LEITFADEN DECKBLATT

GEGENSTAND

DORA-Exit für Archivsoftware

INHALT

Was DORA von Versicherern für Archiv- und Konvertierungssoftware im eigenen Haus verlangt, wo die Vorgaben offen sind und wie sich ein Ausstieg vorbereiten lässt.

STAND

Quellen gelesen am 16.11.2026

QUELLE

Verordnung (EU) 2022/2554 (DORA) und Rechtsakte der Kommission, EIOPA, EBA, BaFin; 10 Quellen, Register 8

UMFANG

24 Seiten · 8 Register

HERAUSGEBER

Doconform

VERFASSER

Florian Albers

REGISTER

1. Auf einen Blick
2. Worum es geht
3. Vorgabe und Praxis
4. Prüfliste
5. Fehlerquellen
6. Doconform
7. Häufige Fragen
8. Quellen

Zitate in „…“ mit Fundstelle · eigene Auslegung als „Unsere Lesart“ gekennzeichnet

QUELLEN GEPRÜFT
16.11.2026

1 Auf einen Blick

FÜNF PUNKTE

KURZFASSUNG

1. DORA gilt seit dem 17. Januar 2025, auch für Versicherungs- und Rückversicherungsunternehmen. [DORA, Art. 2 Abs. 1 Buchst. n, Art. 64]
2. Das Informationsregister erfasst alle vertraglichen Vereinbarungen über IKT-Dienstleistungen von IKT-Drittdienstleistern, auch solche, die keine Auslagerung sind. [DORA, Art. 28 Abs. 3]
3. Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, brauchen Sie Ausstiegsstrategien und getestete Ausstiegspläne. [DORA, Art. 28 Abs. 8; RTS-Leitlinie, Art. 10]
4. Ob eine Lizenz für selbst betriebene Software eine IKT-Dienstleistung ist, hat die Aufsicht nicht ausdrücklich beantwortet. Die Registervorlage kennt die Art „Softwarelizenzierung (ohne SaaS)“. [ITS-Register, Anhang III]
5. Für den Ausstieg zählen die Daten: Sie müssen sich vollständig übertragen oder ins eigene Haus zurückholen lassen. [DORA, Art. 28 Abs. 8 UAbs. 4; Art. 30 Abs. 2 Buchst. d]

2 Worum es geht

DORA ART. 2, 4, 64 · BAFIN-FAQ

DIE VERORDNUNG

Die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor, kurz DORA, regelt unter anderem, wie Finanzunternehmen mit dem Risiko aus IKT-Dienstleistungen Dritter umgehen. Das steht in Kapitel V, Artikel 28 bis 30. Zwei Rechtsakte der Kommission ergänzen diese Artikel: die Durchführungsverordnung (EU) 2024/2956 mit den Vorlagen für das Informationsregister und die Delegierte Verordnung (EU) 2024/1773 zur Leitlinie für vertragliche Vereinbarungen über

IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen.

DORA gilt unter anderem für „Versicherungs- und Rückversicherungsunternehmen“ [DORA, Art. 2 Abs. 1 Buchst. n]. Nicht erfasst sind Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG (das sind die kleinen Unternehmen, für die Solvabilität II nicht gilt) [DORA, Art. 2 Abs. 3 Buchst. b]. Die Verordnung „gilt ab dem 17. Januar 2025“ [DORA, Art. 64]. Alle Pflichten sind nach dem Grundsatz der Verhältnismäßigkeit anzuwenden, also nach Größe, Risikoprofil und Art der Geschäfte [DORA, Art. 4 Abs. 1; Art. 28 Abs. 1 Buchst. b].

WEN SIE TRIFFT

Die Pflichten treffen das Finanzunternehmen. Die BaFin schreibt dazu: „Die Regelungen der DORA-Verordnung gelten nur für Finanzunternehmen. Die Regelungen betreffen die IKT-Drittdienstleister indirekt, da die Finanzunternehmen bei der Vertragsgestaltung bestimmte Anforderungen berücksichtigen müssen.“ [BaFin-FAQ]

UNSERE LESART

Auslegung von Doconform, kein Text von DORA oder der Aufsicht

Für Archiv- und Konvertierungssoftware im eigenen Rechenzentrum stellen sich drei Fragen. Gehört der Vertrag ins Informationsregister? Unterstützt die Software eine kritische oder wichtige Funktion? Und wenn ja: Wie kommen Sie heraus, ohne dass Archiv und Daten am Hersteller hängen? Dieser Leitfaden geht die Fragen der Reihe nach durch.

Dieser Abschnitt ist keine Rechtsberatung.

3 Was DORA verlangt

LINKS ZITAT, RECHTS UNSERE UMSETZUNG

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Software im eigenen Haus ist ein IKT-Asset	Unabhängig von jedem Vertrag ist selbst betriebene Software ein „IKT-Asset“, also „eine Software oder Hardware in den Netzwerk- und Informationssystemen, die das Finanzunternehmen nutzt“ [DORA, Art. 3 Nr. 7]. Finanzunternehmen ermitteln und klassifizieren „alle IKT-gestützten Unternehmensfunktionen“ und „die Informations- und IKT-Assets, die diese Funktionen unterstützen“ [DORA, Art. 8 Abs. 1]. Zu jedem IKT-Asset gehört in die Aufzeichnungen unter anderem die unterstützte Unternehmensfunktion und gegebenenfalls die Frist, nach der es „nicht mehr von ihrem Anbieter oder einem IKT-Drittdienstleister unterstützt“ wird [RTS-RMF, Art. 4 Abs. 2 Buchst. b Ziff. v und ix]. Software, die ihr Anbieter nicht mehr unterstützt, die aber weiter genutzt wird, ist ein „IKT-Altsystem“ [DORA, Art. 3 Nr. 3]. Für Altsysteme verlangt DORA mindestens jährlich eine eigene Risikobewertung [DORA, Art. 8 Abs. 7]. **Unsere Lesart:** Das Inventar ist die erste Stelle, an der Archivsoftware auftaucht. Hier gehört auch das Ende der Pflege jeder eingesetzten Version hin. Läuft die Pflege aus, ohne dass ein Update eingespielt ist, wird aus dem Asset ein Altsystem.	SCHRITT 1 **Software ins Inventar aufnehmen.** Jede eingesetzte Version mit unterstützter Funktion, Standort und Ende der Pflege erfassen. Läuft die Pflege aus, die Software als Altsystem bewerten.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Ist die Lizenz eine IKT-Dienstleistung?	DORA definiert IKT-Dienstleistungen als „digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört“ [DORA, Art. 3 Nr. 21]. Die Definition soll „weit ausgelegt werden“ [DORA, ErwG 35]. Die Verordnung soll für ein breites Spektrum von Anbietern gelten, „darunter Anbieter von Cloud-Computing-Diensten, Software, Datenanalysediensten und Anbieter von Rechenzentrumsdienstleistungen“ [DORA, ErwG 63]. Die Vorlage für das Informationsregister führt unter den Arten von IKT-Dienstleistungen „Softwarelizenzierung (ohne SaaS)“ mit der Beschreibung „Bereitstellung von lokal ausgeführter Software.“ [ITS-Register, Anhang III, S13]. Daneben steht „IKT-Betriebsmanagement (einschließlich Wartung)“ [ITS-Register, Anhang III, S14]. EIOPA hat zu Wiederverkäufern geantwortet: „If a reseller only supplies licenses without providing ICT services on an ongoing basis“, ist er kein IKT-Drittdienstleister im Sinne von Art. 3 Nr. 21 [EIOPA-Q&A 3300]. Zwei Fragen, die genau die Lizenz für selbst betriebene	SCHRITT 2 **Vertrag einordnen.** Prüfen, ob zur Lizenz fortlaufende Leistungen gehören (Updates, Sicherheitsfixes, Support). Wenn ja, den Vertrag ins Informationsregister aufnehmen, mit Art S13 und gegebenenfalls S14. Die Einordnung begründen.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
	Software betrafen, wurden abgelehnt, mit Verweis auf eine allgemeine Antwort der Kommission zu Art. 3 Nr. 21 [EBA-Q&A 7046; EIOPA-Q&A 3622; EIOPA-Q&A 2999]. Nach dieser Antwort müssen die Finanzunternehmen selbst beurteilen, ob die Dienste, auf die sie sich stützen, IKT-Dienstleistungen sind. **Unsere Lesart:** Eine einmal gekaufte Lizenz ohne weitere Leistung ist nach der EIOPA-Antwort eher keine IKT-Dienstleistung. Bei Archiv- und Konvertierungssoftware ist das selten der Fall: Zur Lizenz gehören meist Updates, Sicherheitsfixes und Support für die Laufzeit. Das ist eine fortlaufende Leistung. Wir empfehlen, solche Verträge ins Register aufzunehmen, mit der Art S13 und gegebenenfalls S14, und die Einordnung zu begründen.	

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Kritische oder wichtige Funktion	Kritisch oder wichtig ist eine Funktion, „deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde“ oder deren gestörte Leistung „die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde“ [DORA, Art. 3 Nr. 22]. Die BaFin stellt klar, dass es dabei nicht allein um Verfügbarkeit geht: „Eine Funktion kann zum Beispiel auch unter dem Aspekt der Vertraulichkeit kritisch oder wichtig sein.“ [BaFin-FAQ] Die Bewertung trifft das Finanzunternehmen selbst. Im Register steht sie je Funktion mit Gründen, Datum der letzten Bewertung und Vorgaben für Wiederherstellungszeit und -punkt [ITS-Register, Vorlage B_06.01]. **Unsere Lesart:** Die Software selbst ist keine Funktion. Bewertet wird die Funktion, die sie stützt, etwa die Ablage der Schadenkorrespondenz oder die Aufbewahrung von Vertragsunterlagen. Ob das in Ihrem Haus kritisch oder wichtig ist, hängt davon ab, was ein Ausfall für Schadenbearbeitung, Nachweis-	SCHRITT 3 **Funktion bewerten.** Die Funktion benennen, die die Software stützt, und festhalten, ob sie kritisch oder wichtig ist, mit Gründen, Datum und Wiederherstellungsvorgaben. Vertraulichkeit und Integrität mitbedenken, nicht nur Verfügbarkeit.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
	und Aufbewahrungspflichten bedeutet. Halten Sie die Begründung fest, auch wenn das Ergebnis „nicht kritisch“ lautet.	

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Das Informationsregister	Finanzunternehmen führen „ein Informationsregister, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen bezieht“ [DORA, Art. 28 Abs. 3 UAbs. 1]. Dabei wird unterschieden zwischen Vereinbarungen, die kritische oder wichtige Funktionen unterstützen, und anderen [DORA, Art. 28 Abs. 3 UAbs. 2]. Über jede geplante Vereinbarung zur Unterstützung kritischer oder wichtiger Funktionen ist die Aufsicht „zeitnah“ zu unterrichten, ebenso wenn eine Funktion kritisch oder wichtig geworden ist [DORA, Art. 28 Abs. 3 UAbs. 5]. Die Vorlagen legt die Durchführungsverordnung (EU) 2024/2956 fest. Jeder IKT-Drittdienstleister, der eine juristische Person ist, wird mit einer LEI oder einer EUID identifiziert [ITS-Register, Art. 3 Abs. 5]. Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, fragt die Vorlage B_07.01 unter anderem nach der Substituierbarkeit des Anbieters, dem „Vorliegen eines Ausstiegsplans“ und der „Möglichkeit der Wiedereingliederung der vertraglich vereinbarten IKT-Dienstleistung“ [ITS-Register, B_07.01.0050, 0080, 0090]. Bei der BaFin reichen Sie das Register jährlich über die Meldeplattform MVP ein. Die BaFin bittet, „bis spätestens zum 31. März den	SCHRITT 2 **Vertrag einordnen.** Prüfen, ob zur Lizenz fortlaufende Leistungen gehören (Updates, Sicherheitsfixes, Support). Wenn ja, den Vertrag ins Informationsregister aufnehmen, mit Art S13 und gegebenenfalls S14. Die Einordnung begründen. SCHRITT 4 **Register vollständig führen.** LEI oder EUID des Herstellers einholen, Kündigungsfristen, Substituierbarkeit und Ausstiegsplan eintragen. Jährlich bis 31. März über die MVP einreichen, geplante Verträge für kritische oder wichtige Funktionen zeitnah anzeigen.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
	Einreichungsprozess vollständig und fehlerfrei zu durchlaufen“. Das Register gibt den Stand zum 31. Dezember des Vorjahres wieder [BaFin-Register]. Eine Dummy-LEI akzeptiert die BaFin nicht [BaFin-FAQ]. **Unsere Lesart:** Die Felder in B_07.01 sind die Fragen, die Ihr Exit-Plan beantworten muss. Wer „Ausstiegsplan: Ja“ meldet, sollte ihn vorlegen können.	

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Vor Vertragsschluss	Vor Abschluss einer Vereinbarung über IKT-Dienstleistungen müssen Finanzunternehmen unter anderem beurteilen, ob sie eine kritische oder wichtige Funktion unterstützt, alle relevanten Risiken bewerten, „einschließlich der Möglichkeit, dass diese vertragliche Vereinbarung dazu beitragen kann, das in Artikel 29 genannte IKT-Konzentrationsrisiko zu erhöhen“, und die Eignung des Anbieters prüfen [DORA, Art. 28 Abs. 4]. Für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen ist zu berücksichtigen, ob der Vertrag zu „Verträge[n] mit einem IKT-Drittdienstleister, der nicht ohne Weiteres ersetzbar ist“ führen würde [DORA, Art. 29 Abs. 1 Buchst. a]. Dazu gehört ein Blick auf das Insolvenzrecht und auf „jede Einschränkung, die sich im Zusammenhang mit der dringenden Wiederherstellung der Daten des Finanzunternehmens ergeben könnte“ [DORA, Art. 29 Abs. 2 UAbs. 2]. Die Leitlinie nach RTS verlangt eine Risikobewertung vor Vertragsschluss, die unter anderem „Risiken im Zusammenhang mit der Verfügbarkeit von Daten“ und „IKT-Konzentrationsrisiken auf Unternehmensebene“ abdeckt [RTS-Leitlinie, Art. 5 Abs. 2], und eine Sorgfaltsprüfung des Anbieters, etwa seiner Ressourcen und Informationssicherheitsstandards [RTS-Leitlinie, Art. 6 Abs. 1].	SCHRITT 5 **Vor dem Kauf prüfen.** Risiken bewerten, Konzentration und Ersetzbarkeit einschätzen, die Eignung des Herstellers prüfen, auch Insolvenzrecht und Zugang zu Daten.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
	Unsere Lesart: Für Software, die Sie selbst betreiben, verschiebt sich die Frage. Ersetzbar sein muss weniger der laufende Betrieb, der ohnehin bei Ihnen liegt, als Pflege, Updates und der Zugang zu Ihren Daten. Prüfen Sie deshalb, ob die Software ohne den Hersteller weiterläuft und ob Ihre Daten in offenen Formaten vorliegen.	

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Der Vertrag	Jeder Vertrag über IKT-Dienstleistungen muss Mindestinhalte haben [DORA, Art. 30 Abs. 2]. Für die Archivfrage am wichtigsten sind „Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format“ [DORA, Art. 30 Abs. 2 Buchst. d], die Beschreibung der Dienstleistungsgüte „einschließlich Aktualisierungen und Überarbeitungen“ [DORA, Art. 30 Abs. 2 Buchst. e] sowie Kündigungsrechte und Mindestkündigungsfristen [DORA, Art. 30 Abs. 2 Buchst. h]. Unterstützt die Dienstleistung eine kritische oder wichtige Funktion, kommen weitere Inhalte hinzu, darunter Zugangs-, Inspektions- und Auditrechte [DORA, Art. 30 Abs. 3 Buchst. e] und „Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums“, in dem der Anbieter weiter leistet und der den Wechsel zu einem anderen Anbieter oder auf interne Lösungen ermöglicht [DORA, Art. 30 Abs. 3 Buchst. f]. Der	SCHRITT 6 **Vertrag nachziehen.** Die Mindestinhalte nach Art. 30 Abs. 2 abbilden, bei kritischen oder wichtigen Funktionen auch Abs. 3, vor allem Übergangszeitraum, Audit- und Kündigungsrechte.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
	Vertrag ist schriftlich oder in einem herunterladbaren, dauerhaften und zugänglichen Format zu dokumentieren [DORA, Art. 30 Abs. 1]. **Unsere Lesart:** Viele Lizenz- und Pflegeverträge stammen aus der Zeit vor DORA. Ein Vertragsanhang, der die Punkte aus Art. 30 einzeln abbildet, ist der übliche Weg, sie nachzuziehen. Bei selbst betriebener Software sind einige Punkte schnell beantwortet, etwa der Standort der Datenverarbeitung, der in Ihrem Rechenzentrum liegt. Andere bleiben wichtig, vor allem Übergangszeitraum, Pflegedauer und Zugang zum Quellcode im Insolvenzfall.	

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Die Ausstiegsstrategie	„Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, richten Finanzunternehmen Ausstiegsstrategien ein.“ [DORA, Art. 28 Abs. 8 UAbs. 1] Finanzunternehmen müssen aus Verträgen ausscheiden können, ohne „Unterbrechung ihrer Geschäftstätigkeit“, ohne „Einschränkung der Einhaltung regulatorischer Anforderungen“ und ohne „Beeinträchtigung der Kontinuität und Qualität ihrer für Kunden erbrachten Dienstleistungen“ [DORA, Art. 28 Abs. 8 UAbs. 2]. „Ausstiegspläne müssen umfassend, dokumentiert und im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien ausreichend getestet sein sowie regelmäßig überprüft werden.“ [DORA, Art. 28 Abs. 8 UAbs. 3] Finanzunternehmen entwickeln Übergangspläne, um „die relevanten Daten“ dem Anbieter zu entziehen und „sie sicher und vollständig alternativen Anbietern zu übertragen oder wieder in die eigenen Systeme zu überführen“ [DORA, Art. 28 Abs. 8 UAbs. 4]. Die RTS-Leitlinie verlangt einen dokumentierten Ausstiegsplan „für jede vertragliche Vereinbarung“ im Sinne der Leitlinie, also über IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen. Er berücksichtigt unvorhergesehene Unterbrechungen, mangelhafte Leistung und „eine unerwartete Beendigung vertraglicher Vereinba-	SCHRITT 7 **Exit-Plan schreiben.** Szenarien: Ausfall des Herstellers, schlechte oder ausbleibende Pflege, unerwartete Kündigung. Je Szenario: was weiterläuft, Ersatzlösung, Zeitplan, Zuständige. SCHRITT 8 **Lesbarkeit ohne die Software sicherstellen.** Archivierte Dokumente in einem offenen, genormten Format ablegen, etwa PDF/A, mit Original und Konvertierungsnachweis daneben. SCHRITT 9 **Exit testen.** Den Plan durchspielen, etwa mit einer Ersatzlösung auf einer Stichprobe, und das Ergebnis dokumentieren. Den Plan regelmäßig überprüfen.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
	rungen“. Er muss „realistisch und durchführbar sein, auf plausiblen Szenarien und vernünftigen Annahmen beruhen und einen Durchführungszeitplan enthalten“ [RTS-Leitlinie, Art. 10]. Kündigen können müssen Sie unter anderem bei einem erheblichen Rechtsverstoß des Anbieters, bei nachgewiesenen Schwächen in seinem IKT-Risikomanagement oder wenn die Aufsicht das Finanzunternehmen wegen des Vertrags nicht mehr wirksam beaufsichtigen kann [DORA, Art. 28 Abs. 7]. **Unsere Lesart:** Ein Exit-Plan für Archivsoftware beantwortet vier Fragen. Was läuft weiter, wenn der Hersteller ausfällt oder der Vertrag endet? Wie lange trägt die zuletzt gepflegte Version, bevor sie zum Altsystem wird? Womit ersetzen Sie die Software, und wie lange dauert das? Und: Lassen sich die bereits archivierten Dokumente ohne die Software lesen und prüfen? Die letzte Frage entscheidet, ob der Ausstieg das Archiv berührt.	

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
Daten und Formate	DORA verlangt beim Vertrag die Rückgabe von Daten „in einem leicht zugänglichen Format“ [DORA, Art. 30 Abs. 2 Buchst. d] und beim Ausstieg die sichere und vollständige Übertragung der relevanten Daten [DORA, Art. 28 Abs. 8 UAbs. 4]. Als Grund für schwere Ersetzbarkeit nennt die Registervorlage „Schwierigkeiten bei der teilweisen oder vollständigen Migration der einschlägigen Daten und Arbeitslasten“ [ITS-Register, B_07.01.0060]. Dieselben Schwierigkeiten zählt DORA zu den Kriterien, nach denen die Aufsicht IKT-Drittdienstleister als kritisch einstuft [DORA, Art. 31 Abs. 2 Buchst. d Ziff. ii]. **Unsere Lesart:** Für ein Archiv heißt „leicht zugänglich“: Die Dokumente lassen sich ohne die Software lesen, die sie erzeugt hat, und die Belege der Umwandlung lassen sich ohne sie prüfen. PDF/A ist als ISO 19005 genormt und lässt sich mit einem unabhängigen Validator wie veraPDF prüfen. Ein Konvertierungsvermerk in einem offenen Format (etwa JSON mit veröffentlichtem Schema) hält fest, woraus und wie ein Dokument entstanden ist. Liegen Original, PDF/A und Vermerk zusammen in Ihrem Archiv, nimmt ein Wechsel der Konvertierungssoftware dem Archiv nichts weg. Was PDF/A und seine	SCHRITT 8 **Lesbarkeit ohne die Software sicherstellen.** Archivierte Dokumente in einem offenen, genormten Format ablegen, etwa PDF/A, mit Original und Konvertierungsnachweis daneben. SCHRITT 10 **Stichprobe aus dem Archiv prüfen.** Ältere Dokumente unabhängig von der erzeugenden Software öffnen und validieren. Das zeigt, dass Daten tatsächlich „vollständig“ übertragbar sind.

THEMA	DORA UND AUFSICHT (ZITAT)	IN DER PRAXIS · UNSERE LESART
	Stufen leisten, erklärt der Artikel PDF/A-Stufen erklärt.	

4 Prüfliste

ZUM ABHAKEN IM HAUS

UNSERE LESART
Auslegung von Doconform, kein Text von DORA oder der Aufsicht

Die folgende Liste ist unsere Umsetzung der Vorgaben für Archiv- und Konvertierungssoftware, kein Text von DORA oder der Aufsicht. Jeder Schritt nennt die Stelle, auf die er sich stützt. Wie weit Sie gehen, richtet sich nach Verhältnismäßigkeit und nach Ihrer Bewertung der Funktion.

	SCHRITT	STÜTZE
☐ 1	**Software ins Inventar aufnehmen.** Jede eingesetzte Version mit unterstützter Funktion, Standort und Ende der Pflege erfassen. Läuft die Pflege aus, die Software als Altsystem bewerten.	DORA, Art. 8 Abs. 1, 4 und 7; RTS-RMF, Art. 4 Abs. 2 Buchst. b
☐ 2	**Vertrag einordnen.** Prüfen, ob zur Lizenz fortlaufende Leistungen gehören (Updates, Sicherheitsfixes, Support). Wenn ja, den Vertrag ins Informationsregister aufnehmen, mit Art S13 und gegebenenfalls S14. Die Einordnung begründen.	DORA, Art. 3 Nr. 21; ITS-Register, Anhang III; EIOPA-Q&A 3300
☐ 3	**Funktion bewerten.** Die Funktion benennen, die die Software stützt, und festhalten, ob sie kritisch oder wichtig ist, mit Gründen, Datum und Wiederherstellungsvorgaben. Vertraulichkeit und Integrität mitbedenken, nicht nur Verfügbarkeit.	DORA, Art. 3 Nr. 22; ITS-Register, B_06.01; BaFin-FAQ
☐ 4	**Register vollständig führen.** LEI oder EUID des Herstellers einholen, Kündigungsfristen, Substituierbarkeit und Ausstiegsplan eintragen. Jährlich bis 31. März über die MVP einreichen, geplante Verträge für kritische oder wichtige Funktionen zeitnah anzeigen.	DORA, Art. 28 Abs. 3; ITS-Register, Art. 3 Abs. 5, B_07.01; BaFin-Register

	SCHRITT	STÜTZE
☐ 5	**Vor dem Kauf prüfen.** Risiken bewerten, Konzentration und Ersetzbarkeit einschätzen, die Eignung des Herstellers prüfen, auch Insolvenzrecht und Zugang zu Daten.	DORA, Art. 28 Abs. 4, Art. 29; RTS-Leitlinie, Art. 5 und 6
☐ 6	**Vertrag nachziehen.** Die Mindestinhalte nach Art. 30 Abs. 2 abbilden, bei kritischen oder wichtigen Funktionen auch Abs. 3, vor allem Übergangszeitraum, Audit- und Kündigungsrechte.	DORA, Art. 30; RTS-Leitlinie, Art. 8
☐ 7	**Exit-Plan schreiben.** Szenarien: Ausfall des Herstellers, schlechte oder ausbleibende Pflege, unerwartete Kündigung. Je Szenario: was weiterläuft, Ersatzlösung, Zeitplan, Zuständige.	DORA, Art. 28 Abs. 8; RTS-Leitlinie, Art. 10
☐ 8	**Lesbarkeit ohne die Software sicherstellen.** Archivierte Dokumente in einem offenen, genormten Format ablegen, etwa PDF/A, mit Original und Konvertierungs-nachweis daneben.	DORA, Art. 28 Abs. 8 UAbs. 4; Art. 30 Abs. 2 Buchst. d
☐ 9	**Exit testen.** Den Plan durchspielen, etwa mit einer Ersatzlösung auf einer Stichprobe, und das Ergebnis dokumentieren. Den Plan regelmäßig überprüfen.	DORA, Art. 28 Abs. 8 UAbs. 3; RTS-Leitlinie, Art. 10
☐ 10	**Stichprobe aus dem Archiv prüfen.** Ältere Dokumente unabhängig von der erzeugenden Software öffnen und validieren. Das zeigt, dass Daten tatsächlich „vollständig“ übertragbar sind.	DORA, Art. 28 Abs. 8 UAbs. 4

5 Typische Fehlerquellen

UNSERE LESART, JE MIT VORGABE

VORBEMERKUNG	Die folgenden Punkte sind unsere Lesart. Jeder nennt die Vorgabe, an der er ansetzt.
„KEINE AUSLAGERUNG, ALSO KEIN THEMA“	Das Register erfasst alle Vereinbarungen über IKT-Dienstleistungen, auch solche, die keine Auslagerung sind [DORA, Art. 28 Abs. 3]. Die BaFin schreibt: Das IKT-Drittparteienrisikomanagement nach DORA „ergänzt die bestehenden sektoralen Regelungen zu Auslagerungen oder Ausgliederungen“ [BaFin-FAQ]. Ein Lizenzvertrag mit Pflege kann also ins Register gehören, auch wenn er keine Auslagerung im Sinne des Versicherungsaufsichtsrechts ist.
EXIT-PLAN NUR FÜR DIE CLOUD	Art. 28 Abs. 8 unterscheidet nicht nach Betriebsform. Er knüpft an die Funktion an, die eine IKT-Dienstleistung unterstützt. Wer Exit-Pläne nur für Cloud-Dienste schreibt, übersieht selbst betriebene Software, die eine kritische oder wichtige Funktion stützt.
EIN PLAN, DER NIE GEPROBT WURDE	DORA verlangt „ausreichend getestet[e]“ Ausstiegspläne [DORA, Art. 28 Abs. 8 UAbs. 3], die RTS-Leitlinie einen „realistisch[en] und durchführbar[en]“ Plan mit Zeitplan [RTS-Leitlinie, Art. 10]. Ein Plan, der „Ersatz beschaffen“ sagt, ohne dass je ein Ersatz Ihre Dokumente verarbeitet hat, erfüllt das nach unserer Lesart nicht.
DATEN, DIE NUR DIE SOFTWARE LESEN KANN	Liegen archivierte Dokumente in einem herstellereigenen Format oder hängen Prüfbelege an einer Datenbank der Software, ist der Ausstieg eine Migration des Archivs. Das ist genau die Schwierigkeit, die die Registervorlage als Grund für schwere Ersetzbarkeit nennt [ITS-Register, B_07.01.0060].
LIZENZSPERRE ALS NICHT BEDACHTES SZENARIO	Eine Software, die ihre Lizenz online prüft oder bei Ablauf sperrt, kann ausfallen, obwohl sie in Ihrem Rechenzentrum

läuft. DORA nennt als Risiko „jede Unterbrechung der Geschäftstätigkeit aufgrund unangemessener oder unterlassener Bereitstellung von IKT-Dienstleistungen“ [DORA, Art. 28 Abs. 8 UAbs. 1]. Ein Exit-Plan sollte klären, was bei Ablauf oder Streit um die Lizenz passiert.

ENDE DER PFLEGE NICHT ERFASST

Ohne Datum für das Ende der Pflege merkt niemand, wann eine Version zum Altsystem wird [RTS-RMF, Art. 4 Abs. 2 Buchst. b Ziff. ix; DORA, Art. 3 Nr. 3]. Das ist auch die Frist, die ein Exit-Plan für die zuletzt gepflegte Version ansetzen muss.

FEHLENDE LEI

Ohne LEI oder EUID des Herstellers lässt sich das Register nicht vollständig füllen. Die BaFin akzeptiert keine Dummy-LEI; Anbieter mit Sitz in der EU können über die EUID identifiziert werden [ITS-Register, Art. 3 Abs. 5; BaFin-FAQ]. Fragen Sie die Kennung vor Vertragsschluss ab.

6 Wie Doconform das umsetzt

EIN ABSCHNITT

DOCONFORM

Doconform ist ein Konvertierungsdienst, den Sie im eigenen Rechenzentrum betreiben. Er wandelt E-Mails und Dokumente in PDF/A, veraPDF prüft jedes Ergebnis, und ein Konvertierungsvermerk hält Hashes, Schritte mit Programmversionen, erreichte Stufe und Prüfergebnis fest. Für den Ausstieg zählt, was ohne uns weiterläuft:

- **Lizenz.** Die Lizenz ist eine signierte Datei und wird offline geprüft. Läuft sie ab, wandelt Doconform weiter und meldet den Ablauf in Konsole, Log und Metrik. Ohne gültige Lizenz trägt jedes Ergebnis einen Hinweis im Producer-Feld; es bleibt PDF/A-konform.
- **Kein Zugriff des Herstellers.** Doconform baut keine Verbindung zum Hersteller auf. Eine Fernwartung gibt es nicht. Betrieb, Lizenzprüfung und Updates über das Offline-Bundle gehen ohne Internet.

- **Daten.** Die Ausgaben sind PDF/A und ein JSON-Vermerk mit veröffentlichtem Schema. Das Original lässt Doconform unverändert. Ablage und Aufbewahrung bleiben in Ihrem Archiv.
- **Pflege.** Neue Versionen erscheinen quartalsweise, Sicherheitsfixes sofort als Patch. Jede Version pflegen wir mindestens zwölf Monate. Zu jedem Image gibt es eine signierte Komponentenliste (SBOM).
- **Quellcode.** Für Enterprise ist eine Quellcode-Hinterlegung (Escrow) oder Code-Einsicht auf Anfrage möglich.
- **Was fehlt.** Ein ISO-27001-Zertifikat haben wir nicht. Der Vermerk ist noch nicht signiert; das ist geplant.

Für Versicherer bereiten wir ein **DORA-Paket** vor: Vertragsanhang nach Art. 30, Exit-Plan, Nachweis der Quellcode-Hinterlegung und die Angaben für das Informationsregister. Es ist in Vorbereitung und kommt als Zusatz zur Lizenz, Preis auf Anfrage. Ob Vertrag und Exit-Plan Ihre Anforderungen erfüllen, beurteilen Sie und Ihre Rechtsabteilung. Wie das für Versicherer aussieht, steht unter Versicherer. Den Vermerk zu einer eigenen Datei sehen Sie in der Demo.

7 Häufige Fragen

6 FRAGEN

Gehört Software, die wir selbst betreiben, ins Informationsregister?

Die Aufsicht hat das für reine On-Premises-Lizenzen nicht ausdrücklich beantwortet. Die Registervorlage kennt die Art „Softwarelizenzierung (ohne SaaS)“. Nach unserer Lesart gehört ein Vertrag ins Register, wenn zur Lizenz fortlaufend Updates, Sicherheitsfixes oder Support gehören. Eine Lizenz ohne jede weitere Leistung ist nach einer EIOPA-Antwort zu Wiederverkäufern eher keine IKT-Dienstleistung.

Brauchen wir für jede Software eine Exit-Strategie?

Nein. DORA verlangt Ausstiegsstrategien für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen (Art. 28 Abs. 8). Ob das zutrifft, bewerten Sie je Funktion.

Ist ein Lizenzvertrag eine Auslagerung?

Das richtet sich nach den sektoralen Regeln, für Versicherer nach dem Versicherungsaufsichtsrecht. DORA ergänzt diese Regeln, ersetzt sie nicht. Das Register erfasst alle Verträge über IKT-Dienstleistungen, ob Auslagerung oder nicht.

Muss der Hersteller selbst DORA umsetzen?

Nein. DORA gilt für Finanzunternehmen. Hersteller sind nach der BaFin indirekt betroffen, weil Finanzunternehmen bestimmte Anforderungen in den Vertrag aufnehmen müssen.

Bis wann muss das Register bei der BaFin sein?

Jährlich, über die Meldeplattform MVP. Die BaFin bittet, den Einreichungsprozess bis spätestens 31. März vollständig und fehlerfrei zu durchlaufen. Maßgeblich ist der Stand zum 31. Dezember des Vorjahres.

Was hat PDF/A mit dem Exit zu tun?

DORA verlangt, dass sich Daten beim Ausstieg vollständig übertragen oder ins eigene Haus zurückholen lassen. Nach unserer Lesart erfüllt ein Archiv in PDF/A mit Original und offenem Konvertierungsnachweis diese Bedingung leichter, weil die Dokumente ohne die erzeugende Software lesbar und prüfbar bleiben.

8 Quellen

GELESEN AM 16.11.2026

1. [DORA] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor. ABl. L 333 vom 27.12.2022, S. 1.
https://eur-lex.europa.eu/eli/reg/2022/2554/oj

2. [ITS-REGISTER] Durchführungsverordnung (EU) 2024/2956 der Kommission vom 29. November 2024 zur Festlegung technischer Durchführungsstandards ... im Hinblick auf Standardvorlagen für das Informationsregister. ABl. L, 2024/2956, 2.12.2024.
https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

3. [RTS-LEITLINIE] Delegierte Verordnung (EU) 2024/1773 der Kommission vom 13. März 2024 ... zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen. ABl. L, 2024/1773, 25.6.2024.
https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj

4. [RTS-RMF] Delegierte Verordnung (EU) 2024/1774 der Kommission vom 13. März 2024 ... zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens.
https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj

5. [EIOPA-Q&A 2999] EIOPA, Questions and Answers, DORA030 – 2999, Art. 3 Nr. 21 DORA (Antwort der Europäischen Kommission), Status: final.
https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en

6. [EIOPA-Q&A 3300] EIOPA, Questions and Answers, DORA 215 – 3300, Art. 28 DORA, Status: final.
https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora-215-3300_en

7. [EIOPA-Q&A 3622] EIOPA, Questions and Answers, 3622 – DORA 300, Art. 3 Nr. 21 DORA, Status: abgelehnt.
https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/3622-dora-300_en

8. [EBA-Q&A 7046] EBA, Single Rulebook Q&A 2024_7046, Definition of ICT services, Status: abgelehnt (19.07.2024).
https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2024_7046

9. [BAFIN-REGISTER] BaFin: Informationsregister und Anzeigepflichten.
https://www.bafin.de/DE/unternehmen-maerkte/aufsicht/alle-unternehmen/it-cybersicherheit/register-anzeigepflichten/register-anzeigepflichten_node.html

10. [BAFIN-FAQ] BaFin: Häufig gestellte Fragen zu DORA.
https://www.bafin.de/SharedDocs/Fragen-antworten/DE/faq-dora/faq-dora_node.html