FMA
Finanzmarktaufsicht
Liechtenstein

FMA-Wegleitung 2021/17 – Umsetzung der Richtlinie IKT-Sicherheit

Wegleitung betreffend die Umsetzung der Richtlinie IKT-Sicherheit

Referenz:	FMA-WL 2021/17 / FMA-RL 2021/3
Adressaten:	• Sicherungseinrichtungen nach EAG • Versicherungsvermittler nach VersVertG • Vorsorgeeinrichtungen nach BPVG • Verwaltungsgesellschaften und Investmentunternehmen nach IUG 2015 **sofern diese nicht in den Anwendungsbereich der Verordnung (EU) Nr. 2022/2554 (DORA) fallen. Finanzintermediäre, für die DORA anwendbar ist, sind explizit von der FMA-RL 2021/3 und der FMA-WL 2021/17 ausgenommen.**
Erlass:	11. Mai 2021
Inkraftsetzung:	1. Januar 2022
Letzte Änderung:	28. Januar 2025
Rechtliche Grundlagen:	• Art. 4, Art. 25 Abs. 1 FMAG • FMA-RL 2021/3
Anhänge:	Anhang I: Abstufungen nach Randziffern

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • www.fma-li.li • info@fma-li.li

Diese Wegleitung beschreibt die Möglichkeit einer abgestuften Umsetzung der Richtlinie IKT-Sicherheit (IKT-Richtlinie – FMA-RL 2021/3) unter bestimmten Voraussetzungen. Unter Berücksichtigung von Risiko und Anwendbarkeit der einzelnen Vorschriften wird es den Finanzintermediären ermöglicht, Anforderungen zu reduzieren und eine richtlinienkonforme Umsetzung der Vorgaben unter Anwendung des Proportionalitätsprinzips zu gewährleisten.

1. Allgemeines

Um den Gefahren der stark steigenden Anzahl an Vorfällen im Bereich der IKT-Sicherheit zu begegnen, hat die FMA am 19. Mai 2021 die Richtlinie IKT-Sicherheit (FMA-RL 2021/3) publiziert. Am 17. Januar 2025 ist die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) in Kraft getreten. Die FMA-RL 2021/3 wurde in diesem Zuge angepasst, um einige der enthaltenen Regeln an die Bestimmungen gemäss DORA anzugleichen.

Jene Finanzintermediäre, für die DORA anwendbar ist, wurden im Rahmen dieser Anpassung aus der Anwendbarkeit der FMA-RL 2021/3 ausgenommen, da DORA weitergehende Bestimmungen im Bereich der IKT-Sicherheit vorsieht. Der Anwendungsbereich der FMA-RL 2021/3 wurde dementsprechend auf jene Finanzintermediäre eingegrenzt, für die DORA nicht anwendbar ist. Für diese wird durch die FMA-RL 2021/3 weiterhin nicht nur der Schutz der Kunden erhöht, sondern auch die langfristige Stabilität und Integrität des Finanzmarktes Liechtenstein gewährleistet. Die IKT-Richtlinie folgt dabei dem Proportionalitätsprinzip, wonach die Umsetzung ausgehend von der Grösse und der Komplexität der einzelnen Marktteilnehmenden abhängig ist. Demnach obliegt es dem Finanzintermediär, die Angemessenheit der Umsetzung zu bestimmen.

Jenen Finanzintermediären (gemäss Adressatenkreis), die aufgrund ihrer Grösse und Komplexität unter Umständen einem geringeren Risiko ausgesetzt sind, dient diese Wegleitung als Hilfestellung, sodass die Vorgaben gemäss dem Proportionalitätsprinzip in einer angemessenen Weise erfüllt werden können. Basierend auf der Kategorisierung der Vorgaben (Punkt 2) entscheidet der Finanzintermediär für die einzelnen Randziffern der IKT-Richtlinie, welche Umsetzung anhand der Risikostruktur angemessen ist. Bei der Abstufung sind die Mindestvorgaben gemäss Anhang I zu berücksichtigen.

2. Kategorisierung

Der Finanzintermediär hat die einzelnen Vorgaben der IKT-Richtlinie betreffend Risiko und Anwendbarkeit durch eine Person mit entsprechenden Fachkenntnissen bewerten zu lassen (bspw. durch ein IT Risiko Assessment), falls eine Abstufung vorgenommen werden soll. Die Risikobewertung ist dem Leitungsorgan zur Kenntnis zu bringen. Bei einer vollständigen Umsetzung laut IKT-Richtlinie ist keine Kategorisierung notwendig. Soll für einzelne Vorgaben der IKT-Richtlinie eine reduzierte oder anlassbezogene Umsetzung erfolgen, so müssen die entsprechenden Vorgaben gemäss den folgenden Faktoren bewertet werden:

- Risiko: Das Risiko der Randziffern wird für Dritte nachvollziehbar mit niedrig, mittel oder hoch klassifiziert. Das Risiko bezieht sich dabei auf mögliche negative Auswirkungen auf den Finanzintermediär, seine Kunden, Auftragnehmer, Dritte oder den Finanzplatz bei Abstufung der Umsetzung.
- Anwendbarkeit: Der Finanzintermediär legt den Grad bzw. die Häufigkeit der Anwendbarkeit der einzelnen Vorgaben fest.

3. Abstufung in der Umsetzung

Bei der Umsetzung der Richtlinie IKT-Sicherheit für Finanzintermediäre (gemäss Adressatenkreis) sind folgende Abstufungen in der Umsetzung abhängig von der Kategorisierung möglich.

a) Vollständige Umsetzung laut IKT-Richtlinie: Die Vorschriften der IKT-Richtlinie werden laut Richtlinie vollständig eingehalten. Es findet keine Abstufung statt; eine Begründung der Einstufung ist somit nicht notwendig. Grundsätzlich ist die Umsetzung laut IKT-Richtlinie für alle Vorgaben möglich. Bei mittlerem oder hohem Risiko gemäss Kategorisierung ist ausschliesslich eine vollständige Umsetzung laut Richtlinie erlaubt. Wenn die Einhaltung der Vorschriften dadurch nicht beeinträchtigt wird, kann die Umsetzung standardisiert auf der Basis von Musterdokumenten erfolgen.

b) Reduzierte Umsetzung: Für Vorschriften, bei welchen eine reduzierte Umsetzung möglich ist, werden vor allem formale Anforderungen an die Umsetzung gelockert. Eine Umsetzung hat weiterhin zu erfolgen, die Anforderungen werden jedoch reduziert. Eine reduzierte Umsetzung ist nur für von der FMA festgelegte Randziffern gemäss Anhang I möglich. Zudem muss das Risiko gemäss Kategorisierung als niedrig eingestuft werden.
Der Umfang der Reduktion hinsichtlich der Umsetzung ist zu dokumentieren und für Dritte nachvollziehbar zu begründen. Diese Begründung ist schriftlich festzuhalten. Zum einen beinhaltet diese Abstufung die Reduktion der Anforderungen an die Dokumentation (bspw. Prozessdokumentation), zum anderen können Anforderungen an Kontrollen reduziert werden, sofern das Risiko durch die Reduktion nicht erhöht wird. Wenn eine Einhaltung der Vorschriften dadurch nicht beeinträchtigt wird, kann die Umsetzung standardisiert auf der Basis von Musterdokumenten erfolgen.

c) Anlassbezogene Umsetzung: Eine anlassbezogene Umsetzung bestimmter Vorgaben der Richtlinie IKT-Sicherheit ist nur möglich, wenn die entsprechende Tätigkeit nicht ausgeführt wird und damit keine Anwendbarkeit der Bestimmung und dadurch keine Risiken absehbar sind. Die Nichtumsetzung ist zu dokumentieren und für Dritte nachvollziehbar zu begründen. Diese Abstufung ist nur solange möglich, solange die Voraussetzung zutrifft.

Die vollständige Umsetzung laut IKT-Richtlinie stellt den Standardfall dar. Eine Abstufung kann – muss aber nicht – vorgenommen werden und ist nur dann möglich, wenn die Voraussetzungen erfüllt sind. Die Kategorisierung in Punkt 2 ist mindestens jährlich sowie anlassbezogen zu prüfen. Die Abstufung orientiert sich zudem an den Mindestvorgaben von Anhang I.

4. Datenschutz

Die FMA verarbeitet personenbezogene Daten ausschliesslich nach den allgemeinen Datenverarbeitungsgrundsätzen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) sowie nach dem geltenden Datenschutzrecht.

Sämtliche Informationen zur Verarbeitung personenbezogener Daten, einschliesslich der Angaben zum Verarbeitungszweck, zum Datenverantwortlichen sowie zu den Betroffenenrechten sind in der FMA-Information zum Datenschutz enthalten: https://www.fma-li.li/de/fma/datenschutz/fma-information-zum-datenschutz.html

5. Inkraftsetzung

Diese Wegleitung trat am 1. Januar 2022 in Kraft und wurde am 28. Januar 2025 zuletzt geändert.

6. Änderungsverzeichnis

Am 28. Januar 2025 wurden folgende Änderungen vorgenommen:

- Die Liste der Adressaten wurde angepasst, da die Liste der Adressaten auch in Bezug auf die FMA-Richtlinie IKT-Sicherheit, die die Grundlage für diese Wegleitung darstellt, angepasst wurde.
- Anhang 1: Punkt 9.2 (vormals 8.2, Management von IKT-Vorfällen und -Problemen, Rz. 59): Änderung von «reduziert» zu «Umsetzung lt. RL», da dies als integraler Bestandteil des Vorfallmanagements zu sehen ist.
- Anhang 1: Punkt 11.7 (vormals 10.7): Änderung von «reduziert» zu «Umsetzung lt. RL», da dieser Punkt das angepasste Register der vertraglichen Vereinbarungen mit IKT-Drittdienstleistern betrifft.
- redaktionelle Anpassungen am Text, insbesondere um die Änderungen der IKT-Richtlinie zu berücksichtigen.

  Die Änderungen vom 28. Januar 2025 treten am 1. Februar 2025 in Kraft.

Anhang I: Abstufungen nach Randziffern

Kapitel	Überschrift	RZ	Max. Abstufung
1.	Grundsätze und Rechtsgrundlagen	1-5	n/a
2.	Definitionen	-	n/a
3.	IKT-Strategie	6	Umsetzung lt. RL
		7 a-c	Umsetzung lt. RL
		8	reduziert
4.	IKT-Governance	9	Umsetzung lt. RL
		10	Umsetzung lt. RL
		11	Umsetzung lt. RL, RZ 4
5.	IKT-Risikomanagementrahmen		
5.1	Organisation und Ziele	12	Umsetzung lt. RL
		13	Umsetzung lt. RL
		14	reduziert
		15	reduziert
		16 a-f	reduziert
		17	Umsetzung lt. RL
5.2	Ermittlung von Funktionen, Prozessen und IKT-Assets	18	Umsetzung lt. RL
		19	reduziert
5.3	Einstufung der Kritikalität und Risikobewertung	20	Umsetzung lt. RL
		21	Umsetzung lt. RL
		22	Umsetzung lt. RL
		23	reduziert
		24	reduziert
5.4	Risikominderung	25	reduziert
		26	reduziert
5.5	Berichterstattung	27	Umsetzung lt. RL
5.6	Interne Revision	28	Umsetzung lt. RL, RZ 4
		29	reduziert, RZ 4
6.	Informationssicherheitsmanagement		
6.1	Informationssicherheitsleitlinie	30	Umsetzung lt. RL
		31	reduziert
6.2	Überwachung der IKT- und Informationssicherheit	32 a-c	reduziert
		33	reduziert

		34	reduziert
6.3	Schulung und Sensibilisierung der Informationssicherheit	35	Umsetzung lt. RL
7.	Überprüfung, Bewertung und Testen der digitalen operationalen Resilienz / Testen von IKT-Tools und Systemen		
		36	Umsetzung lt. RL
		37	reduziert
		38 a-b	reduziert
		39	reduziert
		40	reduziert
		41	reduziert
		42	reduziert
8.	Benutzerberechtigungsmanagement		
8.1	Logische Sicherheit / Zugriffsschutz	43 a	Umsetzung lt. RL
		43 b-g	reduziert
		44	Umsetzung lt. RL
8.2	Physische Sicherheit	45	Umsetzung lt. RL
		46	reduziert
		47	reduziert
9.	IKT-Betriebsmanagement	48	reduziert
		49	Umsetzung lt. RL
		50	reduziert
		51	Umsetzung lt. RL
		52	reduziert
		53	reduziert
		54	reduziert
		55	Umsetzung lt. RL
		56	Umsetzung lt. RL
9.1	Sicherheit des IKT-Betriebs	57 a-e	reduziert
		58	reduziert
9.2	Management von IKT-bezogenen Vorfällen	59	Umsetzung lt. RL
		60 a-f	reduziert
10.	IKT-Projekte und Änderungsmanagement		
10.1	IKT-Projektmanagement	61	reduziert
		62	reduziert
		63 a-g	reduziert

		64	reduziert
		65	reduziert
		66	reduziert
10.2	Erwerb und Entwicklung von IKT-Systemen	67	reduziert
		68	reduziert
		69	Umsetzung lt. RL
		70	reduziert
		71	reduziert
		72	reduziert
		73	reduziert
10.3	IKT-Änderungsmanagement	74	reduziert
		75	reduziert
11.	Management des IKT-Drittparteienrisikos		
11.1	Grundsätze	76	Umsetzung lt. RL
		77 a-c	reduziert
		78 a-e	reduziert
		79	reduziert
		80	reduziert, RZ 4
11.2	Richtlinien zum IKT-Drittparteienrisiko	81	Umsetzung lt. RL
11.3	Die Inanspruchnahme von IKT-Drittdienstleistern zur Unterstützung kritischer oder wichtiger Funktionen	82	Umsetzung lt. RL
11.4	Risikobewertung	83	Umsetzung lt. RL
		84	reduziert
		85 a-g	reduziert
		86	reduziert
		87	reduziert
11.5	Due-Diligence-Prüfung	88	Umsetzung lt. RL
		89	reduziert
		90	reduziert
		91	reduziert
		92	reduziert
		93	reduziert
		94	reduziert
11.6	Interessenkonflikt	95	reduziert

11.7	Register der vertraglichen Vereinbarungen mit IKT-Drittdienstleistern	96 a-f	Umsetzung lt. RL
11.8	Vertragliche Vereinbarungen mit IKT-Drittdienstleistern	97	Umsetzung lt. RL
11.9	Unterauftragsvergabe	98	Umsetzung lt. RL
		99	Umsetzung lt. RL
		100	Umsetzung lt. RL
11.10	Datensicherheit	101	Umsetzung lt. RL
		102	reduziert
		103 a-c	reduziert
		104	reduziert
11.11	Datenschutz	105	Umsetzung lt. RL
		106	Umsetzung lt. RL
		107	Umsetzung lt. RL
11.12	Zugangs-, Informations- und Prüfungsrechte	108	Umsetzung lt. RL
		109	Umsetzung lt. RL
		110	Umsetzung lt. RL
		111	Umsetzung lt. RL
		112	Umsetzung lt. RL
11.13	Überwachung	113	Umsetzung lt. RL
		114	reduziert
		115	reduziert
		116	reduziert
11.14	Business Continuity bei Inanspruchnahme von IKT-Drittdienstleistern	117	Umsetzung lt. RL
11.15	Ausstiegsstrategien	118	reduziert
		119 a-d	reduziert
		120	reduziert
		121	reduziert
12.	Notfallkonzept und Business Continuity Management	122	Umsetzung lt. RL
		123	reduziert
12.1	Business-Impact-Analyse (BIA)	124	Umsetzung lt. RL
		125	reduziert
		126	reduziert
12.2	Business Continuity Planning	127	Umsetzung lt. RL
		128	reduziert

		129	reduziert
		130	Umsetzung lt. RL
12.3	Reaktions- und Wiederherstellungspläne	131	reduziert
		132	reduziert
		133	reduziert
		134	reduziert
12.4	Testen von Plänen	135	reduziert
		136	reduziert
		137 a-c	reduziert
		138	reduziert
12.5	Krisenkommunikation	139	Umsetzung lt. RL
		140	Umsetzung lt. RL
13.	Datenschutz	-	n/a
14.	Inkraftsetzung	-	n/a