RA Hon.-Prof. Dr. Clemens Thiele, LL.M. Tax (GGU)/Mag.[a] Jessica Wagner • Salzburg

Vorbildliches IKT-Risikomanagement mit Auftragsverarbeitern im NIS-Zeitalter

Eine Praxisanalyse von Art 28 DSGVO, Art 25 KI-VO und Art 28–30 DORA

» jusIT 2025/2

EU-Gesetzgebung; Finanzsektor, DORA; KI-Systeme; IKT-Risikomanagement; Cybersecurity; Auftragsverarbeiter; IT-Dienstleister; Verpflichtungen, vertragliche; Cybersicherheit; Datenraum; Notfallszenarien; Vertragsgestaltung, datenrechtliche; Konvergenz

§ AEUV: Art 114; VO (EU) 2022/2554: Art 28, 29, 30; VO (EU) 2016/679: Art 28; VO (EU) 2024/1689: Art 25 Abs 4

Die VO (EU) 2022/2554, bekannt als *Digital Operational Resilience Act* (kurz: „*DORA*"),[1] hat das Ziel, die digitale operationale Resilienz des Finanzsektors zu stärken. Sie setzt neue Maßstäbe für das Management von IKT-Drittparteienrisiken, insb für den Einsatz von IKT-Dienstleistern[2] durch Verantwortliche. Für Datenschutzbeauftragte im Bankensektor ist DORA von besonderer Relevanz, da sie strenge Anforderungen an Vertragsgestaltung, Risikomanagement und Compliance stellt. Ausgehend von der Regelung für Auftragsverarbeiter nach Art 28 DSGVO wird über die besonderen Verpflichtungen für Anbieter von KI-Systemen gem Art 25 Abs 4 KI-VO eine Brücke zu den Grundlagen eines modernen IKT-Risikomanagements iSv Art 28–30 DORA gebaut, deren Tragfähigkeit sich in der Praxis bereits bewährt hat.

1. Einleitung

Der folgende Beitrag analysiert Art 28–30 DORA iVm den zugehörigen Erwägungsgründen,[3] um deren praktische Umsetzung im Hinblick auf Datenschutz und Datensicherheit zu erläutern. Darüber hinaus setzt er diese Regelungen in Beziehung zu den Anforderungen an Auftragsdatenverarbeitungsverträge iSv Art 28 DSGVO sowie zu den Verpflichtungen nach Art 25 Abs 4 KI-VO.[4] Schließlich soll gezeigt werden, dass die konsequente Umsetzung von Art 28–30 DORA zu einem universellen Modell für ein zukunftssicheres IKT-Management führt, das als Vorlage für Datendienstleistungsvereinbarungen unter Berücksichtigung eines modernen Cybersicherheitspakets eingesetzt werden kann, welches auch den Anforderungen nach der NIS-2-Richtlinie[5] standhalten dürfte.

DORA gilt seit dem 17. 1. 2025 und ergänzt bestehende Vorschriften, darunter VO (EG) 1060/2009[6] für Ratingagenturen, VO (EU) 648/2012[7] für OTC-Derivate, VO (EU) 600/2014[8] für Finanzinstrumente sowie VO (EU) 909/2014[9] für die Wertpapierabwicklung. Dies gab den Mitgliedstaaten und Finanzunternehmen einen begrenzten Zeitraum, um die Regelungen in ihre betrieblichen Strukturen zu integrieren. Die Verordnung ist unmittelbar anwendbar, ohne dass nationale Umsetzungsgesetze erforder-

1 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/101, ABl L 2022/333, 1.

2 Unter „IKT-Dienstleistern" werden im Folgenden gem Art 3 Abs 1 Nr 21 DORA sämtliche Anbieter digitaler Dienste und Datendienste verstanden, die über IKT-Systeme einem oder mehreren internen oder externen Nutzerinnen und Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen. „IKT" erfasst dabei Informations- und Kommunikationstechnologie und bezeichnet die Technik, die zum Erheben, Speichern, Übertragen und Weiterverarbeiten von Daten und Informationen genutzt wird.

3 ErwGr 64–75 DORA.

4 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, ABl L 2024/1689, 1.

5 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-RL), ABl L 2022/333, 80; Umsetzungsfrist 18. 10. 2024.

6 Verordnung (EG) 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen, ABl L 2009/302, 1, mehrfach geändert, idF ABl L 2023/2869.

7 Verordnung (EU) 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, ABl L 2012/201, 1, mehrfach geändert, idF ABl L 2021/49, 6.

8 Verordnung (EU) 600/2014 des Europäischen Parlaments und des Rates vom 15. Juli 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012, ABl L 2014/173, 84 (konsolidierte Fassung).

9 Verordnung (EU) 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012, ABl L 2014/257, 1 (konsolidierte Fassung).

lich sind. DORA entstand aus der Notwendigkeit, die operationale Resilienz nach der Finanzkrise 2008 und in Anbetracht zunehmender IKT-Risiken zu stärken. Sie ist Teil eines umfassenden digitalen Finanzpakets der EU, das auch Märkte für Krypto-Assets und Distributed-Ledger-Technologien umfasst.

2. Umsetzungsbedarf für Finanzunternehmen

Für die Unternehmen des österreichischen Bankensektors ist davon auszugehen, dass sie im Jahr 2024 ihre Hausaufgaben gemacht haben, um fit ins neue Jahr starten zu können. Gleichwohl umfasst der personelle Anwendungsbereich gem Art 2 DORA nicht nur Banken und Versicherungsunternehmen, die bereits durch die EBA/ESRB-Leitlinien[10] zur IKT-Sicherheit und zum Outsourcing mit derartigen Vorschriften vertraut sind. Auch Handelsplätze, Einrichtungen der betrieblichen Altersversorgung, Anbieter von Krypto-Dienstleistungen, Versicherungsvermittler und zahlreiche weitere Finanzunternehmen fallen in den Anwendungsbereich des neuen Regelwerks.

IKT-Anbieter – einschließlich Cloud-Service-Provider, Rechenzentren, Datenanalysedienste und Softwareanbieter, die Dienstleistungen für Finanzunternehmen erbringen, können nun insb gem Art 2 Abs 1 lit m und lit u DORA gleichermaßen dem Aufsichtsrahmen unterliegen, wenn sie als „*kritische IKT-Anbieter*“ eingestuft werden. Die Kriterien für diese Einstufung werden von den Europäischen Aufsichtsbehörden (ESAs)[11] weiter spezifiziert, basieren aber hauptsächlich darauf, wie kritisch die erbrachten Leistungen für den Finanzmarkt sind sowie in welchem Maße Abhängigkeit vom IKT-Anbieter besteht oder wie leicht dieser ausgetauscht werden kann. Im Einzelnen lassen sich die Anforderungen, wie folgt, gruppieren:

- ✓ *Technische und organisatorische Maßnahmen*: Finanzunternehmen müssen umfassende IKT-Risikomanagementrahmen entwickeln, die die in DORA geforderten Standards erfüllen. Dazu gehören:
  - *Dokumentation*: Einführung eines zentralen Registers für vertragliche Vereinbarungen;
  - *Monitoring*: Etablierung von Mechanismen zur Überwachung der Leistung und Sicherheit von IKT-Dienstleistern.
- ✓ *Anpassung von Verträgen*: Bestehende Vereinbarungen mit Drittanbietern müssen überarbeitet werden, um
  - die in Art 30 spezifizierten Klauseln zu implementieren und
  - Rechte und Pflichten klar zu regeln, insb im Hinblick auf Datenschutz und Datenverfügbarkeit.
- ✓ *Schulung und Awareness*: Mitarbeiter:innen, insb in den Bereichen IT und Recht, müssen auf die Anforderungen von DORA geschult werden. Hierzu zählen:
  - Umgang mit IKT-Risiken,
  - Compliance im Bereich Vertragsgestaltung.
- ✓ *Zusammenarbeit mit Behörden*: Finanzunternehmen müssen sich auf verstärkte Kontrollen durch Aufsichtsbehörden einstellen. Dazu gehört die Bereitschaft, regelmäßig Berichte über Drittparteienrisiken vorzulegen.

DORA stellt damit eine konkrete To-do-Liste für die erwünschte Digitalisierung und Sicherheit im europäischen Finanzsektor dar. Insbesondere Art 28–30 DORA legen klare Standards für den Umgang mit IKT-Drittanbietern fest. Bei ordnungsgemäßer Umsetzung besteht die Möglichkeit, ein effektives IKT-Risikomanagement mit Auftragsverarbeitern weit über den eigentlichen Kern des bankgeschäftlichen Bereichs hinaus zu implementieren. Für Finanzunternehmen iSv Art 2 Abs 1 DORA bedeutet dies

- eine Verbesserung der Transparenz und Sicherheit im Umgang mit digitalen Diensten,
- Anpassungen in Governance, Risikomanagement und Vertragspraxis und
- eine engere Zusammenarbeit mit Behörden.

Durch die frühzeitige Einbindung von Datenschutzbeauftragten und die Entwicklung umfassender Umsetzungsstrategien können Finanzunternehmen die Anforderungen von DORA effektiv und effizient erfüllen, vor allem mit und gegenüber den eingesetzten IKT-Dienstleistern. Denn bereits nach dem „*gewohnten*“ Regime von Art 28 DSGVO sind Verantwortliche grds auch für Datenschutzverletzungen haftbar, die durch Verstöße ihrer Auftragsverarbeiter entstehen. Art 28 DSGVO verpflichtet Verantwortliche iSv Art 4 Z 7 DSGVO nach der Rsp[12] zu einer kontinuierlichen Überwachung des Auftragsverarbeiters. Dies schließt ein, sicherzustellen, dass der Verarbeiter Daten nach Auftragsende unwiderruflich löscht bzw diese an den Verantwortlichen wieder zurückgibt.

Art 28–30 DORA bilden darüber hinaus[13] das (sektorspezifische) Regelwerk zur Handhabung von Risiken, die durch die Nutzung von Informations- und Kommunikationstechnologiedienstleistungen (IKT-Dienstleistungen) im Finanzsektor entstehen. Sie spezifizieren die Anforderungen an Finanzunternehmen im Umgang mit Drittanbietern, die für kritische oder wichtige Funktionen wesentliche IKT-Dienstleistungen bereitstellen.

Bei der Umsetzung der DORA-Anforderungen haben die Finanzunternehmen das DORA-VG zu beachten, mit dem nicht nur eine Reihe an Änderungen nationaler Gesetze (zB BWG,

10 Leitlinien und Empfehlungen und andere von der Europäischen Bankenaufsichtsbehörde (EBA) beschlossene Maßnahmen sowie die vom „European Systemic Risk Board“ (ESRB) ausgesprochenen Warnungen und Empfehlungen, abrufbar unter <https://www.fma.gv.at/eu/eba-leitlinien-und-andere-konvergenzinstrumente/> (14. 1. 2025).

11 In Deutschland die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin); für Österreich die Finanzmarktaufsichtsbehörde (FMA) gem § 2 des Bundesgesetzes über das Wirksamwerden der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA-Vollzugsgesetz – DORA-VG), BGBl I 112/2024.

12 EuGH 5. 12. 2023, C-683/21 (Nacionalinis visuomenes sveikatos centras-Fall), ECLI:EU:C:2023:949 = jusIT 2024/20, 33 (*Kröpfl*): COVID-App; deutlich zuletzt OLG Dresden 10. 9. 2024, 4 U 602/24 (Musik-Streaming-Dienst), openJur 2024, 10701; vgl auch OGH 15. 6. 2016, 4 Ob 30/16i (Schockrechnung des Access-Providers), jusIT 2016/66, 145 (*Thiele*) = MR 2016, 348 (*Blaha*) = ZIIR 2016, 453 (*Thiele*).

13 Die DSGVO bleibt unberührt bzw genießt Vorrang, sofern kein Sonderdatenschutzrecht der DORA eingreift (vgl Art 45 Abs 1 lit c und Art 56 Abs 1 DORA: „im Einklang mit der Verordnung (EU) 2016/679“).

VAG 2016), sondern auch eine Konkretisierung der Verwaltungsstrafen iSv Art 50 Abs 4 DORA bei Verstößen gegen bestimmte DORA-Bestimmungen erfolgt ist. In §§ 7 f DORA-VG können Geldstrafen bei Verstößen gegen Art 28–30 DORA nicht nur gegen juristische Personen, sondern auch gegen natürliche Personen, die zur Vertretung nach außen berufen bzw Beauftragte nach § 9 VStG sind, verhängt werden.[14] Für Verantwortliche iSv § 9 VStG, die das Drittparteienrisiko nicht gem Art 28 Abs 1–8 und Art 29 DORA managen oder vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen nicht gem Art 30 Abs 1–4 DORA treffen, ist die Verhängung einer Verwaltungsstrafe von bis zu € 150.000 möglich. Auch kann die FMA eine Geldstrafe gegen juristische Personen verhängen, die bis zu € 500.000 oder bis zu 1 % des jährlichen Gesamtnettoumsatzes, je nachdem, welcher Betrag höher ist, betragen kann.[15]

3. Allgemeine Prinzipien

3.1. Normzweck und Regelungsgehalt von Art 28 DORA

Art 28 DORA dient der Sicherstellung, dass Finanzunternehmen ihre operationale Resilienz wahren, auch wenn sie IKT-Dienstleistungen von Drittanbietern beziehen. Ziel ist es, eine lückenlose Verantwortlichkeit und ein strukturiertes Risikomanagement zu gewährleisten.

Art 28 DORA stellt sohin die Grundprinzipien für den Umgang mit IKT-Drittparteienrisiken für die Verantwortlichen auf und umfasst die Vorgaben zu Verantwortlichkeiten, Strategien, Dokumentationspflichten, Vertragsgestaltung, Sicherheitsanforderungen, Auditrechten und Kündigungsmodalitäten.

3.2. Verantwortung des Finanzunternehmens (Art 28 Abs 1 DORA)

Da Finanzunternehmen jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen nach DORA verantwortlich bleiben,[16] ist das von den IKT-Drittparteien ausgehende Risiko zu steuern und als integraler Bestandteil ihres IKT- Risikomanagementrahmens zu betrachten. Drittparteienrisiken müssen nahtlos in den unternehmensweiten Rahmen integriert sein. Bei der Verwaltung des IKT-Drittparteienrisikos ist darauf zu achten, dass die Maßnahmen angemessen sind. Dieser Grundsatz der Verhältnismäßigkeit verlangt die individuelle Bewertung von Art, Umfang und Relevanz der Abhängigkeiten des eingesetzten IKT-Dienstleisters. Zu berücksichtigen sind zudem die Risiken infolge vertraglicher Vereinbarungen über die Nutzung von IKT-Dienstleistungen, insb die Abhängigkeiten nach Kritikalität, Komplexität und möglichen Auswirkungen. MaW ist zu beurteilen, wie kritisch die Dienstleistungen sind und welche potenziellen Auswirkungen der Ausfall auf die Kontinuität und Qualität von Finanzdienstleistungen haben könnte.

3.3. Strategie für Drittparteienrisiken (Art 28 Abs 2 DORA)

Vorgesehen ist, dass Finanzunternehmen Strategien[17] für Drittparteienrisiken iSv Art 3 Z 18 DORA entwickeln und diese regelmäßig überprüfen. Diese Strategien[18] müssen klare Leitlinien zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, enthalten sowie die Nutzung mehrerer Anbieter in Betracht ziehen. Die im Rahmen des IKT-Risikomanagementrahmens beschlossenen Strategien sind an aktuelle Entwicklungen anzupassen.

3.4. Informationsregister und Berichterstattung (Art 28 Abs 3 DORA)

Im Rahmen des IKT-Risikomanagementrahmens ist ein Informationsregister[19] mit allen vertraglichen Vereinbarungen zu führen. Diese „*Dokumentationspflicht*“ soll die Transparenz und Nachverfolgbarkeit aller Vereinbarungen gewährleisten. Dabei muss zwischen den Vereinbarungen, die IT-Dienstleistungen für kritische oder wichtige Funktionen betreffen, und denjenigen, die das nicht tun, unterschieden werden. Im Rahmen dieser Pflicht zur Dokumentation müssen die Finanzunternehmen den zuständigen Behörden auch mindestens einmal jährlich Bericht[20] erstatten sowie über jede geplante Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sowie in dem Fall, dass eine Funktion kritisch oder wichtig geworden ist, unterrichten. Auf behördliche Anfrage können sie zudem aufgefordert werden, bestimmte Teile dieses Registers zusammen mit allen Informationen zur Verfügung zu stellen.

3.5. Vertragsprüfungen vor Abschluss (Art 28 Abs 4 DORA)

DORA verlangt, dass vertragliche Vereinbarungen nur dann abgeschlossen werden dürfen, wenn angemessene Standards für die Informationssicherheit eingehalten werden. Diesbezüglich be-

14 Vgl *Tlapak/Repic*, Der Countdown läuft: Was es bei der Umsetzung der DORA im Versicherungswesen zu beachten gilt, ZVers 5/2024, 225 (227).

15 Vgl zu §§ 7, 8 DORA-VG näher *Sedlak/Wagner*, Sanktionsregime, in Hysek (Hrsg), Praxishandbuch DORA, 350 (373 ff) mwH.

16 Vgl Art 28 Abs 1 lit a DORA.

17 ErwGr 65 DORA unterstreicht die Bedeutung eines strategischen Ansatzes: „[...] durch die Annahme einer eigenen Strategie [...] auf der Grundlage einer kontinuierlichen Überprüfung aller Abhängigkeiten“.

18 Näher dazu *Heijmann-Schmid/Muri/Stubbings*, Das Management des Drittparteienrisikos und der neue Überwachungsrahmen für kritische IKT-Drittdienstleister, in Hysek (Hrsg), Praxishandbuch Digital Operational Resilience Act – DORA (2025) 151 (155 f).

19 ErwGr 65 DORA betont: „Finanzunternehmen sollten verpflichtet werden, ein Informationsregister zu führen.“

20 Dieser Bericht hat die Anzahl neuer Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die Kategorien von IKT-Drittdienstleistern, die Art der vertraglichen Vereinbarungen sowie die bereitgestellten IKT-Dienstleistungen und -Funktionen zu enthalten.

steht für die Verantwortlichen eine „*Sorgfaltspflicht*“.[21] Vor Vertragsabschluss ist eine gründliche Analyse[22] durchzuführen und die Risiken, insb Konzentrationsrisiken sowie mögliche Interessenkonflikte, sind sorgfältig zu bewerten.[23]

3.6. Informationssicherheit und Kündigungsrechte

Gem Art 28 Abs 5–7 DORA dürfen nur Anbieter mit aktuellen Sicherheitsstandards eingesetzt werden. Vor Vertragsabschlüssen ist eine umfassende Due-Diligence-Prüfung der IKT-Drittdienstleister vorzunehmen. Betreffen vertragliche Vereinbarungen kritische oder wichtige Funktionen, so sollten Finanzunternehmen darauf achten, dass IKT-Drittdienstleister die aktuellsten und höchsten Standards anwenden.[24] Sicherzustellen ist zudem, dass die vertraglichen Vereinbarungen bestimmte wichtige Kündigungsgründe[25] enthalten, zB wenn ein erheblicher Verstoß des IKT-Drittdienstleisters gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen vorliegt und festgestellt wird.[26]

3.7. Ausstiegsstrategien (Art 28 Abs 8 DORA)

Finanzunternehmen müssen auch Exit-Strategien erarbeiten, um mit Ausfällen von IKT-Dienstleistungen oder Verschlechterungen der Dienstleistungsqualität umgehen zu können. Die Erstellung von Ausstiegsplänen soll diese Risiken gebührend berücksichtigen und einen „*geordneten Übergang*“ zu einem alternativen Anbieter ermöglichen. Ziel dieser Ausstiegsstrategien ist die Aufrechterhaltung der Kontinuität und Qualität der erbrachten Dienstleistungen, sohin die Sicherung der Geschäftskontinuität.[27]

3.8. Rechtsfolgen einer mangelhaften Umsetzung

Neben der Verhängung von Verwaltungsstrafen iSv §§ 7, 8 DORA-VG kann die Nichterfüllung dieser Anforderungen schwerwiegende aufsichtsrechtliche Konsequenzen nach sich ziehen, da sie die operationale Resilienz des Finanzunternehmens gefährdet. Behörden können daher Sanktionen verhängen oder Maßnahmen zur Nachbesserung anordnen.[28]

4. Vorläufige Bewertung des IKT-Konzentrationsrisikos

4.1. Normzweck und Regelungsgehalt von Art 29 DORA

Art 29 schützt vor systemischen Risiken, die durch die Konzentration von Dienstleistungen bei wenigen Anbietern entstehen könnten. Es soll verhindert werden, dass eine Abhängigkeit von einem einzigen IKT-Drittanbieter die digitale Resilienz gefährdet.

Die Vorschrift verlangt von Finanzunternehmen, potenzielle Konzentrationsrisiken zu analysieren, bevor neue Verträge geschlossen werden. Dies umfasst auch die Unterauftragsvergabe an Drittanbieter, insb in Drittländern.

4.2. Risiken durch Konzentration (Art 29 Abs 1 DORA)

Bei der Bewertung von Risiken der IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen haben die Finanzunternehmen zu prüfen, ob IKT-Anbieter leicht ersetzbar sind oder es hierbei zu Schwierigkeiten kommen könnte. Anbieter, die „*nicht ohne Weiteres*“ bzw schwer ersetzbar sind, müssen besonders kritisch bewertet werden. Darüber hinaus ist zu ermitteln, ob mehrfache vertragliche Vereinbarungen mit demselben IKT-Drittdienstleister oder mit eng verbundenen IKT-Drittdienstleistern bestehen. Solche Beziehungen erhöhen das Risiko von Abhängigkeiten und sind, wenn möglich, zu vermeiden. Die Abwägung von alternativen Lösungen ist daher entscheidend, um sicherzustellen, dass die ausgewählten Lösungen mit den geschäftlichen Zielen und der Strategie zur digitalen Resilienz des Unternehmens im Einklang stehen.

4.3. Drittlandsrisiken und Unterauftragsvergabe (Art 29 Abs 2 DORA)

Der Einsatz von IKT-Drittdienstleistern in Drittländern birgt oft zusätzliche Risiken, zB unzureichende Datenschutzstandards, sodass die Finanzunternehmen sicherstellen müssen, dass „*die Rechtsvorschriften in diesem Drittland wirksam durchgesetzt werden*“ können.[29] Dies gilt ebenso bei IKT-Unterauftragnehmern. Bei „*Unteraufträgen*“ müssen Finanzunternehmen zudem die gesamte Kette potenzieller Unterauftragnehmer überwachen, insb im Hinblick auf die Qualität und Sicherheit der IKT-Dienstleistung. Dazu betont ErwGr 67 DORA, dass „*fundierte Analysen von Unterauftragsvereinbarungen*“ notwendig sind.

4.4. Rechtsfolgen der Nichtbeachtung

Neben der Verhängung von Verwaltungsstrafen iSv §§ 7, 8 DORA-VG kann die Nichteinhaltung dieser Vorschriften zu einem Verlust der operativen Kontrolle führen und die Resilienz

21 Zutreffend handelt es sich um „vorvertragliche Pflichten“ (so *Heijmann-Schmid/Muri/Stubbings* in Hysek (Hrsg), Praxishandbuch DORA, 151 [159 ff]).

22 ErwGr 66 DORA nennt dies „eine gründliche Analyse vor Vertragsabschluss“.

23 Vgl auch *Gollmann*, Im Überblick: Regelungsinhalte & Ziele des Digital Operational Resillience Act, in Hysek (Hrsg), Praxishandbuch DORA, 22 (29).

24 Vgl ErwGr 66 DORA.

25 Sog „Ausstiegsplanung“, vgl *Heijmann-Schmid/Muri/Stubbings* in *Hysek* (Hrsg), Praxishandbuch DORA, 151 (161 f).

26 Art 28 Abs 7 lit a DORA.

27 ErwGr 74 DORA stellt klar: „[…] verbindliche Übergangszeiträume, in denen die IKT-Drittdienstleister weiterhin die einschlägigen Dienste bereitstellen sollten“.

28 Vgl *Sedlak/Wagner*, Sanktionsregime, in Hysek (Hrsg), Praxishandbuch DORA, 350 (362 ff).

29 Vgl ErwGr 67.

des Unternehmens untergraben. Neben der Verhängung von Sanktionen[30] kann auch ein Konzessionsentzug die Folge sein.

5. Wesentliche Vertragsbestimmungen

5.1. Normzweck und Regelungsgehalt von Art 30 DORA

Art 30 DORA regelt die Mindestinhalte von Verträgen mit IKT-Dienstleistern und definiert detailliert, welche Vertragsbestandteile für IKT-Dienstleistungen erforderlich sind. Besondere Aufmerksamkeit gilt den Anforderungen für kritische oder wichtige Funktionen. Ziel der Festlegung der wesentlichen Vertragsbestimmungen ist es, die Verantwortlichkeiten eindeutig zuzuweisen und datenschutzrechtliche sowie betriebliche Anforderungen angemessen zu berücksichtigen.

5.2. Schriftlichkeit (Art 30 Abs 1 DORA) und Mindestanforderungen an Verträge (Art 30 Abs 2 und 3 DORA)

Die Parteien müssen klare Vereinbarungen in einem schriftlichen Dokument treffen, welche die Rechte und Pflichten regeln.[31] Die Elemente, die in den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen enthalten sein müssen, sind in Art 30 Abs 2 lit a–i DORA geregelt. Folgende „*Kernelemente*" müssen sich im Vertrag befinden:

- *Leistungsbeschreibung*: detaillierte Beschreibung der IKT-Dienstleistungen und Zulässigkeit der Unteraufträge samt den Bedingungen dafür (lit a);
- *Standorte*: Angabe der Regionen oder Länder, in denen die Dienstleistungen erbracht und Daten verarbeitet werden, Bekanntgabepflicht des IKT-Drittdienstleisters über Standortänderung (lit b);
- *(Datenschutz-)Regelungen* zur Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit, insb zum Schutz personenbezogener Daten (lit c);
- *Datenzugang*: Bestimmungen zum Zugang, zur Rückgabe sowie zur Wiederherstellung von Daten (lit d);
- *Dienstleistungsgüte*: Beschreibung der Qualität der Dienstleistungen, einschließlich Updates (lit e);
- *Unterstützungspflicht bei IKT-Vorfällen* (lit f);
- *Verpflichtung zur Behördenzusammenarbeit* (lit g);
- *Regelungen zu Kündigungsfristen und -rechten* (lit h);
- *Schulung und Sensibilisierung*: Bedingungen zur Teilnahme an Schulungen zur IKT-Sicherheit (lit i).

Die vertraglichen Regelungen zur Nutzung von IKT-Dienstleistungen, die *kritische oder wesentliche Funktionen* unterstützen,[32] müssen zusätzlich die in Abs 3 geforderten Elemente beinhalten. So nennt zB ErwGr 72 DORA „*die Spezifikation der vollständigen Beschreibung der Dienstleistungsgüte*", sodass IKT-Drittdienstleister Sicherheitsmaßnahmen nachweisen und Notfallpläne erstellen müssen (Abs 3 lit c), oder nach Abs 3 lit i das „*uneingeschränkte Auditrecht*" des Finanzunternehmens oder eines beauftragten Dritten vor Ort des IKT-Drittdienstleisters.

5.3. Standardvertragsklauseln (Art 30 Abs 4 DORA)

Zur Erhöhung der Rechtssicherheit können Standardvertragsklauseln als verlässliches Instrument dienen. Die freiwillige Verwendung von Standardvertragsklauseln, die von staatlichen Behörden oder von Organen der Union entwickelt wurden, insb die Verwendung der von der Europäischen Kommission für Cloud-Computing-Dienste entwickelten Vertragsklauseln können den Finanzunternehmen und IKT-Drittdienstleistern eine zusätzliche Rückversicherung bieten, indem sie die Rechtssicherheit in Bezug auf die Nutzung von Cloud-Computing-Diensten im Finanzsektor in voller Übereinstimmung mit den Anforderungen und Erwartungen des Finanzdienstleistungsrechts der Europäischen Union erhöht.[33]

5.4. Rechtsfolgen mangelhafter Vertragsgestaltung

Neben der Verhängung von Verwaltungsstrafen iSv §§ 7, 8 DORA-VG kann die Nichteinhaltung von Art 30 zu ineffektiven Vertragsbeziehungen führen, wodurch Datenschutzverletzungen und operationale Risiken zunehmen. Bei kritischen Funktionen könnten aufsichtsrechtliche Konsequenzen folgen.

6. Verpflichtungen für Anbieter von KI-Systemen nach Art 25 KI-VO

6.1. Parallele Anwendbarkeit

Der risikobasierte Ansatz der KI-VO bringt aus einer Perspektive der Produktsicherheit ebenfalls für bestimmte IKT-Systeme Anforderungen mit sich, die bei der Vertragsgestaltung uU zu beachten sind. Betroffen von den konkreten Verpflichtungen nach Art 25 Abs 4 KI-VO ist lediglich der Einsatz von Hochrisiko-KI.[34] Art 25 Abs 4 KI-VO verpflichtet Anbieter solcher Systeme, sicherzustellen, dass Nutzer diese rechtmäßig und konform mit den Vorschriften betreiben. Als grundlegende Prämisse ist die fehlende Sperrwirkung der KI-VO gegenüber DSGVO und DORA festzuhalten,[35] sodass KI-Systeme iSv Art 3 Z 1 KI-VO[36] nach sämt-

30 Vgl *Sedlak/Wagner*, Sanktionsregime, in Hysek (Hrsg), Praxishandbuch DORA, 350 (363 f).

31 Ansatzweise bereits in Prüffragen *Pollirer*, Checkliste DORA (Teil 1), Dako 2024, 111 (113).

32 Vgl *Heijmann-Schmid/Muri/Stubbings* in Hysek (Hrsg), Praxishandbuch DORA, 151 (163 f).

33 Vgl ErwGr 75 DORA.

34 Siehe dazu gleich unten Abschnitt 6.3.

35 So ausdrücklich Art 2 Abs 7 KI-VO, der festhält, dass diese Verordnung nicht die DSGVO bzw EU-DSGVO oder die ePrivacy-RL oder die JI-RL (EU) 2016/680 „berührt". Eine Rückausnahme davon halten Art 10 Abs 5 und Art 59 KI-VO bereit, worauf aber im Folgenden mangels Themenrelevanz nicht eingegangen wird.

36 Zur äußerst schwierigen Bestimmung dieses Dreh- und Angelpunktes der KI-VO ausf *Martini/Wendehorst/Wendehorst*, KI-VO Kommentar (2024) Art 3 Rz 50 ff.

lichen Rechtsakten ausgestaltet werden können und wohl auch müssen. Denn die KI-VO verdrängt die DSGVO nicht. Sofern personenbezogene Daten iSv Art 4 Z 1 DSGVO verarbeitet werden, ist die DSGVO weiterhin zu beachten.

Für die Kautelarpraxis erscheint daher eine Analyse von Art 25 Abs 4 KI-VO nach Normzweck, Regelungsgehalt und Rechtsfolgen dieser Vorschrift lohnenswert. Anschließend werden die relevanten Themen für eine Vertragsgestaltung offengelegt und Parallelen zu Art 28 DSGVO gezogen.

6.2. Normzweck und Regelungsgehalt von Art 25 Abs 4 KI-VO

Art 25 Abs 4 KI-VO dient dem Schutz von Grundrechten sowie der Sicherheit und Gesundheit der Nutzer und Dritter gleichermaßen.[37] Die mit „*Verantwortlichkeiten entlang der KI-Wertschöpfungskette*“ übertitelte Vorschrift bezweckt, durch ausführliche Dokumentation letztlich die Haftungssituation bei der Verwendung von IKT-Systemen, die der Hochrisikoklassifikation entsprechen, besser abzubilden.[38] Zentrale Hochrisiko-KI-Systeme iSv Art 6 Abs 1 KI-VO oder Art 6 Abs 2 iVm Anhang III KI-VO betreffen gesellschaftlich sensible Bereiche, wie Gesundheitsversorgung, Strafverfolgung oder Bildung, die erhebliche Auswirkungen auf Individuen und ihre Rechte haben können. Ziel der in Art 25 Abs 4 Satz 1 KI-VO vorgesehenen Offenlegungsverpflichtung ist es, Verantwortlichkeiten klar zuzuweisen und den sicheren Betrieb solcher High-Risk-Systeme durch vertragliche Festlegungen sicherzustellen. Dabei macht es keinen Unterschied, ob die jeweiligen Unternehmen selbst das Hochrisiko-KI-System betreiben oder bloß Komponenten, Dienste und Verfahren bereitstellen, die in einem solchen System verwendet oder in ein Hochrisiko-KI-System integriert werden.[39]

Der Regelungsgehalt von Art 25 Abs 4 KI-VO besteht darin, Anbieter der einschlägigen KI-Systeme zu verpflichten, durch vertragliche Vereinbarungen Folgendes sicherzustellen:

- *Transparenz und Bereitstellung von Informationen*:[40] Anbieter müssen Nutzer über die Funktionalität, Risiken und Sicherheitsvorkehrungen informieren.
- *Laufende Überwachung und Wartung*:[41] Sicherheitsupdates und technische Überprüfungen sind während der gesamten Lebensdauer sicherzustellen.
- *Haftungs- und Mitwirkungsregelungen*: Anbieter müssen Nutzer befähigen, Sicherheitsmängel zu melden und den Einsatz anzupassen.

Als Zwischenergebnis lässt sich festhalten, dass sich aus der Hochrisikoeinstufung nach Anhang III der KI-VO ganz wesentliche Schlussfolgerungen für die vertragliche Beauftragung von KI-Systemanbietern zB im Bereich der biometrischen Fernidentifizierung iVm Scoring-Applikationen ergeben.[42]

6.3. Schriftliche Anbieter-Nutzer-Vereinbarungen

Art 25 Abs 4 Satz 1 KI-VO statuiert eine Verpflichtung zur vertraglichen Festlegung in Schriftform, wobei insoweit auch jede elektronische Form ausreicht, die den Beweiszweck erfüllt.[43] Anbieter von Hochrisiko-KI-Systemen und Dritte, die Instrumente, Dienste, Komponenten oder Verfahren bereitstellen, die in solchen Systemen verwendet oder integriert werden, müssen schriftlich die Bereitstellung von Informationen, Fähigkeiten, technischem Zugang und Unterstützung, die erforderlich sind, damit der Anbieter die regulatorischen Anforderungen der KI-VO erfüllen kann, vereinbaren. Diese Verpflichtung gilt nicht für Dritte, die nicht allzweckfähige KI-Modelle, dh keine allgemeinen Verwendungszwecke, unter freier und quelloffener Lizenz öffentlich zugänglich machen.[44]

Die Verpflichtungen für IKT-Dienstleister lassen sich daher folgendermaßen konturieren:

- Bereitstellung relevanter Informationen iSv Art 25 Abs 1 KI-VO;
- Sicherstellung von Sicherheits- und Risikomanagementsystemen iSv Art 9 iVm Art 17 KI-VO;
- Unterstützung der Nutzer durch geeignete Maßnahmen, um deren Compliance sicherzustellen.

Als Adressaten dieser Verpflichtungen gelten neben den Anbietern von Hochrisiko-KI-Systemen auch Dritte, die Instrumente, Dienste, Komponenten oder Verfahren bereitstellen, die in Hochrisiko-KI-Systemen verwendet oder integriert werden. Gleichermaßen besteht auch hier eine Open-Source-Ausnahme für jene Dienstleister, die Open-Source-Tools bereitstellen, die nicht als allgemeine KI-Modelle gelten.

Verstöße gegen Art 25 Abs 4 KI-VO führen zu Bußgeldern. Die KI-VO sieht hohe Sanktionen für Anbieter vor, die den Pflichten nicht nachkommen, namentlich bis zu 6 % des globalen Jahresumsatzes nach Art 71 KI-VO. Darüber hinaus besteht eine erhöhte Haftpflicht. Anbieter können für Schäden haftbar gemacht werden, wenn Nutzer aufgrund fehlender Informationen oder technischer Mängel Schäden erleiden.

37 Vgl ErwGr 88 der KI-VO.
38 Vgl *Martini/Wendehorst/Gössl*, KI-VO Art 25 Rz 3: „Pflichten des Quasi-Herstellers“.
39 Zutr *Martini/Wendehorst/Gössl*, KI-VO Art 25 Rz 53.
40 Vgl Art 13 KI-VO.
41 Vgl Art 23 KI-VO.
42 Vgl EuGH 7. 12. 2023, C-634/21 (SCHUFA Holding), AnwBl 2024/122, 258 (*Feiler/Brandauer*) = DSB 2024, 19 (*Juszcyk*) = ecolex 2024/112, 191 (*Kern*) = VbR 2023/147, 223 (*Leupold/Gelbmann*); dazu *Zavadil/Rohner*, Auswirkungen der SCHUFA-Urteile auf Kreditauskunfteien und Bonitätsbewertungen, Dako 2024/4, 7, und *Salomon/Trieb*, Ermittlung eines Score-Werts kann das Verbot der automatisierten Entscheidung (Art 22 DSGVO) verletzen. Auslegung des Verbots der automatisierten Entscheidung im Rahmen der EuGH-E C-634/21, SCHUFA Holding (Scoring), ZFR 2024, 119.
43 Unklar *Martini/Wendehorst/Gössl*, KI-VO Art 25 Rz 55.
44 Sog „Open-Source-Ausnahme“; *Martini/Wendehorst/Gössl*, KI-VO Art 25 Rz 58: „Open-Access-Privilegierung“.

6.4. Vertragsgestaltung zur Umsetzung von Art 25 Abs 4 KI-VO

Zunächst ist darauf hinzuweisen, dass gem Art 25 Abs 4 UAbs 2 KI-VO das Büro für Künstliche Intelligenz freiwillige Musterbedingungen für Verträge zwischen Anbietern und Dritten ausarbeiten und empfehlen kann. Diese Bedingungen sollen branchenspezifische oder geschäftsspezifische Anforderungen berücksichtigen. Die Musterbedingungen werden kostenlos und in einem nutzerfreundlichen elektronischen Format veröffentlicht.[45] Bereits aus einer Zusammenschau von Art 25 iVm Art 6 Abs 2 KI-VO und Anhang III lässt sich folgender Pflichtenkatalog festhalten:[46]

6.4.1. Transparenz- und Informationspflichten

Die Vereinbarungen müssen klare Regelungen enthalten, die

- Umfang und Inhalt der bereitzustellenden Informationen spezifizieren, einschließlich Dokumentationen zu Algorithmen, Datenquellen und Risiken;
- Schulungsmaßnahmen für Nutzer vorsehen, um diese über den sicheren Einsatz des Systems zu informieren.

6.4.2. Haftungsklauseln

Die Anbieter sollten die Haftung bei Fehlfunktionen präzise definieren. Regelungen zur Haftungsübernahme bei Sicherheitsvorfällen oder Rechtsverstößen müssen enthalten sein.

6.4.3. Wartungs- und Monitoring-Pflichten

Die schriftlichen[47] Vereinbarungen sollten

- Pflichten zur Bereitstellung von Sicherheitsupdates und deren Fristen regeln;
- Mechanismen für die fortlaufende Überprüfung des Systems enthalten, um Konformität sicherzustellen.

6.4.4. Mitwirkungsrechte der Nutzer

Nutzern sollten vertragliche Kontrollrechte eingeräumt werden, wie die Anpassung oder Unterbrechung des Systembetriebs bei Sicherheitsmängeln. Vereinbarungen zu einer Meldepflicht bei festgestellten Sicherheitsrisiken sind unbedingt erforderlich.

6.5. Vergleich mit und Ergänzung der Auftragsdatenvereinbarung iSv Art 28 DSGVO

In der gebotenen Kürze können bereits wesentliche Parallelen für die Vertragspraxis ausgemacht werden:

- *Informationspflichten*: Beide Normen verlangen detaillierte Informationen zu Sicherheitsvorkehrungen und Funktionsweisen.
- *Überwachungspflichten*: Sowohl Art 28 DSGVO als auch Art 25 KI-VO fordern fortlaufende Kontrolle und regelmäßige Updates.
- *Vertragliche Fixierung*: Beide Vorschriften setzen auf schriftliche Vereinbarungen, um die Einhaltung regulatorischer Vorgaben sicherzustellen.

Gleichermaßen fallen *Unterschiede* auf, die einen Adaptierungs- und Ergänzungsbedarf nach sich ziehen:

- Die DSGVO zielt auf den Schutz personenbezogener Daten, während die KI-VO umfassendere Anforderungen an die Funktionsweise und die Sicherheit von KI-Systemen stellt.
- Die KI-VO geht über den Datenschutz hinaus und berücksichtigt die technische Integrität und gesellschaftlichen Auswirkungen von KI.

Daraus lassen sich folgende *relevante Klauseln für die Kautelarpraxis* mitnehmen:

- *Transparenzpflichten*: detaillierte Beschreibung der Funktionalität und Risiken des KI-Systems;
- *Sicherheitsklauseln*: Verpflichtung zu regelmäßigen Updates und technischer Überprüfung;
- *Haftung und Risiko*: Definition der Haftungsübernahme für Fehlfunktionen und Sicherheitsverstöße;
- *Meldepflichten*: Vorgaben zur Kommunikation von Sicherheitsvorfällen und Maßnahmen zur Risikobegrenzung;
- *Nutzerrechte*: Kontroll- und Anpassungsrechte der Nutzer.

Als *Zwischenergebnis* ist zusammenfassend festzuhalten, dass Art 25 Abs 4 KI-VO erhebliche Anforderungen für Anbieter von Hochrisiko-KI-Systemen mit sich bringt. Um Rechtskonformität zu gewährleisten, müssen Anbieter nicht nur technische und organisatorische Maßnahmen ergreifen, sondern auch umfassende vertragliche Regelungen schaffen. Die Einbindung dieser Verpflichtungen in die Kautelarpraxis erfordert eine sorgfältige Abstimmung mit bestehenden Regelungen, insb aus der DSGVO. Dies sichert nicht nur die Rechtmäßigkeit des Betriebs, sondern minimiert auch Haftungsrisiken für Anbieter und Nutzer.

7. Vergleich mit der Auftragsdatenverarbeitung nach Art 28 DSGVO

7.1. Normzweck und Regelungsgehalt (Art 28 DSGVO)

Diese Bestimmung bezweckt die Wahrung des Schutzniveaus der DSGVO im Rahmen der praxisrelevanten Konstellation der Auftragsverarbeitung. Art 28 DSGVO regelt neben der Auswahl bzw dem Einsatz geeigneter Auftragsverarbeiter auch die Rechte und Pflichten, die auf Basis eines Vertrags oder eines anderweitig bindenden Rechtsinstruments[48] geregelt werden müssen.

7.2. Hinreichende Garantien

Der Verantwortliche hat bereits im Rahmen seiner Auswahlentscheidung zu berücksichtigen, ob der Auftragsverarbeiter die

45 Die Umsetzungsfrist dafür endet am 2. 8. 2026 gem Art 113 Abs 2 KI-VO.
46 Ebenso *Söbbing*, KI-VO und Vertragsgestaltung, ITRB 2024, 326 f.
47 Aus Beweisgründen kommen auch sonstige (gleichwertige) elektronische Formate in Betracht.
48 Die Rechte und Pflichten zwischen Verantwortlichem und Auftragsverarbeiter können zB in den Materiengesetzen (bei der Heranziehung von Behörden) oder in individuellen Rechtsakten (Anordnung der Staatsanwaltschaft, gerichtlicher Beschluss) festgelegt werden.

hinreichenden Garantien zur Durchführung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten bietet und eine datenschutzkonforme Verarbeitung gewährleisten kann.[49] Die notwendigen Garantien setzen insb voraus, dass der Auftragsverarbeiter über genügend Fachwissen, Zuverlässigkeit und Ressourcen verfügt.[50]

7.3. Schriftlichkeit und Mindestanforderungen an Verträge (Art 28 Abs 3 DSGVO)

Die Auftragsverarbeitung muss auf der Basis eines Vertrages oder eines anderweitig bindenden Rechtsinstruments durchgeführt werden. Art 28 Abs 3 DSGVO verlangt zunächst grundlegende Festlegungen zu folgenden Punkten:

- Gegenstand und Dauer der Vereinbarung;
- Art und Zweck der Verarbeitung;
- Art der personenbezogenen Daten;
- Kategorien betroffener Personen und
- Pflichten und Rechte des Verantwortlichen.

Orientiert an dem risikobasierten Ansatz, sind insb auch die Pflichten des Auftragsverarbeiters bei der geplanten (Auftrags-) Verarbeitung zu berücksichtigen:[51]

- *Dokumentation der Weisungen* (lit a): Die Auftragsverarbeitung ist nur gemäß den erteilten Weisungen erlaubt, die vom Auftragsverarbeiter auf ihre Rechtmäßigkeit überprüft werden müssen; bei Zweifeln ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen unverzüglich zu informieren.
- *Verschwiegenheitsverpflichtung* (lit b): Auch die Mitarbeiter:innen des Auftragsverarbeiters sind zur Vertraulichkeit verpflichtet.
- *Datensicherheitsmaßnahmen* (lit c): Der Auftragsverarbeiter muss versichern, dass er die erforderlichen Datensicherheitsmaßnahmen iSv Art 32 DSGVO ergreift.
- *Sub-Auftragsverarbeiter* (lit d): Falls ein Unterauftragsverhältnis nicht ausgeschlossen wird, ist sicherzustellen, dass bei der Vergabe weiterer Aufträge bei den Sub-Auftragsverarbeitern dieselben Anforderungen erfüllt sind, denen der Auftragsverarbeiter unterliegt.
- *Unterstützungspflichten* (lit e, f): insb im Hinblick auf die Unterstützungspflicht bei Betroffenenanfragen, die Gewährleistung der Datensicherheit, Melde- und Benachrichtigungspflichten im Fall von Datenschutzverletzungen, etwaige Datenschutz-Folgenabschätzungen und die ggf notwendige Vorabkonsultation der Datenschutzbehörde durch den Verantwortlichen.
- *Rückgabe- bzw Löschungsverpflichtung* (lit g): Dem Verantwortlichen kommt ein Wahlrecht zu. Eine Löschungsverpflichtung gilt allerdings nur dann, wenn nicht andere gesetzliche Regelungen (zB Aufbewahrungspflichten) entgegenstehen.
- *Kontrollbefugnisse* (lit h): Der Verantwortliche muss faktisch in der Lage sein, die Einhaltung der Verpflichtungen zu überprüfen, insb durch zB Vor-Ort-Kontrollen, Vorlage eines schlüssigen Datensicherheitskonzepts, Anforderungen von Prüfergebnissen, Informationseinholung mithilfe von Fragebögen, Einschaltung von Sachverständigen. Diese Kontrollrechte werden durch entsprechende Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters flankiert.

7.4. Parallelen zu Art 28 DORA

Nicht nur aus formaler Perspektive sind Art 28 DSGVO und Art 28 DORA ähnlich. Der materielle Gehalt beider Vorschriften ist ähnlich, wobei die für den Finanzsektor geschaffene Regelung zusätzlich ein (Cyber-)Sicherheitspaket enthält, das auf einen universellen Datenraum übertragen werden kann, wie ein demonstrativer, vergleichender Blick auf den Wortlaut der Bestimmungen samt Regelungsgehalt enthüllt:

Art 28 DSGVO	Art 28–30 DORA	Regelungsgehalt (Stichwort)
Regelung der Verarbeitung von personenbezogenen Daten im Auftrag	Sicherstellungen der operativen Resilienz von Finanzunternehmen, die IKT-Dienstleister einsetzen	Zweck
Gilt für alle datenschutzrechtlich Verantwortlichen, die Auftragsverarbeiter einsetzen	Gilt für alle Finanzunternehmen, die für die Ausübung ihrer Geschäftstätigkeit, IKT-Drittanbieter nutzen	Anwendungsbereich
Verpflichtende schriftliche Vereinbarungen zwischen dem datenschutzrechtlichen Verantwortlichen und dem eingesetzten Auftragsverarbeiter	Vertragliche Vereinbarungen sind nur mit IKT-Drittdienstleistern zu schließen, die angemessene Standards für Informationssicherheit einhalten können	Vertragliche Vereinbarungen
Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zu ergreifen	IKT-Dienstleister muss angemessene Sicherheitsmaßnahmen gewährleisten und implementieren	Sicherheitsmaßnahmen
Unterstützung und Zusammenarbeit	Duldungs- und Nachweispflichten des IKT-Dienstleisters	Überwachung und Kontrolle
Umfassende Unterstützungspflicht	Meldepflicht	Information bei IKT-Vorfall
Aufsichts- bzw Datenschutzbehörde ist Anlaufstelle	Enge Zusammenarbeit mit der Aufsichtsbehörde durch Führung eines Informationsregisters und jährliche Berichterstattung	Behörden

49 Vgl *Pachinger*, Datenschutzverträge[3] (2024) 63 f.
50 Vgl *Jahnel* in Jahnel (Hrsg), Kommentar zur DSGVO (2021) Art 28 Rz 8.
51 Ausf zum Vertragsinhalt nach Art 28 Abs 3 *Jahnel*, DSGVO Art 28 Rz 14 ff; *Pachinger*, Datenschutzverträge[3], 83 ff.

Als *Zwischenergebnis* lässt sich festhalten, dass Datenschutzverantwortliche nach Art 28 DSGVO sicherzustellen haben, dass

- eine kontinuierliche Überwachung externer Dienstleister stattfindet,
- vertragliche Lösch- und Sicherheitsstandards genau geprüft und eingehalten werden sowie
- auch nach Beendigung des Vertrags die Löschung/Rückgabe der Daten dokumentiert ist.

Die bisherige Rsp[52] verdeutlicht, dass die Haftung ausweislich von Art 28 Abs 3 DSGVO nicht einfach auf den Auftragsverarbeiter abgewälzt werden kann, und betont die Wichtigkeit einer strikten Überwachung iSd effektiven Kontrolle von IKT-Dienstleistern.

8. Praktische Umsetzung im Finanzsektor und in anderen Datenräumen

Basierend auf den Anforderungen von Art 28–30 DORA und den Erwägungsgründen sollten Finanzunternehmen die folgenden Maßnahmen ergreifen:

- *Erstellung eines umfassenden Informationsregisters*: Dieses sollte sowohl vertragliche als auch technische Details enthalten, einschließlich der Standorte, an denen Daten verarbeitet werden.
- *Etablierung von Ausstiegsstrategien*: Datenschutzkonforme Verfahren zur Datenmigration und Datenlöschung sollten Bestandteil dieser Strategien sein.
- *Standardisierung von Vertragsklauseln*: Die Verwendung von standardisierten Klauseln, die sowohl DORA- als auch DSGVO-Anforderungen berücksichtigen, kann Rechts- und Planungssicherheit bieten.
- *Risikobasierte Auswahl von Dienstleistern*: Finanzunternehmen sollten systematisch prüfen, ob IKT-Dienstleister höchsten Datenschutz- und Sicherheitsstandards genügen.
- *Identifikation und Segmentierung der IKT-Dienstleister*: Zu bestimmen sind die IKT-Dienstleister sowie ihre Leistungsverträge aus historisch unterschiedlichen Quellen. Die Unterstützung kritischer oder wichtiger Funktionen ist ein entscheidendes Merkmal für die Intensität der zukünftigen Steuerung von Dienstleistern.
- *Nachweis des IKT-Dienstleisters über ein eigenes IKT-Risikomanagement*: Dieses ist vom IKT-Dienstleister vorzuweisen, um sich für die Unterstützung kritischer oder wichtiger Funktionen zu qualifizieren, und hat die Erkennung von Risiken sowie geeignete Nachweise für die Wirksamkeit des Risikomanagements zu umfassen.
- *Geeignete vertragliche Regelungen*: Zentrale Aspekte wie Datenschutz, Sicherheitsanforderungen sowie Haftungsfragen sind zu regeln. Anpassungen bestehender Verträge können erforderlich sein. Klauseln im Vertrag zu Vertragsänderungen, Nachverhandlungen oder zur Kündigung bei Nichteinhaltung können verankert werden.
- *Assurance, Reporting und Evidenzmittel (zB Zertifikate)*: Sicherstellung der Sicherheit, Zuverlässigkeit und Compliance von IKT-Dienstleistern, insb durch Audits, Zertifizierungen, regelmäßige Überprüfung der erforderlichen Anforderungen sowie durch die Berichterstattung durch den IKT-Dienstleister an den Verantwortlichen.
- *Einsatz von Sub-Dienstleistern und deren Steuerung*: Die Überwachung von Sub-Dienstleistern erfordert klare Schritte und Verfahren, um die Risiken zu minimieren und die Überwachung zu gewährleisten.
- *Incident-Meldewesen*: Die Integration von IKT-Dienstleistern im Meldeprozess zu Sicherheitsvorfällen ist erforderlich, um eine Abstimmung der Meldepflichten zu gewährleisten.

9. Synopsis der Anforderungen an ein übergreifendes IKT-Managementsystem durch Mindestvertragsinhalte nach Art 28 DSGVO, Art 25 KI-VO und Art 28–30 DORA

Regelungsthematik	Vertragsklausel(inhalt)	Rechtsgrundlagen		
Vertragsgegenstand	Definition des Auftragsgegenstandes	Art 28 Abs 3 Satz 1 DSGVO	Art 25 Abs 4 iVm Art 6 KI-VO	Art 28 Abs 5, Art 30 Abs 1 DORA
Beschreibung der IKT-Dienstleistung	Gegenstand und Umfang der Beauftragung	Art 28 Abs 3 DSGVO	Art 25 Abs 4 iVm Art 13 KI-VO	Art 30 Abs 2 lit a, lit e, Art 30 Abs 3 lit a DORA
Standort	Ort der Verarbeitung	Art 28 Abs 3 DSGVO	Art 25 Abs 4 iVm Art 2 Abs 7 KI-VO	Art 30 Abs 2 lit b DORA
Überwachung	Weisungs- und Überwachungsbefugnisse des Auftraggebers samt Dokumentationen	Art 28 Abs 3 Satz 2 lit a DSGVO	Art 25 Abs 4 iVm 12, 17–19 KI-VO, Art 26 Abs 5 KI-VO	Art 28 Abs 3, Art 30 Abs 1 lit a DORA

52 EuGH 5. 12. 2023, C-683/21 (Nacionalinis visuomenes sveikatos centras-Fall), ECLI:EU:C:2023:949 = jusIT 2024/20, 33 (Kröpfl): COVID-App; OLG Linz 12. 6. 2019, 6 R 49/19x (Haartransplantation), ZIIR 2020, 404 (*Thiele*).

Regelungsthematik	Vertragsklausel(inhalt)	Rechtsgrundlagen		
Verantwortlichkeiten	Rechtsstellung des Auftraggebers	Art 28 Abs 1 iVm Art 4 Z 7 DSGVO	Art 25 Abs 4 Satz 1 iVm Art 8, 16 KI-VO	Art 28 Abs 1 lit a, Art 30 Abs 1 DORA
Vertraulichkeit	Anforderung an Personal und System	Art 28 Abs 3 Satz 2 lit b iVm Art 32 und 25 DSGVO	Art 25 Abs 4 iVm Art 4, 14, 15 KI-VO	Art 30 Abs 2 lit c, Art 30 Abs 3 lit i DORA
Sicherheit	Maßnahmen zur Sicherheit	Art 28 Abs 3 Satz 2 lit c DSGVO	Art 25 Abs 4 iVm Art 13, 15 KI-VO	Art 30 Abs 3 lit c DORA
Unterauftragsvergabe	Inanspruchnahme weiterer Auftragsverarbeiter und die Bedingungen	Art 28 Abs 2, Abs 3 Satz 2 lit d und Abs 4 DSGVO	Art 25 Abs 4 iVm Art 2 Abs 7 KI-VO	Art 29 Abs 2, Art 30 Abs 2 lit a DORA
Aufsicht und Berichterstattung	Unterstützungs- und Mitteilungspflichten	Art 28 Abs 3 Satz 2 lit e DSGVO iVm Kapitel III DSGVO, Art 28 Abs 3 Satz 2 lit f DSGVO	Art 25 Abs 4 iVm Art 14, 20, 21 KI-VO	Art 30 Abs 2 lit g, Art 30 Abs 3 lit a, b, d DORA
IKT-Vorfall	Informations- und Unterstützungspflicht bei Datensicherheitsvorfällen	Art 28 Abs 3 Satz 2 lit f DSGVO	Art 25 Abs 4 iVm Art 73 KI-VO	Art 30 Abs 2 lit f DORA
Datenzugriff	Datenlöschung und -rückgabe	Art 28 Abs 3 Satz 2 lit g DSGVO	Art 25 Abs 4 iVm Art 10, 18, 21 KI-VO	Art 28 Abs 8, Art 30 Abs 2 lit d DORA
Prüfrechte	Nachweise und Überprüfungen	Art 28 Abs 3 Satz 2 lit h DSGVO	Art 25 Abs 4 iVm Art 9, 43 KI-VO	Art 28 Abs 6, Art 30 Abs 3 lit e DORA
Kündigung	Vertragsdauer und besondere Beendigungsregeln	Art 28 Abs 3 Satz 1 DSGVO	keine explizite	Art 28 Abs 7, 8, Art 30 Abs 2 lit h, Art 30 Abs 3 lit b, lit f DORA
Sonstige Regelungen	Haftung und Vertragsstrafe	Art 28 DSGVO iVm Art 82, 83 DSGVO	Art 25 Abs 4 iVm Art 99, 100 KI-VO	Art 30 iVm Art 51 DORA

10. Zusammenfassung

Art 28–30 DORA bieten einen umfassenden Rahmen für das Management von IKT-Drittparteienrisiken. Datenschutzbeauftragte im Finanzsektor spielen eine zentrale Rolle bei der Sicherstellung der datenschutzrechtlichen Konformität und der Stärkung der digitalen Resilienz. Der Aufbau eines IKT-Managementsystems hat zunächst bei Art 28 DSGVO anzusetzen und gegebenenfalls die Verpflichtungen für Anbieter von KI-Systemen nach Art 25 Abs 4 KI-VO zu beachten, um schließlich den notwendigen Datenschutz mit der erforderlichen Informationssicherheit gemäß den Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos nach Kapitel V Abschnitt I DORA zu verschränken. Die dort enthaltenen Art 28–30 DORA bergen vorbildhafte Handlungsanweisungen, um IKT-Risiken im Finanzsektor zu minimieren. Die detaillierten Anforderungen fördern eine nachhaltige digitale Resilienz und schaffen klare Verantwortlichkeiten zwischen Finanzunternehmen und IKT-Dienstleistern. Ein tiefes Verständnis der Normen und Begriffe ist unabdingbar, um eine rechtskonforme und praxisgerechte Umsetzung sicherzustellen, kann aber auch dazu genützt werden, eine optimale Umsetzung der in anderen Sektoren maßgeblichen NIS-2-RL zu befördern. Durch die Kombination von rechtlicher Präzision und technischen Schutzmaßnahmen kann eine effektive Umsetzung bewirkt werden.

Annex: Mustervertrag

Mustervertrag für die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen

abgeschlossen zwischen

[Name des Finanzunternehmens], mit Sitz in [Adresse], vertreten durch [Name, Position], im Folgenden „*Auftraggeber*" genannt, und **[Name des IKT-Dienstleisters]**, mit Sitz in [Adresse], vertreten durch [Name, Position], im Folgenden „*Dienstleister*" genannt.

Präambel

Dieser Vertrag regelt die Bereitstellung von IKT-Dienstleistungen durch den Dienstleister im Einklang mit den Anforderungen der Verordnung (EU) 2022/2554 (DORA) und Art 28 DSGVO sowie weiteren anwendbaren Gesetzen. Ziel ist es, die digitale operationale Resilienz des Auftraggebers und den Schutz personenbezogener Daten sicherzustellen.

1. Vertragsgegenstand

1.1. Der Dienstleister stellt IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bereit, wie in **Anlage 1 (Leistungsbeschreibung)** detailliert aufgeführt.

1.2. Der Dienstleister übernimmt folgende Aufgaben:

- Bereitstellung, Wartung und Betrieb der beschriebenen Dienste;
- Sicherstellung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der verarbeiteten Daten;

- Gewährleistung der Einhaltung datenschutzrechtlicher Anforderungen gemäß DSGVO.

1.3. Der Dienstleister bestätigt, dass die Dienste mit den Anforderungen des Auftraggebers und den höchsten Standards für Informationssicherheit kompatibel sind.

2. Unterauftragsvergabe

2.1. Die Vergabe von Unteraufträgen ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig.

2.2. Bei genehmigter Unterauftragsvergabe gelten für den Unterauftragnehmer dieselben datenschutzrechtlichen und sicherheitstechnischen Verpflichtungen wie für den Dienstleister.

2.3. Der Dienstleister verpflichtet sich, eine Liste aller genehmigten Unterauftragsverhältnisse zu führen und dem Auftraggeber auf Anfrage bereitzustellen.

2.4. Wird ein Unterauftragnehmer in einem Drittland tätig, stellt der Dienstleister sicher, dass die Anforderungen gemäß Art. 44 ff. DSGVO (Datenübermittlung in Drittländer) eingehalten werden.

3. Datenschutz und Datensicherheit

3.1. Der Dienstleister verarbeitet personenbezogene Daten ausschließlich im Auftrag des Auftraggebers und gemäß dessen dokumentierten Weisungen (Art 28 Abs 3 lit a DSGVO).

3.2. Der Dienstleister verpflichtet sich zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art 32 DSGVO).

3.3. Der Dienstleister stellt sicher, dass alle mit der Datenverarbeitung beauftragten Personen vertraglich zur Vertraulichkeit verpflichtet sind (Art 28 Abs 3 lit b DSGVO).

3.4. Der Dienstleister unterstützt den Auftraggeber bei der Erfüllung der Pflichten gemäß Art 32 bis 36 DSGVO, insbesondere bei:

- Sicherstellung der Datensicherheit;
- Meldung von Datenschutzverletzungen (Art 33 und 34 DSGVO);
- Durchführung von Datenschutz-Folgenabschätzungen (Art 35 DSGVO).

3.5. Nach Beendigung des Vertrags hat der Dienstleister alle personenbezogenen Daten nach Wahl des Auftraggebers entweder sicher zu löschen oder zurückzugeben und dies schriftlich zu bestätigen (Art 28 Abs 3 lit g DSGVO).

4. Standorte der Datenverarbeitung

4.1. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich an den in **Anlage 2 (Standorte der Datenverarbeitung)** genannten Orten.

4.2. Der Dienstleister informiert den Auftraggeber schriftlich und rechtzeitig über geplante Änderungen dieser Standorte und holt dessen vorherige Zustimmung ein.

5. Zugriffs- und Überwachungsrechte

5.1. Der Auftraggeber und gegebenenfalls zuständige Behörden haben das uneingeschränkte Recht, die Einhaltung der vertraglichen und gesetzlichen Verpflichtungen durch Inspektionen und Audits zu überprüfen.

5.2. Der Dienstleister gewährt Zugang zu allen relevanten Informationen und Räumlichkeiten.

5.3. Audits erfolgen nach vorheriger Ankündigung, es sei denn, es liegt ein dringender Grund vor. Die Kosten für Audits trägt der Auftraggeber, es sei denn, es werden erhebliche Verstöße festgestellt.

6. Verfügbarkeit und Dienstleistungsgüte

6.1. Der Dienstleister verpflichtet sich, die vereinbarten Dienstleistungen gemäß den in **Anlage 3 (Service Level Agreements, SLAs)** festgelegten Qualitätsparametern bereitzustellen.

6.2. Werden die vereinbarten SLAs nicht eingehalten, ergreift der Dienstleister unverzüglich angemessene Maßnahmen und informiert den Auftraggeber.

6.3. Bei wiederholten SLA-Verstößen hat der Auftraggeber das Recht, den Vertrag außerordentlich zu kündigen.

7. Notfall- und Ausstiegsstrategien

7.1. Der Dienstleister entwickelt und dokumentiert Notfallpläne zur Sicherstellung der Kontinuität kritischer Dienstleistungen. Diese Pläne sind regelmäßig zu testen und zu aktualisieren.

7.2. Der Dienstleister unterstützt den Auftraggeber bei der sicheren Migration von Daten und Dienstleistungen im Falle einer Vertragsbeendigung.

7.3. Die Datenmigration erfolgt in einem standardisierten, maschinenlesbaren Format gemäß **Anlage 4 (Datenmigration und -wiederherstellung)**.

8. Meldepflichten

8.1. Der Dienstleister informiert den Auftraggeber unverzüglich über:

- Sicherheitsvorfälle, die die bereitgestellten Dienstleistungen betreffen;
- Änderungen, die die Erbringung der Dienstleistungen wesentlich beeinträchtigen könnten.

8.2. Bei Datenschutzverletzungen erfolgt die Meldung gemäß den Vorgaben des Auftraggebers innerhalb von 24 Stunden.

9. Haftung

9.1. Der Dienstleister haftet für Verstöße gegen Datenschutz- und Sicherheitsanforderungen gemäß den Bestimmungen dieses Vertrags und geltendem Recht.

9.2. Die Haftung des Dienstleisters erstreckt sich auch auf Schäden, die durch Unterauftragnehmer verursacht werden.

10. Vertragsdauer und Kündigung

10.1. Dieser Vertrag tritt mit Unterzeichnung in Kraft und gilt für die Dauer von [Zeitraum].

10.2. Der Vertrag kann vom Auftraggeber außerordentlich gekündigt werden, wenn:

- der Dienstleister wesentliche Pflichten verletzt,
- wiederholte SLA-Verstöße auftreten,
- datenschutzrechtliche Bestimmungen nicht eingehalten werden.

10.3. Eine ordentliche Kündigung ist mit einer Frist von [Zeitraum] zum Monatsende möglich.

11. Schlussbestimmungen

11.1. Es gilt das Recht der Europäischen Union, insbesondere die Verordnung (EU) 2022/2554 und die DSGVO.

11.2. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.

11.3. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Regelungen unberührt.

Ort, Datum:

Für den Auftraggeber:	**Für den Dienstleister:**
_____	_____
[Unterschrift]	[Unterschrift]
[Name, Position]	[Name, Position]

Anlagen

- **Anlage 1:** Leistungsbeschreibung
- **Anlage 2:** Standorte der Datenverarbeitung
- **Anlage 3:** Service Level Agreements (SLAs)
- **Anlage 4:** Datenmigration und -wiederherstellung

Foto: Wass

Der Autor:

RA Hon.-Prof. Dr. **Clemens Thiele**, LL.M. Tax (GGU) Fulbright Stipendiat für US-Steuerrecht; Anwaltliche Tätigkeit in Deutschland und den USA; Gründer der Kanzlei EUROLAWYER®; Honorarprofessor der Universität Salzburg; Autor und Herausgeber von Publikationen zum IP/IT-Recht; gerichtlich beeideter Sachverständiger für Urheberfragen aller Art.

lesen.lexisnexis.at/autor/Thiele/Clemens

Foto: privat

Die Autorin:

Mag.[a] iur. **Jessica Wagner** ist Absolventin der rechtswissenschaftlichen Fakultät der Universität Salzburg. Sie ist seit Oktober 2017 Mitglied des EUROLAWYER® Datenschutzteams als Data Fieldwork Expertin in zahlreichen Datenschutz-Audits von Einrichtungen des öffentlichen Bereichs sowie in mittleren und großen Unternehmen. Verfasserin von diversen Buch- und Fachzeitschriftenbeiträgen zum Datenschutzrecht. Mitherausgeberin und Co-Autorin des Praxiskommentar zum Österreichischen Datenschutzgesetz (2022).

lesen.lexisnexis.at/autor/Wagner/Jessica

GESETZGEBUNGSMONITOR

RA Hon.-Prof. Dr. Clemens Thiele, LL.M. Tax (GGU) • Salzburg

Gesetzgebungsmonitor Rechtsinformation: Änderung des Gerichtsorganisationsgesetzes bringt allgemeine Veröffentlichungspflicht von OLG-Entscheidungen

» jusIT 2025/3

Dieser Kurzbeitrag gibt einen Überblick über die Änderung des Gerichtsorganisationsgesetzes durch das Strafprozessrechtsänderungsgesetz 2024,[1] soweit darin eine allgemeine Veröffentlichungspflicht der rechtskräftigen Entscheidungen der Oberlandesgerichte iS eines verbesserten Zugangs zum Recht verankert und einem bisherigen praktischen Defizit in der Rechtsinformation abgeholfen worden ist.

1 Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz, das Gerichtsorganisationsgesetz, das Finanzstrafgesetz, das Justizbetreuungsagentur-Gesetz, das Allgemeine Verwaltungsverfahrensgesetz 1991 und das Jugendgerichtsgesetz 1988 geändert werden, BGBl I 157/2024.