

BEIBLATT FÜR DEN FINANZSEKTOR

DORA, MaRisk und BAIT.

Was in einem Notfallhandbuch zusätzlich stehen muss,
wenn Sie der Finanzaufsicht unterliegen.

Die Hauptvorlage deckt ab, was jeder Betrieb braucht. Dieses Beiblatt ergänzt die vier Punkte, an denen Institute darüber hinaus nachweispflichtig sind: kürzere Meldefristen, ein gepflegtes Informationsregister, erprobte Wiederanlaufpläne und die Frage, von wo im Ernstfall gearbeitet wird.

Welches Regelwerk gilt für Sie

REGELWERK	RECHTSNATUR	GILT FÜR	WAS ES ZUM NOTFALL SAGT
DORA	Verordnung (EU) 2022/2554, unmittelbar geltend seit 17.01.2025	Banken, Versicherungen, Wertpapierfirmen, Zahlungsdienstleister und deren IKT-Dienstleister	Art. 11: Reaktions- und Wiederherstellungspläne, mindestens jährlich erprobt. Art. 19: Meldung schwerwiegender Vorfälle.
KWG § 25a	Bundesgesetz	Kreditinstitute	Ordnungsgemäße Geschäftsorganisation mit angemessenem Risikomanagement. Die nationale Grundlage, auf der MaRisk und BAIT aufsetzen.
MaRisk	BaFin-Rundschreiben	Kreditinstitute	Mindestanforderungen an das Risikomanagement, einschließlich Notfallkonzept und Auslagerungssteuerung.
BAIT	BaFin-Rundschreiben	Kreditinstitute	Eigenes Kapitel zum IT-Notfallmanagement: Wiederanlaufpläne, Wiederherstellungsziele, Tests und Anforderungen an ausgelagerte Standorte.

Eine Abgrenzung vorab. DORA unterscheidet nach Art des Unternehmens, nicht nach Größe. Ein kleines Institut ist nicht deshalb ausgenommen, weil es klein ist. Umgekehrt gilt: wer als Kreditinstitut zugleich als wichtige Einrichtung nach NIS2 eingestuft ist, unterliegt beiden Meldewegen. Die Fristen auf der nächsten Seite stehen deshalb nebeneinander, nicht alternativ.

ERGÄNZUNG ZU ABSCHNITT 8

Meldefristen im Vergleich.

Drei Regelwerke, drei Uhren, drei Adressaten. Sie können bei demselben Vorfall gleichzeitig laufen. Tragen Sie unten ein, welche für Sie gelten, und hängen Sie diese Seite neben die Notfallkarte.

REGELWERK	MELDUNG	FRIST LÄUFT AB	SPÄTESTENS	AN WEN
DORA	Erstmeldung	Einstufung als schwerwiegend	4 Stunden	BaFin, MVP-Portal
	Erstmeldung, absolute Grenze	Entdeckung des Vorfalls	24 Stunden	BaFin, MVP-Portal
	Zwischenmeldung	Abgabe der Erstmeldung	72 Stunden	BaFin, MVP-Portal
	Abschlussmeldung	letzte Zwischenmeldung	1 Monat	BaFin, MVP-Portal
NIS2	Frühwarnung	Kenntniserlangung	24 Stunden	BSI, § 32 BSIg
	Folgemeldung	Kenntniserlangung	72 Stunden	BSI, § 32 BSIg
	Abschlussbericht	Kenntniserlangung	1 Monat	BSI, § 32 BSIg
DSGVO	Datenschutzverletzung	Kenntniserlangung	72 Stunden	Landesdatenschutzbehörde, Art. 33

Die Vier-Stunden-Frist ist die kritische. Sie läuft nicht ab Entdeckung, sondern ab dem Moment, in dem Sie den Vorfall als schwerwiegend einstufen. Genau deshalb muss vorher feststehen, wer diese Einstufung vornimmt und nach welchen Kriterien. Ohne benannte Person und ohne Kriterienraster verstreicht die Frist, während noch diskutiert wird, ob der Vorfall meldepflichtig ist.

STUFT VORFÄLLE ALS SCHWERWIEGEND EIN

VERTRETUNG, ERREICHBAR INNERHALB VON ____ MINUTEN

UNSERE ZUGÄNGE ZUM MVP-PORTAL DER BAFIN LIEGEN

ZULETZT AUF FUNKTION GEPRÜFT AM

Die Einstufung richtet sich nach der Delegierten Verordnung (EU) 2024/1772, die Fristen nach Art. 19 DORA in Verbindung mit der Delegierten Verordnung (EU) 2025/301. Stand Oktober 2026, keine Rechtsberatung.

ERGÄNZUNG ZU ABSCHNITT 4, 5 UND 7

Was zusätzlich dokumentiert sein muss.

Vier Nachweise, die in einem allgemeinen Notfallhandbuch nicht vorkommen und in einer Prüfung als Erstes aufgeschlagen werden.

1. Informationsregister nach DORA Art. 28

Jeder, der für Sie IKT-Leistungen erbringt, gehört hinein, auch der kleine Softwareanbieter und der Dienstleister des Dienstleisters. Das Register ist der unspektakulärste Teil von DORA und zugleich der, nach dem in Prüfungen zuerst gefragt wird.

GEFÜHRT VON	ZULETZT AKTUALISIERT	LIEGT WO	ABGLEICH MIT ABSCHNITT 9 AM

2. Wiederherstellungsziele je kritischer Funktion

Abschnitt 3 der Hauptvorlage fragt nach dem vertraglichen Stillstand. Für Institute reicht das nicht: BAIT und DORA verlangen je kritischer Funktion ein festgelegtes Wiederanlaufziel und einen zulässigen Datenverlust, beide beschlossen und dokumentiert, nicht geschätzt.

KRITISCHE FUNKTION	WIEDERANLAUF IN (RTO)	MAX. DATENVERLUST (RPO)	BESCHLOSSEN AM	ZULETZT ERREICHT
1				
2				
3				
4				
5				

3. Testpflicht nach DORA Art. 11

Mindestens jährlich und zusätzlich nach jeder wesentlichen Änderung an der Infrastruktur. Entscheidend ist nicht, dass getestet wurde, sondern dass das Ergebnis dokumentiert und die festgestellten Mängel nachverfolgt wurden.

DATUM	WAS WURDE ERPROBT	ZIEL ERREICHT	FESTGESTELLTE MÄNGEL	BEHOBEN AM

4. Von wo wird gearbeitet. Ein Wiederanlaufplan, der vorsieht, dass eine kritische Funktion innerhalb von vier Stunden wieder läuft, muss auch beantworten, wer sie ausführt und von welchem Ort. Das ist Abschnitt 7 der Hauptvorlage. Die geografische Trennung eines Ausweichstandorts vom Hauptstandort ist dabei keine Bequemlichkeit, sie ergibt sich aus den Auslagerungsanforderungen der BAIT.

ZUM SCHLUSS

Die drei Punkte, an denen Prüfungen scheitern.

Nicht an fehlenden Dokumenten. An Dokumenten, die etwas behaupten, das sich nicht belegen lässt.

- ☐ **Das Informationsregister ist unvollständig.** Es fehlt regelmäßig der Unterauftragnehmer eines gelisteten Dienstleisters. Fragen Sie Ihre Anbieter schriftlich, wen sie ihrerseits einsetzen, und legen Sie die Antwort ab.
- ☐ **Das Wiederanlaufziel ist nie gemessen worden.** Vier Stunden stehen im Plan, getestet wurde nie, oder der Test lief unter Bedingungen, die mit dem Ernstfall nichts zu tun haben. Ein Test ohne gestoppte Zeit ist kein Nachweis.
- ☐ **Der Ausweichstandort existiert nur auf dem Papier.** Ein Vertrag über Plätze ist kein Nachweis der Arbeitsfähigkeit. Nachweisbar wird es erst, wenn dort einmal tatsächlich gearbeitet wurde und das protokolliert ist.

Selbstprüfung vor der nächsten Vorlage

- | | |
|---|--|
| ☐ Informationsregister vollständig, inklusive Unterauftragnehmer | ☐ Einstufende Person für die Vier-Stunden-Frist benannt, mit Vertretung |
| ☐ RTO und RPO je kritischer Funktion beschlossen und datiert | ☐ Zugang zum MVP-Portal geprüft und erreichbar |
| ☐ Letzter Test weniger als zwölf Monate her | ☐ Ausweichstandort einmal tatsächlich genutzt und protokolliert |
| ☐ Ergebnis des Tests dokumentiert, Mängel nachverfolgt | ☐ Notfallhandbuch außerhalb der eigenen IT verfügbar |

Wenn Sie beim letzten Punkt nicht sicher sind. CentricCom betreibt vorbereitete Ausweicarbeitsplätze an drei geografisch getrennten Standorten in Deutschland, ausgelegt entlang DORA, KWG § 25a, MaRisk und BAIT. Wir richten sie ein, testen sie mit Ihnen und liefern das Protokoll, das die Prüfung sehen will.

Jürg Raess, Sales & Business Development
+49 69 4015000-33 · Montag bis Freitag, 7 bis 17 Uhr
centriccom.de/notfallarbeitsplaetze.html

Woher die Angaben stammen

DORA, Verordnung (EU) 2022/2554, anwendbar seit dem 17. Januar 2025, insbesondere Art. 11, 19 und 28. Meldefristen nach der Delegierten Verordnung (EU) 2025/301, Einstufungskriterien nach der Delegierten Verordnung (EU) 2024/1772. KWG § 25a sowie die BaFin-Rundschreiben MaRisk und BAIT. NIS2-Fristen nach § 32 BSIG in der seit dem 6. Dezember 2025 geltenden Fassung. Stand Oktober 2026. Diese Übersicht ersetzt keine Rechtsberatung und keine Prüfung durch Ihre Compliance-Funktion.