FMA

Finanzmarktaufsicht
Liechtenstein

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

Referenz:	FMA-WL 2021/17
Adressaten:	- Verwaltungsgesellschaften und OGAW nach UCITSG - Verwaltungsgesellschaften und Investmentunternehmen nach IUG 2015 - Verwalter alternativer Investmentfonds nach AIFMG - Vermögensverwaltungsgellschaften nach VVG - Versicherungsvermittler nach VersVertG - Vorsorgeeinrichtungen nach BPVG - Pensionsfonds nach PFG
Betrifft:	FMA-RL 2021/3
Publikationsort:	Website
Publikationsdatum:	19. Mai 2021
Letzte Änderung	-

Die 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 Proportionalitätsgrundsatzes 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. Dadurch kann nicht nur der Schutz der Kunden erhöht, sondern auch die langfristige Stabilität und Integrität des Finanzmarktes Liechtenstein gewährleistet werden. Die IKT-Richtlinie baut dabei auf dem Proportionalitätsprinzip auf, wonach die Umsetzung ausgehend von der Grösse und der Komplexität des einzelnen Marktteilnehmers abhängig ist. Demnach obliegt es dem Finanzintermediär, die Angemessenheit der Umsetzung zu bestimmen.

Finanzintermediäre (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 zu berücksichtigen sind die Mindestvorgaben gemäss Anhang I.

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 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 folgender 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.

Erfolgt eine Abstufung und somit keine Umsetzung laut IKT-Richtlinie, so ist die Begründung schriftlich festzuhalten.

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) Umsetzung laut IKT-Richtlinie: Die Vorschriften der IKT-Richtlinie werden laut Richtlinie 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 Umsetzung laut Richtlinie erlaubt. Wenn eine Einhaltung der Vorschriften dadurch nicht beeinträchtigt wird, kann die Umsetzung standardisiert auf der Basis von Musterdokumenten (bspw. im OHB) 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. Die reduzierte Umsetzung ist zu dokumentieren und für Dritte nachvollziehbar zu begründen. 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 (bspw. im OHB) erfolgen.

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

Eine Umsetzung laut IKT-Richtlinie ist jederzeit möglich, auch wenn einer oder mehrere Faktoren in Punkt 2 als niedrig eingestuft werden. 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 wurde von der Geschäftsleitung der FMA am 11.05.2021 genehmigt und tritt am 1. Januar 2022 in Kraft.

Für weitere Rückfragen steht die FMA zur Verfügung.

Bereich Wertpapiere und Märkte
Abteilung Aufsicht

FMA

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- und Informationssicherheitsrisikomanagement		
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	Überprüfung, Bewertung und Testing der Informationssicherheit	35	Umsetzung lt. RL
		36	reduziert
		37 a-b	reduziert
		38	reduziert
		39	reduziert
		40	reduziert
		41	reduziert
6.4	Schulung und Sensibilisierung für Informationssicherheit	42	Umsetzung lt. RL
7.	Benutzerberechtigungsmanagement		
7.1	Logische Sicherheit / Zugriffsschutz	43 a	Umsetzung lt. RL
		43 b-g	reduziert
		44	Umsetzung lt. RL
7.2	Physische Sicherheit	45	Umsetzung lt. RL
		46	reduziert
		47	reduziert
8.	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
8.1	Sicherheit des IKT-Betriebs	57 a-e	reduziert
		58	reduziert
8.2	Management von IKT-Vorfällen und -Problemen	59	reduziert
		60 a-f	reduziert
9.	IKT-Projekte und Änderungsmanagement		
9.1	IKT-Projektmanagement	61	reduziert
		62	reduziert
		63	reduziert
		64	reduziert

		65	reduziert
		66	reduziert
9.2	Erwerb und Entwicklung von IKT-Systemen	67	reduziert
		68	reduziert
		69	Umsetzung lt. RL
		70	reduziert
		71	reduziert
		72	reduziert
		73	reduziert
9.3	IKT-Änderungsmanagement	74	reduziert
		75	reduziert
10.	Auslagerungen (inkl. Cloud)		
10.1	Grundsätze	76	Umsetzung lt. RL
		77 a-e	reduziert
		78	reduziert
		79	reduziert
		80	reduziert, RZ 4
10.2	Auslagerungsrichtlinien	81	Umsetzung lt. RL
10.3	Wichtige IKT-Dienste und/oder IKT-Systeme	82	Umsetzung lt. RL
10.4	Risikobewertung	83	Umsetzung lt. RL
		84	reduziert
		85	reduziert
		86	reduziert
		87	reduziert
10.5	Due-Diligence-Prüfung	88	Umsetzung lt. RL
		89	reduziert
		90	reduziert
		91	reduziert
		92	reduziert
		93	reduziert
		94	reduziert
10.6	Interessenkonflikt	95	reduziert
10.7	Register der Auslagerungsvereinbarungen	96	reduziert
10.8	Auslagerungsvereinbarung	97	Umsetzung lt. RL

10.9	Weiterverlagerungen	98	Umsetzung lt. RL
		99	Umsetzung lt. RL
		100	Umsetzung lt. RL
10.10	Datensicherheit	101	Umsetzung lt. RL
		102	reduziert
		103	reduziert
		104	reduziert
10.11	Datenschutz	105	Umsetzung lt. RL
		106	Umsetzung lt. RL
		107	Umsetzung lt. RL
10.12	Zugangs-, Informations- und Prüfungsrechte	108	Umsetzung lt. RL
		109	Umsetzung lt. RL
		110	Umsetzung lt. RL
		111	Umsetzung lt. RL
		112	Umsetzung lt. RL
10.13	Überwachung	113	Umsetzung lt. RL
		114	reduziert
		115	reduziert
		116	reduziert
10.14	Business Continuity für ausgelagerte ITK Dienste und/oder Systeme	117	Umsetzung lt. RL
10.15	Ausstiegsstrategien	118	reduziert
		119	reduziert
		120	reduziert
		121	reduziert
11.	Notfallkonzept und Business Continuity Management	122	Umsetzung lt. RL
		123	reduziert
11.1	Business-Impact-Analyse (BIA)	124	Umsetzung lt. RL
		125	reduziert
		126	reduziert
11.2	Business Continuity Planning	127	Umsetzung lt. RL
		128	reduziert
		129	reduziert
		130	Umsetzung lt. RL
11.3	Reaktions- und Wiederherstellungspläne	131	reduziert

		132	reduziert
		133	reduziert
		134	reduziert
11.4	Testen von Plänen	135	reduziert
		136	reduziert
		137	reduziert
		138	reduziert
11.5	Krisenkommunikation	139	Umsetzung lt. RL
		140	Umsetzung lt. RL
12.	Datenschutz	-	n/a
13.	Inkraftsetzung	-	n/a