer Bestimmungen eingeschränkt und die Kontinuität und Qualität der Dienstleistung beeinträchtigt wird. Diese Ausstiegsstrategien sind zu dokumentieren und zu testen und enthalten auch Übergangspläne, die eine Rückführung der relevanten Daten ermöglichen.*		
Frage 65: Erfolgt durch das Finanzunternehmen eine vorläufige Bearbeitung des IKT-Konzentrationsrisikos? ***Anmerkung:*** *Art 29 Abs 1 DORA-VO fordert, dass bei der Ermittlung der Risiken überprüft wird, ob der IKT-Dienstleister nicht ohne weiteres ersetzbar ist und ob nicht insgesamt diese kritischen Funktionen mit demselben IKT-Dienstleister oder mit den verbundenen IKT-Dienstleistern vergeben werden.*		
Frage 66: Wird vom Finanzunternehmen geprüft, ob nicht eine mögliche Weitergabe einer kritischen oder wichtigen Funktion vom IKT-Dienstleister per Subauftrag an andere IKT-Dienstleister vergeben werden kann, die uU in einem Drittland niedergelassen sind? ***Anmerkung:*** *IdZ fordert Art 29 Abs 2 DORA-VO, dass das Finanzunternehmen die Vorteile und Risiken beurteilt. Weiters sind die Auswirkungen einer Insolvenz des IKT-Dienstleisters insb in Bezug auf eine schnelle Wiederherstellung der Daten zu prüfen sowie, ob die Durchsetzbarkeit der Rechts- und Datenschutzvorschriften gewährleistet ist.*		
Frage 67: Enthält der mit dem IKT-Dienstleister abgeschlossene Vertrag eine eindeutige Zuweisung der Rechte und Pflichten zwischen den Parteien? ***Anmerkung:*** *Art 30 Abs 1 DORA-VO fordert, dass der zwischen dem Finanzunternehmen und dem IKT-Dienstleister abzuschließende Vertrag die Rechte und Pflichten eindeutig zuweist und schriftlich darlegt. Dieser Vertrag kann in Papierform zur Verfügung gestellt werden oder in einem anderen herunterladbaren dauerhaften und zugänglichen Format.*		
Frage 68: Umfasst der mit dem IKT-Dienstleister abgeschlossene Vertrag mindestens die in Art 30 Abs 2 lit a bis i bzw die in Art 30 Abs 3 lit a bis f DORA-VO festgelegten Inhalte? ***Anmerkung:*** *Die in Art 30 Abs 2 DORA-VO angeführten Inhalte des IKT-Dienstleistungsvertrages sind bei Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen um die in Abs 3 angeführten Inhalte zu ergänzen.* *Der* ***„Final report DORA RTS on subcontracting“***[3] *enthält nähere Spezifikationen zu diesem Thema.* ***Die BaFin hat mit 4. 9. 2024 eine detaillierte Übersicht über die Mindestvertragsinhalte veröffentlicht.***[4]		

[3] https://kurzelinks.de/dxlh [4] https://kurzlinks.de/at0e

Dako 2025/7

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

Literatur und Links

- BaFin, Mindestvertragsinhalte DORA: https://kurzlinks.de/at0e;
- FMA, DORA – Digitale operationale Resilienz im Finanzsektor: www.fma.gv.at/querschnittsthemen/dora/;
- Cyber Trust Austria, Alles über NIS 2 & DORA, www.cyber-trust.at/nis/.

Raphael Toman/Fabian Schinerl[1]
BRANDL TALOS Rechtsanwält:innen GmbH/Universität Wien

Rechtsprechung

Pre-Trial Discovery auf Grundlage der DSGVO? Die Reichweite des Art 15 DSGVO steht erneut auf dem Prüfstand. Auskunftsrecht ohne Zweckbindung? Die Grenze ist und bleibt der Rechtsmissbrauch.

Entscheidung

Das datenschutzrechtliche Auskunftsrecht (Art 15 DSGVO) wird in der Praxis immer häufiger als **strategisches Instrument zur Beweissicherung** im Vorfeld rechtlicher Auseinandersetzungen genutzt. Unlängst hat sich auch das OLG Wien zu dieser Frage geäußert.[2] Mit Verweis auf die Rs C-307/22[3] scheint eine Judikaturwende eingeleitet.[4]

[1] Ra Dr. Raphael Toman, LL.M., ist Partner bei BRANDL TALOS Rechtsanwält:innen GmbH, Mag. Fabian Schinerl ist wissenschaftlicher Mitarbeiter bei BRANDL TALOS Rechtsanwält:innen GmbH und Universitätsassistent am Institut für Europarecht, Internationales Recht und Rechtsvergleichung an der Universität Wien.

[2] OLG Wien 10. 6. 2024, 14 R 48/24t. [3] EuGH 26. 10. 2023, C-307/22, *Copies du dossier médical*, ECLI:EU:C:2023:811.
[4] Vgl *Ehmann* in *Ehmann/Selmayr*, DSGVO[3] Art 15 Rz 24: *„Auch ErwGr 63 S 1 bietet keinen Hebel, um ein Auskunftsverlangen als rechtsmissbräuchlich anzusehen, weil es ‚datenschutzfremden Zwecken‘ wie etwa der Vorbereitung einer zivilrechtlichen Rechtsverfolgung dienen soll“*; *Franck* in *Gola/Heckmann*, DS-GVO/BDSG[3] Art 15 DSGVO Rz 1: *„Auch reine Neugieranfragen sind zulässig“*; zur (vermeintlichen) Judikaturwende in Deutschland sa *Riemer*, Der Datenauskunftsanspruch gem Art. 15 DS-GVO als Tool zur Informationsgewinnung, DAR 2022, 127; *Leibold*, Übersicht über den Schadensersatzanspruch nach Art 82 DS-GVO – im Zeitraum 2018-2022, ZD-Aktuell 2023, 01191; *Lang*, Der Auskunftsanspruch nach § 15 Abs 1 und 3 DSGVO – Sind wir auf dem Weg zu einer „pre-trial discovery“? BKR 2024, 421; zur dt Rsp s BGH 29. 3. 2022, VI ZR 1352/20, Rn 16–19; BGH 29. 3. 2022, VI ZR 1352/20, Rn 20.