Dr. Tretzmüller LL.M IT-LAW
Interdimensionale
IT-Rechtskanzlei

Der Digital-Operational-Resilience-Act

Skriptum zum Kurs/Vortrag/Online-Kurs

Datum: 7.2.2025

ÜBERSICHT UND ZIELE DES DORA

1.1. Überblick:

Die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14.12.2022 über die digitale operationale Resilienz im Finanzsektor (in der Folge „**DORA**“) umfasst 64 Artikel und 106 Erwägungsgründe.

Es handelt sich um eine europäische **Verordnung**, weshalb diese unmittelbar in sämtlichen Mitgliedstaaten der Europäischen Union gilt.

Die Ziele des DORA sind ein hohes gemeinsames Niveau an digitaler operationaler Resilienz und einheitliche Anforderungen für die **Sicherheit von Netzwerk- und Informationssystemen**, die die Geschäftsprozesse von **Finanzunternehmen** unterstützen. Vor allem im Bankengeschäft ist die Entwicklung der Produkte mit der IKT eng verknüpft, da diese beinahe vollständig informationsbasiert sind, denn Dienstleistungen umfassen im Unterschied zum Kauf von Waren keine physischen Komponenten, weshalb Informationen die primären Produkte darstellen[1]. Mit der digitalen Revolution werden zusätzliche weitere Geschäftsprozesse entwickelt, realisiert und implementiert, wie etwa Big Data, Data-Analytics, Cloud-Computing, mobile Endgeräte oder künstliche Intelligenz[2].

Mit dem DORA – aber auch dem Cyber Resilience Act, der KI-VO, der NIS-2-Richtlinie oder dem Produkthaftungsrecht neu – wird der Aspekt der IT-Sicherheit zu einem **MUSS-Kriterium**, das nicht mehr optional ist bzw von vorhandenen Ressourcen, Strategien oder der Risikoneigung der Geschäftsführung abhängig sein darf. In diesem Sinne erfährt die

[1] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 3.
[2] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 5.

Digitalisierung eine zwangsweise Reifegraderhöhung, die aber notwendig ist, damit sie weiterhin Bestand hat[3].

Im **Überblick** regelt der DORA:

- Das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie
- Die Meldung schwerwiegender IKT-bezogener Vorfälle
- Die Meldung schwerwiegender zahlungsbezogener Betriebs- und Sicherheitsvorfälle
- Tests der digitalen operationalen Resilienz
- Austausch von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen
- Maßnahmen für das solide Management des IKT-Drittparteienrisikos
- Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IKT-Drittdienstleistern und Finanzunternehmen
- Vorschriften über die Einrichtung und Ausführung des Überwachungsrahmens für kritische IKT-Drittdienstleister

Art 1 Abs 2 bzw ErwGr 16 stellt klar, dass der DORA gegenüber der NIS-2-Richtlinie die **speziellere Norm für Finanzunternehmen** ist und somit diese verdrängt.

Der Anwendungsbereich der „**Finanzunternehmen**" ist in Art 2 DORA weit gefasst und erfasst Kreditinstitute, Zahlungsinstitute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen, Versicherungs- und Rückversicherungsunternehmen, Einrichtungen der betrieblichen Altersversorgung ebenso wie beispielweise Versicherungsvermittler. Etwas verwirrend ist, dass Art 2 Abs 1 lit u „IKT-Drittdienstleister" als Normadressaten nennt. Dies muss wohl so verstanden werden, dass IKT-Drittdienstleister umfasst sind, sofern diese IKT-Dienstleistungen für Finanzunternehmen erbringen – und nicht, dass IKT-Dienstleister per se

[3] *Rosenkranz*/*Skopik* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 108.

von der DORA umfasst sind. Teilweise sind Ausnahmen zu beachten. So sind etwa Versicherungsvermittler, bei denen es sich um Kleinst- oder klein oder mittlere Unternehmen handelt, ausgeschlossen. Der DORA folgt damit einem sogenannten "*cross-sektoralen-Ansatz*", da dieser über die unterschiedlichen Zweige der Finanzindustrie hinweg einen harmonisierten Rechtsrahmen für die digitale operationale Resilienz begründet[4].

Wichtige **Legaldefinitionen** sind:

- „**digitale operationale Resilienz**" die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen. Das IKT-Risiko wird als Unterkategorie des operationellen Risikos eingestuft[5];
- „schwerwiegender IKT-bezogener Vorfall" meint einen IKT-Vorfall, der umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme hat, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen;
- „schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfall" einen zahlungsbezogenen Betriebs- oder Sicherheitsvorfall, der umfassende nachteilige Auswirkungen auf die bereitgestellten zahlungsbezogenen Dienste hat;
- „bedrohungsorientierte Penetrationstests (TLPT — Threat-Led Penetration Testing)" einen Rahmen, der Taktik, Techniken und Verfahren realer Angreifer, die als echte Cyberbedrohung empfunden werden, nachbildet und einen kontrollierten,

[4] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 23.

[5] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 5.

maßgeschneiderten, erkenntnisgestützten (Red-Team-) Test der kritischen Live-Produktionssysteme des Finanzunternehmens ermöglicht;

- IKT-Drittparteienrisiko“ ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Dienstleistungen entstehen kann, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern, einschließlich über Vereinbarungen zur Auslagerung, bereitgestellt werden;
- „IKT-Drittdienstleister“ ein Unternehmen, das IKT-Dienstleistungen bereitstellt;
- „kritische oder wichtige Funktion“ eine Funktion, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde;
- „kritischer IKT-Drittdienstleister“ einen IKT-Drittdienstleister, der gemäß Artikel 31 als kritisch eingestuft wurde;
- „Leitungsorgan“ ein Leitungsorgan im Sinne von Artikel 4 Absatz 1 Nummer 36 der Richtlinie 2014/65/EU, von Artikel 3 Absatz 1 Nummer 7 der Richtlinie 2013/36/EU, von Artikel 2 Absatz 1 Buchstabe s der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates (31), von Artikel 2 Absatz 1 Nummer 45 der Verordnung (EU) Nr. 909/2014, von Artikel 3 Absatz 1 Nummer 20 der Verordnung (EU) 2016/1011 sowie im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten oder die entsprechenden Personen, die das Unternehmen tatsächlich leiten oder im Einklang mit dem einschlägigen Unionsrecht oder nationalen Recht Schlüsselfunktionen wahrnehmen

1.2. Zeitlicher Anwendungsbereich und nationales Begleitgesetz:

Die Verordnung gilt gemäß Art 64 ab dem **17.1.2025**.

Nachdem der DORA punktuell einer Spezifizierung auf nationaler Ebene bedarf, wurde in Österreich das **DORA-Vollzugsgesetz** erlassen. In Österreich wurde mit dem Bundesgesetz über das Wirksamwerden der Verordnung EU (2022/2554) über die digitale operationale Resilienz im Finanzsektor (DORA-VG) ein nationaler Rahmen geschaffen, um die Vorgaben der EU umzusetzen. Das Vollzugsgesetz tritt - im Wesentlichen - zeitgleich mit der DORA-Verordnung am 17. Jänner in Kraft. Ein zentraler Bestandteil des Gesetzes sind die klar definierten und spürbaren Sanktionen, die sicherstellen sollen, dass Unternehmen ihre digitale Resilienz ernst nehmen.

Die Hauptinhalte des DORA-Vollzugsgesetztes sind:

1. Zuständigkeit der FMA: Die Finanzmarktaufsicht (FMA) wird als zuständige Behörde für die Überwachung der Einhaltung der DORA-Verordnung in Österreich festgelegt.
2. Aufsichts- und Sanktionsbefugnisse: Die FMA erhält erweiterte Befugnisse, um die Einhaltung der DORA-Vorgaben durchzusetzen, einschließlich der Möglichkeit, Sanktionen bei Verstößen zu verhängen.
3. Erweiterter Anwendungsbereich: Das Gesetz stellt klar, dass die DORA-Verordnung für eine breite Palette von Finanzunternehmen gilt, einschließlich nationaler Institute, um eine umfassende Abdeckung sicherzustellen.
4. Zusammenarbeit mit der OeNB: Es werden Regelungen zur Zusammenarbeit zwischen der FMA und der Oesterreichischen Nationalbank (OeNB) im Bereich der digitalen Resilienz festgelegt.
5. Anpassung bestehender Rechtsakte: Bestehende Gesetze im Finanzmarktbereich werden angepasst, um die Kohärenz mit den neuen DORA-Vorgaben sicherzustellen.

Ein herausragender Aspekt des DORA-Vollzugsgesetzes ist die Einführung eines klaren **Sanktionssystems**. Die FMA ist befugt, empfindliche Geldstrafen zu verhängen und weitere Anordnungen zu erteilen. Diese zielen darauf ab, Unternehmen und IKT-Drittanbieter zur Einhaltung der Vorgaben zu verpflichten. Folgende Sanktionsmöglichkeiten sind vorgesehen:
1. Sanktionen gegen juristische Personen:

Wenn eine Person in Führungsposition den Verstoß zu verantworten hat, kann eine Strafe von bis zu 500.000 € oder 1 % des weltweiten Jahresumsatzes des Unternehmens verhängt werden (§ 8 Abs. 3 DORA-VG).

2. Sanktionen gegen verantwortliche Personen:

Wer als Verantwortlicher eines der DORA-VO unterliegenden Rechtsträgers einen Verstoß gegen die Verordnung begeht, ist mit einer Geldstrafe von bis zu 150.000 € zu bestrafen (§ 7 DORA-VG).

3. Maßnahmen gegen den Rechtsträger:

Die FMA kann etwa die Einschränkung oder Aussetzung der Nutzung bestimmter IKT-Systeme oder Dienstleistungen oder die Umsetzung von Maßnahmenplänen, um identifizierte Schwachstellen zu beheben, anordnen (§ 4 Abs 2. DORA-VG).

4. Öffentliche Bekanntmachung:

Verstöße können öffentlich gemacht werden, um Unternehmen zur Einhaltung der Vorschriften zu motivieren und Verbraucher zu informieren (§ 4 Abs. 2 und § 11 DORA-VG).

Beispiele für Verstöße

§ 7 DORA-Vollzugsgesetz regelt, welche Verstöße gegen die DORA-VO als Verwaltungsübertretung zu bestrafen sind. Beispielhaft genannt seien:

- Unzureichendes IKT-Risikomanagement: Wenn ein Unternehmen keine angemessenen Verfahren zur Bewertung und Behandlung von IKT-Risiken und IKT-bezogenen Vorfällen etabliert.
- Fehlende Sicherheitsmaßnahmen: Vernachlässigung grundlegender Cybersicherheitsstandards.
- Nicht (ordnungsgemäße) Durchführung der Testung der digitalen Resilienz.
- Unzureichende Kontrolle über Drittanbieter: Fehlende Vereinbarungen oder Audits zur Sicherstellung der Resilienz von ausgelagerten IKT-Diensten.

1.3. Zuständigkeit und Sanktionen:

Die Regelung der **zuständigen Behörde** ist in Art 46 DORA – ungewöhnlich komplex – geregelt. Je nachdem ob es sich um ein Kreditinstitut, Zahlungsinstitut, eine Wertpapierfirma, einen Anbieter von Krypto-Dienstleistungen, einen Zentralverwahrer, eine zentrale Gegenpartei, einen Handelsplatz, ein Transaktionsregister, einen Verwalter alternativer Investmentfonds, eine Verwaltungsgesellschaft, ein Versicherungs- oder Rückversicherungsunternehmen, einen Versicherungsvermittler, Rückversicherungsvermittler, eine Einrichtung der betrieblichen Altersversorgung, eine Ratingagentur, einen Administrator kritischer Referenzwerte, einen Schwarmfinanzierungsdienstleister oder ein Verbriefungsregister handelt, variiert die zuständige Behörde.

In Österreich obliegt der **Finanzmarktaufsichtsbehörde** der Vollzug der Aufsichtsgesetze gemäß §§ 1 f Finanzmarktaufsichtsbehördengesetz. Somit obliegt der FMA etwa die Bankenaufsicht, Versicherungsaufsicht, Pensionskassenaufsicht sowie die Wertpapieraufsicht.

Die zuständigen Behörden verfügen über Aufsichts-, Untersuchungs- und Sanktionsbefugnisse. Dazu gehört etwa auch (Art 50 Abs 2 lit a DORA) die Durchführung von Vor-Ort-Inspektionen.

Interessant ist weiters, dass die **Höhe etwaiger verwaltungsrechtlicher Sanktionen** an die Mitgliedstaaten delegiert wird. Art 50 Abs 3 zweiter Absatz normiert „lediglich“, dass die Sanktionen und Maßnahmen „wirksam, verhältnismäßig und abschreckend sein“ müssen. Konkreter sind hingegen die Vorgaben hinsichtlich der Höhe des Zwangsgelds, wenn kritische IKT-Drittdienstleister nicht angemessene mit der Überwachungsbehörde kooperieren. In diesem Fall kann ein Zwangsgeld von 1% des durchschnittlichen weltweiten Tagesumsatzes des IKT-Drittdienstleisters verhängt werden (Art 35 Abs 8 DORA).

Zu beachten ist, dass die DORA freilich nicht isoliert, betrachtet werden darf. Neben der DSGVO und der NIS-2-Richtlinie (bzw dessen nationalen Umsetzungsgesetzes) gilt es

zahlreiche weitere **nationale gesetzliche Bestimmungen** zu beachten. So bildet die wesentliche Rechtsgrundlage für die generelle gesellschaftsrechtliche Verantwortlichkeits- und Haftungsnormen und die daraus abzuleitenden Organisationspflichten die Bestimmungen nach § 84 öAktG und § 25 öGmbHG. Weiters ist speziell die Regelung des § 39 BWG hervorzuheben. Demnach sind die Geschäftsleiter dazu verpflichtet, ihre Geschäfte mit der "Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters" zu führen. Diese gesetzlichen Regeln geben jedoch in Bezug auf die gebotene IKT-Sicherheit freilich nur einen groben Rahmen[6].

1.4. IKT-Risikomanagement:

Art 5 normiert programmatisch, dass Finanzunternehmen über einen **internen Governance- und Kontrollrahmen** für ein wirksames und umsichtiges Management von IKT-Risiken gewährleisten müssen. Der IKT-Risikomanagementrahmen muss auch „gut dokumentiert" sein (Art 6 Abs 1). Er muss mindestens einmal jährlich dokumentiert und überprüft werden. Das Kapitel 2 des DORA behandelt das "IKT-Risikomanagement" .

Um die IKT-Risiken zu managen, müssen stets **auf dem neusten Stand** zu haltende IKT-Systeme, -Protokolle und -Tools eingesetzt werden (Art 7).

Art 5 Abs 2 normiert dezidiert, dass die Verantwortung für die Umsetzung der IKT-Risikomanagementmaßnahmen beim **Leitungsorgan** liegt. Konkret gilt Folgendes:

- Verantwortung des Leitungsorgans: Das Leitungsorgan trägt die letztendliche Verantwortung für das Management der IKT-Risiken des Finanzunternehmens.

[6] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 10.

- Leitlinien für Datenstandards: Es führt Leitlinien ein, um hohe Standards in Bezug auf Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuerhalten.

- Aufgaben und Verantwortlichkeiten: Das Leitungsorgan legt klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen fest und sorgt für angemessene Governance-Regelungen.

- Strategie für digitale Resilienz: Es trägt die Gesamtverantwortung für die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz.

- Überwachung und Überprüfung: Das Leitungsorgan genehmigt, überwacht und überprüft regelmäßig die Umsetzung der IKT-Geschäftsfortführungsleitlinie und der IKT-Reaktions- und Wiederherstellungspläne.

- IKT-Revisionspläne: Es genehmigt und überprüft regelmäßig die internen IKT-Revisionspläne des Finanzunternehmens.

- Budgetmittel: Das Leitungsorgan weist angemessene Budgetmittel zu und überprüft diese regelmäßig, um den Anforderungen an die digitale operationale Resilienz gerecht zu werden.

- Nutzung von IKT-Dienstleistungen: Es genehmigt und überprüft regelmäßig die Leitlinie des Finanzunternehmens in Bezug auf Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden.

- Meldekanäle: Das Leitungsorgan richtet Meldekanäle ein, um ordnungsgemäß über Vereinbarungen mit IKT-Drittdienstleistern und relevante geplante Änderungen informiert zu werden.

Art 8 bis Art 11 verdeutlichen, dass – wie bei einem Risikomanagementsystem üblich – IKT-Risiken (i) identifiziert, (ii) angemessen verhindert, (iii) erkannt und (iv) angemessen darauf reagiert werden muss (**Plan-Do-Check-Act**).

Viele Vorgaben an die IKT-Sicherheit sind bereits aus der **EBA ICT Guideline** (EBA GL/2019/04) bekannt und werden nun im Fokus der neuen Themen wie Management von Drittparteienrisiken (IKT-Dienstleister), Erweiterungen der Überwachung der operationalen Resilienz sowie der Fokussierung auf den Prozess der Erkennung, Behebung und Meldung von IKT bezogenen Vorfällen erweitert[7].

Gemäß Art 5 Abs 2 muss ein angemessenes Budget für die Sensibilisierung und **Schulung** von den Mitarbeitern in Bezug auf die digitale operationale Resilienz gewährleistet sein. Konkreter normiert Art 13 Abs 6, dass Finanzunternehmen Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz entwickeln müssen, die für die Mitarbeiter obligatorisch sind. Diese Programme müssen angemessen komplex sein und den konkreten, jeweiligen Aufgabenbereich umfassen. Gegebenenfalls sind auch die IKT-Drittdienstleister in die einschlägigen Schulungsprogramme aufzunehmen. Personeller Nachwuchs wird vor allem im Bereich der Compliance entstehen, bei Experten für Risikoanalysen und Personal für Penetration Test, die Handhabung von Vulnerabilitäten, die Härtung von Systemen und der Auditierung[8].

Da in der Praxis, insbesondere bei Ransomware-Attacken, besonders wichtig, ist in Art 12 das **Backup-Management** detailliert geregelt:

Finanzunternehmen entwickeln und dokumentieren Richtlinien und Verfahren zur Datensicherung, um die Wiederherstellung von IKT-Systemen und Daten mit minimaler Ausfallzeit sowie begrenzten Störungen und Verlusten sicherzustellen. Diese Richtlinien

[7] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 50.
[8] *Rosenkranz*/*Skopik* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 109.

legen den Umfang der zu sichernden Daten und die Mindesthäufigkeit der Sicherung fest, basierend auf der Kritikalität der Informationen oder dem Vertraulichkeitsgrad der Daten. Zusätzlich werden Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden entwickelt.

Die Unternehmen richten Datensicherungssysteme ein, die in Übereinstimmung mit den festgelegten Richtlinien und Verfahren aktiviert werden können, ohne die Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten zu gefährden. Diese Systeme und Verfahren werden regelmäßig getestet.

Bei der Wiedergewinnung gesicherter Daten verwenden die Unternehmen IKT-Systeme, die physisch und logisch vom Quellsystem getrennt sind, um unbefugten Zugriff oder Manipulationen zu verhindern und eine rechtzeitige Wiederherstellung der Dienste zu ermöglichen. Zentrale Gegenparteien und Datenbereitstellungsdienste unterhalten zusätzliche Ressourcen und Einrichtungen, um ihre Dienste jederzeit aufrechterhalten zu können.

Finanzunternehmen, die keine Kleinstunternehmen sind, unterhalten redundante IKT-Kapazitäten, die ausreichen, um den Geschäftsbedarf zu decken. Kleinstunternehmen bewerten, ob diese Kapazitäten notwendig sind. Zentralverwahrer unterhalten mindestens einen sekundären Verarbeitungsstandort, der geografisch vom primären Standort entfernt ist und die Kontinuität kritischer Funktionen gewährleisten kann.

Bei der Festlegung der Wiederherstellungszeit und -punkte berücksichtigen die Unternehmen die Kritikalität der Funktionen und die potenziellen Auswirkungen auf die Markteffizienz. Nach IKT-bezogenen Vorfällen führen sie Prüfungen durch, um die Datenintegrität sicherzustellen, auch bei der Rekonstruktion von Daten externer Interessenträger.

1.5. Meldepflichten:

Das Kapitel 3 des DORA betrifft die Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle. Ein weiterer wichtiger Aspekt des IKT-Risikomanagements, ist die Kommunikation von „schwerwiegenden IKT-bezogenen Vorfällen“ oder (!) Schwachstellen **gegenüber Kunden sowie der Öffentlichkeit**. Interessant ist dabei die Formulierung, „je nach Sachlage einer verantwortungsbewussten Offenlegung“ (Art 14 Abs 1), was einen gewissen Interpretationsspielraum ermöglicht. Bei der Bewertung IKT-bezogener Vorfälle und Cyberbedrohungen, sind folgende Kriterien zu beachten:

- Anzahl und/oder Relevanz der betroffenen Kunden oder Gegenparteien im Finanzbereich, einschließlich des Werts oder der Anzahl der betroffenen Transaktionen und eventueller Reputationsschäden.

- Dauer des IKT-bezogenen Vorfalls, einschließlich der Ausfallzeiten des Dienstes.

- Geografische Ausbreitung der betroffenen Gebiete, insbesondere wenn mehr als zwei Mitgliedstaaten betroffen sind.

- Verfügbarkeits-, Authentizitäts-, Integritäts- oder Vertraulichkeitsverluste von Daten, die mit dem IKT-bezogenen Vorfall verbunden sind.

- Kritikalität der betroffenen Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens.

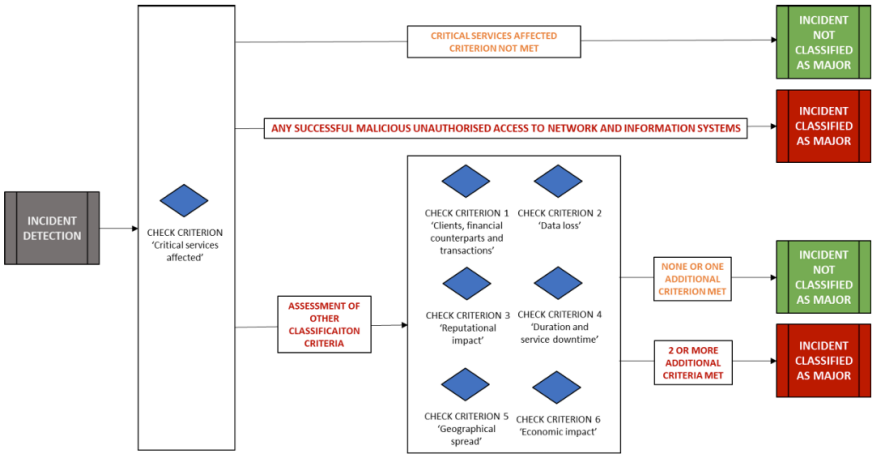
- Wirtschaftliche Auswirkungen des IKT-bezogenen Vorfalls, insbesondere direkte und indirekte Kosten und Verluste auf absoluter und relativer Basis.

Sämtliche Vorfälle müssen anhand definierter Kriterien klassifiziert werden (Art 18 DORA). Die Ausgestaltung dieser Kriterien erfolgt im “**Regulatory Technical Standard on**

classification of incidents" ("RTS"). Dieser Standard definiert auch die Wesentlichkeitsschwellen für schwerwiegende Vorfälle und erhebliche Cyberbedrohungen. Besonders relevant ist dabei die Identifikation von schwerwiegenden Vorfällen. Das Schema sowie die Erläuterungen aus dem RTS sind zwingend für die Klassifizierung von schwerwiegenden IKT-bezogenen bzw Sicherheits- oder betrieblichen Zahlungsvorfällen anzuwenden[9].

Die folgende Grafik bildet das **Prüfungsschema** zur Bewertung eines wesentlichen Vorfalles ab[10]:

Figure 1: Approach for classifying major incidents under DORA



Wesentlich ist dabei, dass jeder erfolgreiche böswillige unbefugte Zugriff auf Netzwerk- und Informationssysteme als schwerwiegender IKT-bezogener Vorfall zu klassifizieren ist. Hat hingegen (noch) kein erfolgreicher unbefugter Zugriff stattgefunden, müssen die insgesamt

[9] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 109.
[10] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 117.

sechs Entscheidungskriterien evaluiert werden. Treffen zwei oder mehr Kriterien zu, ist der Vorfall als schwerwiegend zu qualifizieren[11].

Hinsichtlich der Meldepflichten ist zu differenzieren zwischen den Meldepflichten gegenüber Kunden und Meldepflichten gegenüber der zuständigen Behörde. Gemäß Art 19 Abs 3 DORA: Wenn ein schwerwiegender IKT-bezogener Vorfall auftritt und die finanziellen Interessen **der Kunden** betroffen sind, informieren die Finanzunternehmen ihre Kunden **unverzüglich** über den Vorfall und die ergriffenen Maßnahmen zur Minderung der nachteiligen Auswirkungen.

Gegenüber der jeweils zuständigen Behörde hingegen ist folgendes Meldeprozedere zu beachten (Art 19 Abs 4):

- Zunächst muss eine Erstmeldung erfolgen
- Danach erfolgt eine Zwischenmeldung auf Basis der neuen, verfügbaren Informationen
- Und schließlich erfolgt eine Abschlussmeldung mitsamt einer Ursachenanalyse.

Bei der **Erstmeldung** sollen folgende Fragen beantwortet werden[12]:

- Was ist geschehen?
- Welche Dienste und Services sind betroffen?
- Welche Auswirkungen hat der Vorfall für Kunden 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?

[11] https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf
[12] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 121.

- Wie gravierend ist der Vorfall aus Sicht des Finanzinstituts zum Zeitpunkt der Meldungsabgabe?
- Wie schwer wird der Vorfall eingeschätzt: Sehr niedrig, niedrig, mittel, hoch, sehr hoch
- Sind nachteilige Auswirkungen auf das Finanzunternehmen, seine Kundschaft oder gar den Finanzmarkt zu erwarten?
- Ist es wahrscheinlich, dass auch andere Finanzunternehmen betroffen sind?

In der **Zwischenmeldung** müssen unter anderem folgende Fragen behandelt werden[13]:

- Dauert die Einschränkung durch den Vorfall noch an?
- Wurde der Geschäftsbetrieb wieder hergestellt?
- Hat sich der Vorfall verschärft?

In der **Abschlussmeldung** schließlich müssen folgende Aspekte behandelt werden[14]:

- Was war die Ursache des Vorfalls?
- Welche Maßnahmen wurden umgesetzt?
- Welche Kosten sind entstanden?
- Welche Schäden sind entstanden?

Bezüglich der zu berücksichtigenden Kosten gibt der RTS vor, dass folgende Kosten zu berücksichtigen sind:

- Haftungen für enteignete Gelder oder finanzielle Vermögenswerte
- Ersatz- und Umsatzkosten
- Personalkosten

[13] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 122.
[14] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 122.

- Gebühren für Vertragsverstöße
- Wiedergutmachungs- und Schadenersatzkosten
- Entgangene Einnahmen
- Kommunikationskosten
- Beratungskosten

Finanzunternehmen können die Meldungspflichten an externe Dienstleister auslagern, jedoch bleibt auch in diesem Falle das Finanzinstitut in vollem Umfang für die Erfüllung der Meldepflichten verantwortlich[15].

Die diesbezüglichen Fristen werden noch durch die ESA ausgearbeitet (Art 20 lit a Nummer ii). Laut RTS betragen die **Meldefristen**[16]:

- Erstmeldung:
  - 4 Stunden nach Klassifizierung des Vorfalls als schwerwiegend
  - Maximal 24 Stunden nach Erkennung eines schwerwiegenden Vorfalls
- Zwischenmeldung:
  - 72 h nach der Klassifizierung des Vorfalls als schwerwiegend oder nach Normalisierung des Geschäftsbetriebs
- Abschlussmeldung:
  - 1 Monat nach der Klassifizierung des Vorfalls als schwerwiegend oder, falls der Vorfall noch nicht behoben werden konnte, am Tag nach dessen dauerhafter Behebung

Bis zur Implementierung einer einheitliche EU-Meldeplattform müssen die Meldungen **auf elektronischem Wege** an die FMA erfolgen. Für diesen Zweck wird es seitens der FMA ein Web-Formular geben[17].

[15] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 120.
[16] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 122.
[17] *Hefler* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 123.

1.6. Das Testen der digitalen operationalen Resilienz:

Kapitel 4 des DORA behandelt das Testen der digitalen operationalen Resilienz. Ein wichtiger Aspekt zur Erreichung der digitalen operationalen Resilienz ist das Testen der IKT-Infrastruktur (Artikel 24). Diese Tests müssen durch unabhängige Personen erfolgen.

Die Tests umfassen etwa (Art 25):

- Schwachstellenbewertungen- und Scans
- **Open-Source-Analysen**
- Netzwerksicherheitsbewertungen
- Lückenanalysen
- Überprüfungen der physischen Sicherheit
- **Fragebogen und Scans von Softwarelösungen**
- Quellcodeprüfungen
- Szenariobasierte Tests
- Kompatibiltätstests
- Leistungstest
- End-to-End-Tests
- Penetrationtests

Eine besondere Rolle spielen dabei die **Tester bezüglich der Durchführung von TLPT** (threat-led Penetration testing). Diese Tester müssen von höchster Eignung und Ansehen sein; über technische und organisatorische Fähigkeiten verfügen und spezifisches Fachwissen in den Bereichen Bedrohungsanalyse, Penetrationstest und Red-Team-Test nachweisen; von einer Akkreditierungsstelle zertifiziert sein oder formale Verhaltenskodizes oder ethische Rahmenregelungen einhalten; über eine einschlägige Berufshaftpflichtversicherung verfügen und einen Auditbericht in Bezug auf das zuverlässige Management von Risiken vorlegen. Der Mechanismus des “Threat-Led Penetration Testing” soll bewirken, dass die

Tests in einem realen und spezifischen Bedrohungsumfeld abgehalten werden. Dabei wird zunächst eine "Generic Threat Landscape" erstellt, die einen Überblick über die Bedrohungslandschaft des gesamten Finanzsektors im jeweiligen Land darstellt. Darauf aufbauend werden dann die umzusetzenden Maßnahmen abgeleitet[18].

So ist es etwa notwendig, **bei der Einführung** von neuen Produkten oder bei Projekten, die Risiken gleich zu Beginn zu identifizieren und adäquat zu adressieren, um nicht später Mehrkosten zu riskieren[19]. Insbesondere bei der aktuell üblichen Nutzung von Softwaremodulen dritter Entwickler (insbesondere im Bereich der Open Source Software) ist eine hohe Abhängigkeit von der Zuverlässigkeit und Sicherheit dieser Fremdsoftware gegeben[20].

[18] *Rosenkranz/Skopik* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 105.
[19] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 51.
[20] *Rosenkranz/Skopik* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 103.

2. DAS MANAGEMENT VON IKT-DRITTPARTEIEN

2.1. Die Rolle von IKT-DRITTPARTEIEN:

Eine Schlüsselrolle bei der Herstellung der gebotenen digitalen operationalen Resilienz haben zweifellos **IKT-Drittparteien**. Demnach ist Kapitel 5 des DORA dem Management des IKT-Drittparteienrisiko gewidmet. Das Spektrum von IKT-Drittdienstleistern ist dabei breit, und umfasst Cloud-Computing-Dienste, Software, Datenanalysedienste, Anbieter von Rechenzentrumsdienstleistungen aber auch Tochterunternehmen, die IKT-Dienstleistungen für bspw die Muttergesellschaft erbringen (ErwGr 63). Insbesondere dieses "3rd Party Risk Management" stellt eine Weiterentwicklung des status quo dar und bindet viele Ressourcen[21].

Das Vorgehen des europäischen Gesetzgebers ist aber insofern legitim, da die Auslagerung an IKT-Drittdienstleister **erhebliche Risiken** birgt. Neben den Risiken wie potentielle Qualitätsprobleme und mögliche Verluste von internem Wissen, schlagen vor allem Lock-In-Effekte sowie erhöhte IKT-Risiken ins Gewicht. Im Rahmen eines Outsoucrings kann es zu einer ungewollten Abhängigkeit vom Dienstleister kommen, was etwa dazu führen kann, dass vom Dienstleister geforderte, überraschende und/oder unverhältnismäßige Preissteigerungen akzeptiert werden müssen, bzw was generell die Verhandlungsposition schwächt[22]. Ein weiteres Risiko, das sich stetig erhöht, ist das **Cyberrisiko in der Lieferkette**. Der IKT-Dienstleister wird zum Eintrittstor für Cyberattacken[23].

Die Angriffe auf die Lieferkette scheinen sich seit der Digitalisierungswelle im Jahr 2020 **kontinuierlich zu vergrößern**. Ein möglicher Grund dafür dürfte sein, dass die großen Organisationen einen relativ robusten Sicherheitsschutz umgesetzt haben, und sich daher

---

[21] *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 54.
[22] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 151.

[23] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 152.

die Angriffsziele auf schlechter geschützte IKT-Dienstleister in den KMU-Bereichen verlagern[24]. Durch die bestehende Geschäftsbeziehung und enge technische und organisatorische Schnittstellen entsteht häufig ein trügerisches Gefühl der Sicherheit[25].

Der Unionsgesetzgeber hat diese Problematik erkannt und daher in DORA ein ganzes Kapitel mit der Bezeichnung "Management des Drittparteienrisikos" aufgenommen. Art 28 Abs 5 DORA stellt klar: Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die **angemessene Standards für Informationssicherheit einhalten**. Sofern kritische oder wichtige Funktionen betroffen sind, müssen sogar **die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit** angewendet werden.

Art 28 Abs 1 DORA nennt als allgemeine Prinzipien zum Management des IKT-Drittparteienrisikos:

- Die Finanzunternehmen selbst bleiben, auch wenn sie die IKT-Dienstleistungen ausgelagert haben, stets voll verantwortlich
- Es ist auch der **Grundsatz der Verhältnismäßigkeit** zu beachten, wobei folgende Faktoren zu berücksichtigen sind:
    - Art, Ausmaß, Komplexität und Relevanz IKT-bezogener Abhängigkeiten
    - Potentielle Auswirkungen auf die Kontinuität und Verfügbarkeit auf Einzel- und Gruppenebene

Art 28 Abs 1 lit a iVm Art 28 Abs 3 zweiter Absatz DORA dürfte wohl dahingehend auszulegen sein, dass eine **vertragliche Vereinbarung** zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister abgeschlossen werden muss. Diese Vereinbarung ist auch zu dokumentieren, wobei zu differenzieren ist, ob sich die IKT-Dienstleistung auf kritische oder

[24] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 153.
[25] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 153.

wichtige Funktionen oder Funktionen, bei denen dies nicht der Fall ist, bezieht. Einmal pro Jahr muss der **zuständigen Behörde proaktiv** ein Bericht über die Anzahl neuer Vereinbarungen über die Nutzung von IKT-Dienstleistungen, den Kategorien von IKT-Drittdienstleistern, der Art der vertraglichen Vereinbarung sowie die bereitgestellte IKT-Dienstleistung und -Funktion berichtet werden. Auf Verlangen muss den Behörden das vollständige Informationsregister zur Verfügung gestellt werden, die für eine wirksame Beaufsichtigung als notwendig erachtet wird.

Vor Abschluss der vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen müssen Finanzunternehmen gemäß 28 Abs 4 DORA folgende Beurteilungen evaluieren:

- Ob die Vereinbarung kritische oder wichtige Funktionen unterstützt.
- Sind aufsichtsrechtliche Bedingungen erfüllt.
- Sind alle relevanten Risiken, einschließlich IKT-Konzentrationsrisiken, bewertet worden.
- Sind IKT-Drittdienstleister sorgfältig ausgewählt und bewertet worden.
- Sind mögliche Interessenkonflikte identifiziert und bewertet werden.

Bei der vertraglichen Gestaltung müssen auch Sonderkündigungsrechte (Art 28 Abs 7) und, sofern kritische und wichtige Funktionen betroffen sind, spezielle Ausstiegsstrategien (**Exit-Management**) vertraglich geregelt werden. Die Ausstiegspläne, die auch dokumentiert werden müssen, müssen letztlich die Business-Kontinuität sicherstellen.

Zu beachten ist dabei, dass bereits vor dem Inkrafttreten der DORA Finanzunternehmen bei sogenannten "**Auslagerungen**" gesetzliche Anzeigepflichten beachten mussten. Die zentralen Normen, die nach wie vor in Kraft sind und daher nach wie vor zu berücksichtigen sind, sind dabei § 25 BWG, § 109 Abs 2 und Abs 4 VAG sowie § 18 Abs 1 AIFMG und § 28 iVm § 151 InvFG. Das bedeutet, das bei einer Vereinbarung über die Nutzung von IKT-Drittdienstleistungen zu prüfen ist, ob weitere sektorspezifische Anzeigeverpflichtungen

ausgelöst werden[26]. Trotz Änderung der terminologischen Anknüpfungspunkte (von ”Auslagerung” zu ”IKT-Drittparteinenrisiko”) ist davon auszugehen, dass die nach aktueller Definition als IKT-Auslagerung klassifizierten Vorgänge künftig in den Anwendungsbereich der DORA fallen[27].

2.2. Kritische und wichtige IKT-Dienstleistungen:

Jedes Finanzunternehmen hat gemäß Art 28 Abs 3 DORA bei jeder Inanspruchnahme eines IKT-Drittdienstleisters zu prüfen, ob die betreffende IKT-Dienstleistung **kritische oder wichtige Funktionen** unterstützt. Dies ist gemäß der Legaldefinition nach Art 3 Z 22 DORA dann der Fall, wenn:

„kritische oder wichtige Funktion“ eine Funktion, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde

Bei einem kritischen IKT-Drittdienstleister handelt es sich um eine Entität, deren IKT-Dienstleistungen von systemischer Bedeutung für Finanzunternehmen- und Dienstleistungen sind und deren Substituierbarkeit problembehaftet ist. Deren **Einstufung** erfolgt durch die ESA (“Europäische Aufsichtsbehörden”). Die Einstufung wird im Laufe des Jahres 2025 stattfinden, da zuvor die durch Finanzunternehmen zu übermittelnden Informationsregister von den jeweiligen nationalen Behörden an die ESA übermittelt werden[28]. In der Praxis ist der Begriff der kritischen und wichtigen Funktionen (Anfang 2025)

[26] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 154.
[27] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 155.
[28] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 174.

kaum greifbar, weshalb Finanzunternehmen mehr oder weniger unterschiedslos alle Bestandsverträge regulatorisch so behandeln, dass sie kritische oder wichtige Geschäftsfunktionen des Finanzunternehmens unterstützen könnten.[29]

Die Einstufung als kritische oder wichtige Funktion führt zu **zusätzlichen Anforderungen** an die Verwendung von IKT-Drittdienstleistern, nämlich:

- Die Inanspruchnahme von IKT-Drittdienstleistern zur Unterstützung von kritischen oder wichtigen Funktionen sind der Behörde **vor Vertragsabschluss anzuzeigen**
- Bei diesen sind die **höchsten Standards** im Zusammenhang mit Informationssicherheit zu stellen
- Im Rahmen der **Business-Continuity** sind diese gesondert zu berücksichtigen
- Es sind detaillierte **Ausstiegsstrategien** für diese Funktion zu erstellen
- Weiters müssen die in Art 30 Abs 3 vorgegebenen **vertraglichen Bestimmungen** aufgenommen werden

2.3. Technische Regulierungsstandards:

Mit Ausnahme von Kleinstunternehmen, bzw Unternehmen, die einen gemäß Art 16 DORA vereinfachten IKT-Risikomanagementrahmen anwenden dürfen, müssen Finanzinstitute eine spezifische **Strategie** hinsichtlich des Umgangs mit IKT-Drittparteienrisiko beschließen. Diese Strategie ist gemäß Art 28 Abs 2 DORA auch regelmäßig zu überprüfen.

Die Strategie enthält eine unternehmensinterne Leitlinie hinsichtlich der Nutzung von IKT-Dienstleistungen Dritter zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden. Konkrete Vorgaben zum Inhalt dieser Leitlinie für die Nutzung derartiger Dienstleister finden sich in den **technischen Regulierungsstandards** (RTS). Demnach sollen in der Leitlinie unter anderem folgende Aspekte adressiert werden[30]:

[29] Vgl *Bischof/Intveen*, ITRB 2/2025, S 45.
[30] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 158.

- Bestandteile und Parameter hinsichtlich der Governance-Struktur
- Risikomanagement
- Interne Kontrollrahmen in Bezug auf kritische oder wichtige IKT-Drittdienstleister
- Festlegung des Lifecycle-Management
- Modalitäten hinsichtlich einer Ex-ante-Risikobewertung
- Due Diligence-Bewertung samt entsprechenden Prozess dazu
- Berücksichtigung von Interessenkonflikten
- Verpflichtende Vertragsbestandteile
- Überwachung der vertraglichen Vereinbarung
- Anforderungen für einen Ausstiegsplan samt Testung des Ausstiegsplans

Die Leitlinie muss gemäß Art 3 DelVO 224/1773 **zumindest einmal jährlich** durch die Geschäftsleitung überprüft und gegebenenfalls angepasst werden.

2.4. Vorvertragliche Verpflichtungen:

Bereits vor Abschluss einer vertraglichen Vereinbarung mit einem IKT-Drittdienstleister muss gemäß Art 28 Abs 4 eine Prüfung erfolgen, ob die aufsichtsrechtlichen Bedingungen für eine Auftragsvergabe erfüllt sind. Dies geht mit einer entsprechenden **Due Diligence** Prüfung einher[31].

Die **RTS Leitlinie** hinsichtlich der Nutzung von IKT-Drittdienstleistern konkretisiert die Kriterien für die Auswahl und Bewertung des IKT-Drittdienstleisters. Demnach sind unter anderem folgende Punkte zu evaluieren:

- Reputation
- Fähigkeiten
- Finanzielle, personelle und technische Ressourcen

[31] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 159.

- Organisationsstruktur
- Möglichkeit technologische Entwicklungen zu überwachen
- Digitale betriebliche Widerstandsfähigkeit
- Einsatz von Untervergaben
- Im Falle eine Drittlandbezuges eine gesonderte Risikobewertung
- Vertraglich vereinbarte Vor-Ort-Prüfungen
- Ethisch und sozial verantwortliches agieren
- Risikoermittlung und Risikobewertung
- Und letztlich, Einhaltung der **aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit**

2.5. Wesentliche Vertragsbestimmungen:

Art 30 DORA normiert die wesentlichen, mindestens Vertragsbestimmungen, die in den Verträgen mit den IKT-Dienstleistern vereinbart werden müssen. Die Normen greifen de facto in die Vertragsfreiheit der Beteiligten ein, da Finanzunternehmen und IKT-Drittdienstleister dazu verpflichtet sind, bestimmte Mindeststandards und spezielle Anforderungen bei der Vertragsgestaltung zu beachten und bestimmte Regelungen ausdrücklich zu beachten[32]:

- **Beschreibung der Dienstleistungen**: Eine vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitstellen soll. Es muss angegeben werden, ob die Vergabe von Unteraufträgen zulässig ist und unter welchen Bedingungen dies geschehen kann.
- **Standorte**: Die Regionen oder Länder, in denen die Dienstleistungen erbracht und Daten verarbeitet werden, müssen angegeben werden. Der IKT-Drittdienstleister ist verpflichtet, das Finanzunternehmen über Änderungen dieser Standorte zu informieren.

[32] Vgl *Ernst* in CR 1/2025, S 17.

- **Datenschutz**: Bestimmungen zur Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten, einschließlich des Schutzes personenbezogener Daten, müssen enthalten sein.
- **Zugang zu Daten**: Es muss sichergestellt werden, dass das Finanzunternehmen Zugang zu den Daten hat, insbesondere im Falle einer Insolvenz oder Beendigung der vertraglichen Vereinbarungen. Die Daten müssen in einem leicht zugänglichen Format wiederhergestellt und zurückgegeben werden.
- **Dienstleistungsgüte**: Beschreibungen der Dienstleistungsgüte, einschließlich der Bedingungen für Aktualisierungen und Überarbeitungen, müssen festgelegt werden. Der Zusammenhang und die englische Fassung (service level descriptions) legen nahe, dass es sich bei der Beschreibung der Dienstleistungsgüte letztlich um Klauseln handelt, wie sie sich üblicherweise in einem Service Level Agreement finden[33].
- **Unterstützung bei IKT-Vorfällen**: Der IKT-Drittdienstleister muss Unterstützung bei IKT-Vorfällen leisten, die mit den bereitgestellten Dienstleistungen in Verbindung stehen. Diese Unterstützung muss ohne zusätzliche – extra – Kosten oder zu vorab festzusetzenden Kosten erfolgen.
- **Zusammenarbeit mit Behörden**: Der IKT-Drittdienstleister ist verpflichtet, mit den zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten.
- **Kündigungsrechte**: Es müssen Kündigungsrechte und Mindestkündigungsfristen festgelegt werden, die den Erwartungen der zuständigen Behörden entsprechen[1].
- **Schulungen und Sensibilisierung**: Der IKT-Drittdienstleister muss an Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz teilnehmen. Art 13 Abs 6 DORA sehen solche Programme für Mitarbeiter von Finanzunternehmen vor, aber auch für IKT-Drittdienstleister.

Sofern der **IKT-Drittdienstleister eine kritische** oder wichtige Funktion wahrnimmt, müssen darüber hinaus auch folgende Aspekte geregelt werden:

[33] Vgl *Ernstl*, CR 1/2025, S 19.

- Präzise quantitative und qualitative Leistungsziele (Service Levels)
- Notfallpläne
- Verpflichtung zur Durchführung von Penetrationtests
- Detaillierte Regelungen betreffend Auditrechte
- Regelung für Ausstiegsstrategien

Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters sind eindeutig festzuhalten und in einem Dokument zu **verschriftlichen**. Der Zugang zu diesem Dokument muss jederzeit gewährleistet sein (Art 30 Abs 1). Art 8 Abs 4 RTS verlangt eine schriftliche Dokumentation mit Datum und Unterschrift für den Fall von wesentlichen Änderungen im Vertragsinhalt.

Die (Un-)Zulässigkeit von Unteraufträgen in Bezug auf kritische Funktionen ist ebenso in den Vertrag aufzunehmen wie die Verpflichtung, Änderungen bei der **Unterauftragsvergabe** an das Finanzunternehmen bekanntzugeben[34].

Die Grundlagen der Vertragsgestaltung werden in Art 30 DORA gesetzt; ergänzt werden diese Bestimmungen durch Art 8 RTS und Art 4 TS-E SUB.

Auch wenn ein großer Teil der verlangten Regelungen bereits in den Verträgen existieren sollte, empfiehlt sich in der Regel eine erneute Wiedergabe der DORA-Vertragszusätze “am Gesetz entlang”, da für die Auslegung der Normen noch keine Anhaltspunkte bestehen[35]. Die Praxis arbeitet dabei mit Ergänzungen zu bereits bestehenden IT-Dienstleistungsverträgen um die vorgegebenen Aspekte umzusetzen. In der Praxis ist den Finanzunternehmen dringend zu empfehlen, sich **möglichst an den Gesetzeswortlaut** zu halten: Der Verzicht auf DORA-Mindestvertragsinhalte vergrößert unnötig die aufsichtsrechtlichen Risiken für das Finanzunternehmen. Eine Verschärfung über DORA

[34] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 165.
[35] Vgl *Ernst*, CR 1/2025, S 21.

hinaus hingegen erschwert schnell die Akzeptanz beim Vertragspartner, mit dem sich das Finanzunternehmen auf die Vertragsänderung einigen muss[36].

Zu beachten ist, dass Art 28 Abs 1 lit b und Art 4 DORA ausdrücklich betonen, dass das **Prinzip der Verhältnismäßigkeit** auch und gerade bei der Vertragsgestaltung zu beachten ist.

2.6. Prüfung von Drittdienstleistern:

Der DORA verpflichtet die Normadressaten zur Berücksichtigung der IKT-Dienstleister in die Risikoanalyse der Organisation. Folgende Fragen müssen in diesem Zusammenhang unter anderem beantwortet werden[37]:

- Werden kritische Aufgaben an den Dienstleister übergeben?
- Ist der Dienstleister (noch) geeignet?
- Wie behandelt der Dienstleister den Aspekt der Informationssicherheit?

Die damit verbundenen Maßnahmen wie Auditrechte, Kündigungsrechte und **Exit-Szenarien** zwingen die Organisationen zu evaluieren, wie ihre digitalen Dienste gemanagt werden und wie gegebenenfalls ein Wechsel stattfinden soll. In diesem Zusammenhang sollen auch die Regelungen betreffend Cloud-Switching nach dem Data Act erwähnt werden. Konkret normiert Art 28 Abs 8 DORA, dass hinsichtlich IKT-Drittdienstleistern, die kritische oder wichtige Funktionen erbringen, eine Exit-Strategie hinsichtlich folgenden Szenarien **vertraglich vereinbart** werden muss:

- Unvorhergesehene und anhaltende Unterbrechung des Dienstes
- Unangemessene oder fehlgeschlagene Leistungserbringung
- Unerwartete Beendigung des Vertragsverhältnisses

[36] Vgl *Bischof/Intveen*, ITRB 2/2025, S 48.
[37] *Rosenkranz/Skopik* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 103.

Die Maßnahmen und Schlüsselindikatoren zur laufenden Überwachung des Vertragspartners sind vertraglich festzulegen. Dabei müssen konkrete **Service Levels** in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der verwendeten Daten und Informationen konkret vereinbart und laufend überprüft werden. Die Messung der Leistung des IKT-Drittdienstleister hat anhand eindeutig definierter Leistungskennzahlen sowie Leistungs- und Schlüsselkontrollindikatoren zu erfolgen (Art 9 Abs 2 DelVO).

Gemäß Art 8 Abs 2 lit c RTS kann – unter gewissen, strengen Vorgaben – auch auf **Zertifizierungen Dritter** zurückgegriffen werden.

Diese Kontrollpflicht bezieht sich nicht nur auf den unmittelbaren/direkten IKT-Drittdienstleister des Finanzunternehmens, sondern bei Untervergaben **auch auf die Tätigkeiten von Unterauftragnehmer**, sofern kritische und wichtige Funktionen unterstützt werden[38]. In der Praxis ist die Überprüfung derartiger Vertragsketten herausfordernd, zumal die Unterauftragnehmer bislang häufig gar nicht mitgeteilt werden. Diese Praxis ist mit Inkrafttreten des DORA grundlegen zu überarbeiten[39].

Empfehlenswert ist in diesem Zusammenhang ein **Zero-Trust-Ansatz**, wonach die Zugriffsrechte auf das absolute Mindestmaß reduziert werden und zudem laufend neu geprüft werden muss, ob das eingeräumte Vertrauen nach wie vor gerechtfertigt ist[40].

Mit Blick auf das Framework NISTIR 8276 “Key Practices in Cyber Supply Chain Risk Management” und NCSC “How to assess and gain confidence in your supply chain cyber security” können auch folgende Fragen bei der Einschätzung des IKT-Drittparteien-Risiko sinnvoll sein[41]:

---

[38] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 165.
[39] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 165.
[40] *Rosenkranz/Skopik* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 103.
[41] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 181.

- Hat der IKT-Drittdienstleister Zugriff auf geistiges Eigentum
- Hat der IKT-Drittdienstleister Zugriff auf Daten
- Hat er Zugriff auf die System- und Netzwerkinfrastruktur
- Hat er Zugriff auf Kundendaten
- Gibt es eine Schnittstelle
- Hat er einen "Monopolstellung"
- Ist er in den Innovations- und Entwicklungsprozess eingebunden
- Führt dessen Ausfall zu einem Prozessstopp bzw zu einer Prozessverzögerung
- Liefert er ein vernetztes, digitales Produkt
- Sind dessen Services (umgehend) durch Alternativen ersetzbar
- Hat er einen Fernwartungszugang zu den IT-Systemen
- Handelt es sich um einen SaaS-Anwendung

Bei den Aspekten zur Evaluierung der gebotenen **Basissicherheit** kann in verschiedenen Standards Orientierung gefunden werden[42]. Zu nennen sind hierbei:

- Der BSI IT-Grundschutz
- CIS Top, 18
- ENISA Essential Baseline Security Standards
- KSÖ Cyber Risk Rating Schema sowie
- ISO-27001-Norm

Folgende **Mindeststandards** sollten dabei jedenfalls erfüllt werden[43]:

- Vorhandensein einer aktuellen Informationssicherheitsrichtlinie
- Durchführung von Schulungen zur Informationssicherheit

[42] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 186.
[43] *Heijman-Schmid/Muri/Stubbings* in *Hysek*, Praxishandbuch DORA, Linde-Verlag, S 186.

- Klare Verantwortlichkeit zum Thema Informationssicherheit
- Erstellung und Pflege eines Verzeichnisses aller IT-Assets und –Services
- Identitäts- und Berechtigungskonzeptes
    - Es muss sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Profils einen Bedarf dafür haben (“**Need-to-know-Prinzip**")
- Sichere Authentifizierung
    - Mindestkriterien für Passwörter
    - Verwendung von Multifaktor-Authentifizierung
- Sichere Konfiguration aller IT-Systeme
- Regelmäßige Aktualisierung aller IT-Systeme und Anwendungen mit Sicherheitsupdates
- Überprüfung der IT-Systeme auf Sicherheitslücken
- Laufende Überwachung aller IT-Systeme auf Malware
- Überwachung der Systemlandschaft auf ungewöhnliche Aktivitäten und Anomalien
- Verschlüsselung sensibler Daten bei der Übertragung im Internet
- Mechanismen zur Sicherheit individuell entwickelter Software
    - Es muss eine Policy zur **sicheren Software-Entwicklung** geben, die die Sicherheitsanforderungen, Secure-Coding-Rules, Testkonzepte aber auch den Schutz Rechter Dritter sowie Open Source Compliance umfasst
- Protokollierung der Systemevents aller IT-Systeme
- Erkennung und Behandlung von Sicherheitsvorfällen
- Prozess zum Management der Lieferantenrisiken
- Vorhandensein eines Notfallplans und angemessene Resilienzmaßnahmen
- Daten und Servicewiederherstellung
    - **Backup-Management**

2.7. Führung eines Informationsregisters:

Art 28 Abs 3 DORA (bzw ErwG 65) normiert für Finanzunternehmen eine **Verpflichtung zur Führung eines Informationsregisters**. Dieses Register muss sämtliche vertraglichen

Vereinbarungen hinsichtlich der Nutzung von IKT-Dienstleistungen umfassen. Diese Verpflichtung gilt auch für Kleinstunternehmen. Die Unternehmen müssen einmal pro Jahr einen Bericht hinsichtlich der neuen Vereinbarungen schaffen. Zudem ist eine Meldung an die Behörde erforderlich, wenn die beabsichtigte Veränderung dazu führt, dass eine Funktion kritisch oder wichtig wird.

Die EBA hat mit den "*ITS on the register of Information*" eine **Standardvorlage** des Informationsregister veröffentlicht, welches insgesamt 15 zu befüllende Blätter umfasst. In diesem Zusammenhang sind in der Praxis häufig Anfragen, nach der "LEI" (legal entity identifier) zu registrieren.