DORA-Webinar 5.11.2024

Hinweise zu während des Webinars erhaltenen Fragen

FMA- und OeNB-Hinweise beziehen sich insb. auf diese Unterlage.

Stand der Hinweise ist 20.11.2024. Aktualisierungen erfolgen laufend auf der FMA-DORA-Website.

FMA- und OeNB-Antworten sind in dieser Form dargestellt.

1. Inhaltliche Frage zu DORA Dry-Run: wird es noch eine (individuelle) Information zum Ergebnis/Bewertung (an die Teilnehmer) geben?
   Siehe Folie 47: Individuelles Feedback der ESAs wird mit den teilnehmenden Unternehmen geteilt werden. Zudem bieten die ESAs am 18. Dezember 2024, von 10:00 bis 13:00, einen Workshop zur Vorbereitung der Informationsregister und zu den Ergebnissen der Dry Run Exercise 2025 an (Anmeldelink).

2. Rolle des CISO - weisungsfreie Unterordnung z.B. beim CIO in Ordnung oder Stabsstelle unter Vorstand/GF?
   CISO-Vorgaben sind in der DORA-VO nicht umfasst. Diese sieht jedoch eine IKT-Risikokontrollfunktion vor. Gemäß Art. 6 Abs. 4 DORA-VO stellen Finanzunternehmen ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicher, um Interessenskonflikte zu vermeiden. Die Finanzunternehmen sorgen für eine angemessene Trennung und Unabhängigkeit von IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen gemäß dem Modell der drei Verteidigungslinien oder einem internen Modell für Risikomanagement und Kontrolle.
   Die IKT-Risikokontrollfunktion kann dabei auch durch den CISO wahrgenommen werden, sofern ein angemessenes Maß an Unabhängigkeit gem. Art 6 Abs. 4 DORA-VO gewährleistet ist.
   Da eine angemessene Trennung entsprechend den oben angeführten Vorgaben und dem Grundsatz der Verhältnismäßigkeit zu berücksichtigen ist, kann die organisatorische Ausgestaltung nur im Rahmen einer individuellen Würdigung geklärt werden.

3. Was würde passieren, wenn man DORA nicht am 17.01.2025 einführen kann? Gibt es eine zusätzliche Frist?
   DORA ist ab 17.1.2025 anwendbar. Es sind keine Übergangsfristen vorgesehen.

4. Wann werden finale Versionen der ITS zum Informationsregister und der RTS on Subcontracting erwartet?
   Wir rechnen grundsätzlich noch Ende des Jahres mit den finalen Versionen. Da dies von Prozessen auf europäischer Ebene abhängt, können wir hier aber keine definitive Aussage treffen.
   Die ESAS haben eine Decision on reporting of information necessary for the designation of critical ICT third-party service providers am 15. November 2024 veröffentlicht:
   - Informationsregister im Jahr 2025 sollen für das Referenzdatum 31. März 2025 aufbereitet sein.
   - Die zuständigen Behörden sollen Informationsregister an die ESAs bis zum 30. April 2025 übermitteln.

- Beaufsichtigte Unternehmen melden Informationsregister im Jahr 2025 voraussichtlich in den ersten Aprilwochen an FMA.

5. Ist der EUID oder LEI-Nummer verpflichtend? Oder bleibt es auch bei der Möglichkeit, die FB-Nummer etc. anzuführen, wenn keine LEI-Nummer vorhanden ist?
   Gs. ist die Idee, verpflichtend LEI-Codes anzuführen, sofern diese vorhanden sind. Ansonsten wäre ein alternativer Code anzuführen; ob hier verpflichtend die EUID zu wählen ist, oder auch FB-Nummern valide Alternativen bleiben, ist noch nicht klar entschieden.

6. In den FAQ zum Dry Run 2024 wird bekanntlich auf eine Ausnahme für Finanzunternehmen verwiesen (74i und 75ii). Gibt es hier schon eine generelle Klarstellung seitens der ESMA, dass Dienstleistungen eines regulierten Finanzunternehmens nicht als IKT-Dienstleistung betrachtet werden?
   Die Frage wird in Gremien noch abgestimmt. Die endgültige Beantwortung wird dann auf der FMA-DORA-Website veröffentlicht. Ausnahmen könnten sich lediglich auf die iZm der Lizenz erbrachten Dienstleistung beziehen. (Siehe auch Folie 54.)

7. Können IKT RM Funktion und IKT-Drittdienstleister-Überwachungsfunktion von derselben Person besetzt werden? Gibt es hier Interessenskonflikte? Ebenso Ausübung der beiden Funktionen durch einen CISO.
   In Art. 3 Abs. 5 Delegierte Verordnung 2024/1773 RTS zu IKT-Drittdienstleistern wird klargestellt, dass die Zuständigkeit für die Überwachung der einschlägigen vertraglichen Vereinbarungen eindeutig zu regeln ist.
   Diese Vorgabe widerspricht grundsätzlich nicht der Etablierung einer gemeinsamen Kontrollfunktion iSd Art. 6 Abs. 4 DORA, auch in der Funktion des CISO. Eine Einzelfallprüfung ist jedoch erforderlich. Auf ausreichende Ressourcenausstattung ist jedenfalls zu achten.

8. Die Bafin hat folgendes veröffentlicht... Stellt ein isolierter Softwarebezug eine IKT-Dienstleistung dar?

   Bei reinen Softwarelizenzen handelt es sich üblicherweise um Nutzungsrechte, die keine IKT-Dienstleistung i.S.d. Art. 3 Nr. 21 DORA darstellen. Häufig gibt es aber noch begleitende IKT-Dienstleistungen, z.B. über mit dem Lizenzkauf verbundene Wartungs- und Supportverträge. - Wie ist dazu die Sichtweise der FMA?
   Siehe Folie 50.

9. Definition ICT Service/ICT Service provider: means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services - means an undertaking providing ICT services --> ist Wartung ein ICT Service? Ist das Bereitstellen von Ressourcen ein ICT Service?
   Wartung wäre lt. Annex III des ITS Informationsregister eine Form von IKT-Dienstleistung (sofern Bezug zu Geschäftsprozessen und dauerhafte Basis gegeben sind).

10. Wie ist der Anwendungsbereich von DORA auf Leasingunternehmen als Teil einer KI-Gruppe zu verstehen für jene Anforderungen, die auf konsolidierter Ebene die gesamte Gruppe umfassen sollen (Major Incident Reporting, ICT Risk Management Framework Report, Register of Information)? Sind in den konsolidierten Meldungen/Reports die Daten von Leasingtöchtern zu inkludieren?
    Siehe Folie 20.
    Da Leasingunternehmen nicht in den DORA-Anwendungsbereich fallen, müssen sie selbst kein Register führen. Wenn sie keine IKT-Dienstleistungen erbringen, müssen sie auch nicht in den Registern anderer Unternehmen berücksichtigt werden.

11. Spezialinstitute oder Versicherungsgesellschaften führen oftmals den Zahlungsverkehr über andere Bankinstitute durch, wofür entsprechende Online Banking Plattformen auf den Servern dieser

Spezialinstitute implementiert wurden. Ist insofern aus Sicht der FMA das Bankinstitut, das die Onlinebanking-Plattform zur Verfügung stellt, insofern als IKT Dienstleister zu sehen?
Siehe dazu insb. Fragen 48 und 33.

12. Ist das bloße zur Verfügung stellen von zB Index Daten auch via .csv data provision und somit IKT-Dienstleistung?
Das konkrete Format (z.B. csv) ist grundsätzlich unerheblich. Wenn von einem Dienstleister periodisch auf elektronischem Wege Daten übertragen werden und diese im Rahmen von IKT-Systemen in Geschäftsprozessen genutzt werden, liegt ein Indikator für eine IKT-Dienstleistung iSv DORA vor. (Siehe auch Annex III ITS Informationsregister.)

13. Gibt es eine Vorlage von der FMA für die Meldung der IKT-Vorfälle?
Hier sind die endgültigen Vorgaben abzuwarten. Das Template entspricht voraussichtlich Annex I des Draft ITS zu major incidents. Wir werden das endgültige Template schnellstmöglich – jedenfalls über die FMA Incoming-Plattform – zur Verfügung stellen.

14. Wenn Software über einen Software-Reseller (Bsp. SoftwareOne) bezogen wird. Der Reseller ist ja sozusagen zwischengeschalten zwischen Bank und Software-Dienstleister. Wie soll dieses im Informationsregister dargestellt werden? Wird dies als direkter Vertragspartner (Rang = 1) und der Software-Provider dann als Subdienstleister? Oder ist es nicht notwendig, den Reseller in der Kette darzustellen?
Siehe Folie 52.

15. Es würde allen sehr helfen, wenn seitens der Aufsichtsbehörden ein konsolidierten FAQ in Bezug auf IKT Dienstleistungen geben würde, insbesondere, ob bestimmte Dienstleistungen/Services eine IKT-DL iSd DORA darstellt oder nicht. Es macht 0 Sinn, dass sich 1000 Köpfe über die gleichen Fragen wochenlang Gedanken machen müssen!
Links zu EBA, ESA, FMA Q&As:
Joint Q&As - EIOPA
Preparation for DORA application | European Banking Authority
DORA – Überwachungsrahmen kritischer IKT-Drittdienstleistender - FMA Österreich

16. Steht bereits das finale "Format" für das Informationsregister fest (z.B. Exceltabelle, Tooling-Lösung etc)? Soll es der Dry-Run Struktur folgen (dies war kein allzu benutzerfreundliches Format und auch nicht sehr übersichtlich für die Praxis)?
Daten werden über ein xlsx-Template zu übermitteln sein, die Ausführung eines Makros wird nicht erforderlich sein.

17. Bafin hat folgendes veröffentlicht... Stellt ein isolierter Softwarebezug eine IKT-Dienstleistung dar? Bei reinen Softwarelizenzen handelt es sich üblicherweise um Nutzungsrechte, die keine IKT-Dienstleistung i.S.d. Art. 3 Nr. 21 DORA darstellen. Häufig gibt es aber noch begleitende IKT-Dienst…
Wie in der Definition der 'IKT-Dienstleistung' in der DORA-VO beschrieben, ist eine Form von 'dauerhafter Bereitstellung' einer Leistung nötig; ein reiner Einmalkauf würde dieses Kriterium nicht erfüllen. Siehe auch Folie 42.

18. Artikel 6(5): Jährlicher Bericht: wie oft/regelmäßig wird der vorrausichtlich vom Regulator angefordert, und wie viele Tage wird dem Unternahmen Zeit gegeben, um den Bericht zu liefern?
Der FMA ist auf Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens zeitnah vorzulegen. Format und Inhalt des Berichts über die Überprüfung des IKT-Risikomanagementrahmens sind in Art. 27 Delegierte Verordnung (EU) 2024/1774 (RTS zum Risikomanagement geregelt.
Eine regelmäßige Übermittlung ist aktuell nicht vorgesehen.

19. Sind Ratingagenturen wie Fitch Datenanbieter und somit IKT-Drittanbieter im Sinne der DORA Verordnung?

Dies ist abhängig von der konkreten Vertragsbeziehung mit der Ratingagentur. Wenn ein Vertrag mit einer Ratingagentur besteht, auf dessen Basis periodisch Daten über eine elektronische Schnittstelle bezogen werden, welche dann über IKT-Systeme in den eigenen Geschäftsprozessen genutzt werden, kann eine IKT-Dienstleistung iSv DORA vorliegen.

20. Informationsregister RT.07.01.: In der Anweisung zum Ausfüllen der Vorlage wird folgendes beschrieben: Wenn eine kritische o. wichtige Funktion oder wesentliche Teile davon unterstützt werden, ermöglicht diese Vorlage weitere Beurteilungen der IKT-DLen, die von IKT-DDL, einschließlich des ersten konzernexternen Subunternehmen in der IKT-DL-Kette, für das Finanzinstitut erbracht werden, wenn die vorherigen IKT-DDL konzernintern sind. Frage: Kommt dies auch zur Anwendung, wenn der direkte IKT-DDL nicht ein konzerninterner IKT-DL ist?
Hier sind Details zu Dienstleistungen zu geben, welche für kritische/wichtige Funktionen entweder direkt von einem Dienstleister erbracht werden oder der ersten Ebene an Subdienstleistern angehören, wenn der direkte Dienstleister konzernintern ist. Ist der direkte DL konzernextern, sind dessen Subdienstleister nicht in Template 07.01 zu erfassen.

21. Wird auch das neue / angepasste Template für die Meldungen vorgestellt?
Das finale Template ist noch nicht verfügbar. Änderungen beziehen sich voraussichtlich auf Feldbezeichnungen und neue Spalten in Sheet 05.01. Siehe auch Folie 43.

22. Viele Konsequenzen an Anforderungen an IKT-Drittdienstleister ergeben sich daraus, dass kritische oder wichtige Funktionen "unterstützt " werden. Kann man dieses Wort so interpretieren, dass die einzelne Dienstleistung auch einen wesentlichen Beitrag zur Funktion leistet?
Bzgl. der Definition zu ‚Unterstützung kritischer oder wichtiger Funktionen' wird auf DORA Q&A Nr. 2750 hingewiesen (Siehe https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/2750-dora006_en) Die Europäische Kommission hat dbzgl folgende Antwort übermittelt: „DORA does not provide thresholds on the level or intensity of the use of an ICT service in delivering a critical or important function of a financial entity. However, the level of engagement required for an ICT service should be considered in the light of the notion of 'critical or important functions', which is defined under Article 3(22) DORA as 'a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law'. The word "supporting" is referring to the fact that an ICT service is necessary for the delivery of critical or important functions. The ICT services should also be considered in the light of DORA's objective to achieve a high level of digital operational resilience of financial entities."
Aus Sicht der FMA ist bei der Einstufung, welche Dienstleister kritische oder wichtige Funktionen unterstützen, ein risikobasiertes Vorgehen erforderlich. Der ESA Q&A 2750 folgend, ist bei der Einstufung insb. die Frage relevant, ob der Ausfall des Systems/Dienstleisters die betroffene(n) Funktion(en) materiell (va im Hinblick auf Kontinuität und Sicherheit) einschränken würde.
Allfällige zukünftige Äußerungen oder Auslegungen der ESAs sind hier jedenfalls zu berücksichtigen.

23. Wie geht die FMA mit der 72-Stunden Regelung für den Intermediate - Report um? Besetzung z.B. am Wochenende, Bestätigung des Erhalt des Reports am Wochenende oder Feiertag,..?
Die Meldevorgaben sind einzuhalten. FMA-Bestätigungen zum Erhalt erfolgen nach Einbringung, unabhängig vom Wochentag.

24. Wenn ein Ausfall mehr als 24h dauert, aber kein kritisches Service betrifft, muss trotzdem gemeldet werden (sofern weiteren Meldeschwellen erreicht sind)?
Siehe dazu insb Art 6 Delegierte Verordnung 2024/1772.

25. Wird neben der nationalen NIS-Behörde auch das nationale Computer Notfallteam informiert?
Nein. Meldungen werden an jene in Art. 19 Abs. 6 DORA-VO genannten Institutionen weitergeleitet.

26. Wann wird das Template für das Reporting verfügbar sein bzw. hoffe ich, es beinhaltet auch die entsprechenden "list of values" als Top-Down Menüs ?
    Templates werden gs. so ausgestaltet, dass Auswahlfelder nach Möglichkeit vorgegeben sind.

27. Als Kleinstunternehmen haben wir alles in der Microsoft Cloud. Wie ist damit umzugehen? Microsoft behauptet Dora Anforderungen zu erfüllen.
    Wenn Ihr Finanzinstitut in den Anwendungsbereich von DORA fällt, wäre(n) jedenfalls mind.:
    - die von Microsoft bezogenen Dienstleistungen im Informationsregister zu erfassen (in diesem Falle wohl als Dienstleister, welcher kritische/wichtige Funktionen unterstützt).
    - zu prüfen, ob die Mindestvertragsinhalte nach Artikel 30 DORA-VO erfüllt sind.
    - die Vorgaben zur DL-Governance nach Artikel 28 und 29 DORA-VO einzuhalten. (Siehe auch *RTS to specify the policy on ICT services supporting critical or important functions.*)

    Individuelle Würdigungen sind durchzuführen.

28. Wie und in welcher Regelmäßigkeit wird es einen Rückkanal zu den Instituten aus den Vorfallsmeldungen geben?
    Die FMA wird jede erhaltene Meldung gem. Art. 19 Abs 4 DORA-VO bestätigen. Darüber hinaus kann die FMA zeitnah sachdienliche und angemessene Rückmeldungen oder allgemein gehaltene Orientierungshilfen übermitteln, insbesondere durch Zurverfügungstellung relevanter anonymisierter Informationen und Erkenntnisse zu ähnlichen Bedrohungen, sowie auf Ebene des Unternehmens angewandte Abhilfemaßnahmen und Möglichkeiten zur Minimierung und Minderung nachteiliger Auswirkungen auf den gesamten Finanzsektor erörtern. Unbeschadet der aufsichtlichen Rückmeldung bleiben Finanzunternehmen in vollem Umfang für die Handhabung und die Folgen der gemäß Art. 19 Abs. 1 DORA-VO gemeldeten IKT-bezogenen Vorfälle verantwortlich. FMA wird in Folge auch Berichte zu erhaltenen Incident-Meldungen veröffentlichen und plant, den Informationsaustausch zu Cyberbedrohungen zwischen Finanzunternehmen zu fördern.

29. Ein Katalog von kritischen/wichtigen Funktionen aus Sicht der FMA wäre hilfreich - andernfalls denken alle Institute monatelang darüber nach...
    Gibt es eine genauere Definition von "kritischen und wichtigen Funktionen"? Von welchen Ecken aus können diese Funktionen ermittelt bzw. identifiziert werden? Gibt es evtl. eine Liste an möglichen "kritischen und wichtigen Funktionen", die werden von Unternehmen zu Unternehmen wohl nicht massiv abweichen? Könnten Sie evtl. anhand anhand eines Beispiels erklären, wie man auf eine "kritische, wichtige Funktion" kommen kann?
    Blickwinkel dafür ist BRRD bzw. BaSAG.
    Die Definition einer kritischen/wichtigen Funktion unter DORA ist unabhängig von sektoralen Vorschriften zu sehen und lautet wie folgt: „*eine Funktion, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde*“ (Art. 3 Z 22 DORA-VO).
    Aufgrund der großen Spannweite der Geschäftsmodelle jener Unternehmen, die unter DORA fallen, ist die Vorgabe einer konkreten Anleitung oder Liste durch die FMA nicht möglich.
    Hier kann ua von den kritischen Geschäftsprozessen ausgegangen werden und anhand der internen Organisation abgeklärt werden, welche Komponenten dieser Prozesse (und verbundener Hilfsprozesse) kritische und wichtige Funktionen darstellen.

30. Leider gibt es keine Standardvertragsklauseln, das macht Vertragsanpassungen mit großen Playern sehr mühsam!
    Zur Erstellung von Standardvertragsklauseln sind uns keine Tätigkeiten bekannt. Wir haben den Wunsch nach Standardvertragsklauseln im Rahmen der europäischen Zusammenarbeit eingebracht.

31. Müssen signifikante Institute das Register of Information auch an die FMA übermitteln, oder wird es direkt über CASPER an die EZB übermittelt?
    Signifikante Institute werden das Informationsregister voraussichtlich ausschließlich an EZB übermitteln. Andernfalls würden sie über eine Einmeldung an FMA noch informiert.

32. Das bedeutet, ohne Aufforderung durch FMA oder ECB muss ich keine TLPTs verpflichtend durchführen?
    Verpflichtete Unternehmen werden von FMA informiert. Die Kriterien des RTS (noch nicht final veröffentlicht) geben bereits eine Indikation, ob man jedenfalls zur Durchführung verpflichtet wird. Es können auch weitere Unternehmen verpflichtet werden; auch hier erfolgt eine entsprechende Notifizierung.

33. Heißt das, dass die OeKB als Meldestelle für Meldungen gemäß InvFG nicht als IKT-Dienstleister zu sehen ist? Sind Meldungen an OeKB wie zb FundsXML Meldungen und zB Prospektveröffentlichungen, Priips-BIB usw eine IKT-DL gem DORA Art.3, Zi 21? Ähnlich wohl auch bei RegisTR SARL?
    Sofern ein Finanzunternehmen unmittelbar zur Erfüllung gesetzlicher Meldepflichten Daten an die zuständigen Behörden bzw. Adressaten übermittelt, liegt gs keine IKT-Drittdienstleistung vor (siehe Folie 55, Frage 14).
    Allgemein ist darauf hinzuweisen, dass es sich bei Dienstleistungen der OeKB um IKT-Dienstleistungen iSv DORA handeln kann, wenn diese für einen im Anwendungsbereich von DORA liegenden Empfänger erbracht werden und weitere Kriterien zur Abgrenzung von IKT-Dienstleistungen (siehe Folie 42) vorliegen.
    Die Frage, ob oder inwieweit Dienstleistungen eines regulierten Finanzunternehmens nicht als IKT-Dienstleistung betrachtet werden, wird in Gremien noch abgestimmt. Die endgültige Beantwortung wird dann auf der FMA-DORA-Website veröffentlicht.
    Bezüglich RegisTR ist festzuhalten, dass die FMA nicht für die Aufsicht von Transaktionsregistern zuständig ist, sondern diese der direkten Aufsicht durch die ESMA unterliegen.

34. Software licencing (excluding SaaS) Provision of software run on premises. ist auch enthalten - daher hätten wir angenommen, Lizenzen sind inkludiert? Was ist mit Lizenzen die weder on prem noch als SaaS bereitgestellt werden (bspw. im RZ des Anbieters ...)?
    Siehe Annex III des ITS zum Informationsregister. ‚Software Licensing' ist als eigene Art der IKT-Dienstleistung enthalten. Sobald also Softwarelizenzen bezogen werden, kann eine IKT-Dienstleistung vorliegen, unabhängig davon, ob die Software on premise oder bei einem RZ-Betreiber installiert ist. Wie in der Frage angemerkt, ist hier die Abgrenzung zu SaaS zu beachten.

35. Wie ist die Situation mit Jahreslizenzen (oft auch Abos) wo man immer eine Lizenz für eine bestimmte Zeit bezieht? Ist das als repetitiver Kauf einer Zeitlizenz zu sehen oder begründet das eine dauerhafte IKT-DDL?
    Sobald Leistungen vom selben Anbieter auf laufender Basis bezogen werden, kann eine IKT-Dienstleistung iSv DORA vorliegen. Diese Definition umfasst auch periodische Käufe oder Werkvertragsketten, da sich aus diesen Varianten von Verträgen kein Ausschluss von IKT-Drittparteienrisiken ergibt.

36. Im Template des Dry-Run mussten unter anderem Informationen aus dem Jahresabschluss der beinhalteten Gesellschaften angegeben werden. Diese werden formal zu diesem Zeitpunkt (Anfang April) für das Vorjahr (2024) noch nicht final vorhanden sein. Sollen hier dann geschätzte Werte herangezogen werden oder jene Werte aus dem Vor-Vorjahr (2023)?
    Die zum Stichtag 31.3.2025 aufrechten Verträge sollen für die Meldung des Informationsregisters 2025 erfasst sein.

37. Informationsregister: Sind somit vor dem 31.03.2025 ausgelaufende Verträge out-of-scope? Wir haben aktuell das Thema mit per 31.12. auslaufenden Verträgen.
    Das erste zu meldende Informationsregister soll auf den 31.3.2025 referenzieren. Davor ausgelaufene Verträge sind dann nicht zu melden. Im Ergebnis werden nur zum Stichtag 31.3.2025 aufrechte Verträge zu erfassen sein.

38. Gruppe ist ausschließlich in AT vertreten. Gem. DORA müssen Informationsregister auch auf teilkonsolidierter Ebene geführt werden. Bedeutet das, dass je Gesellschaft ein Informationsregister intern zu führen ist, jedoch nur ein konsolidiertes Informationsregister an die FMA zu übermitteln ist?
    Informationsregister sind gem. Art 28 Abs.3 DORA-VO durch Finanzunternehmen auf Unternehmensebene sowie auf teilkonsolidierter und konsolidierter Ebene zu führen. Zur Meldung des Informationsregisters an die FMA Siehe Folie 44. Für die Meldung ist die höchstmögliche Konsolidierungsstufe vorgesehen. Die Konsolidierung überschreitet dabei auch Ländergrenzen.

39. Gilt das Reg. of Info. Cut-Off-Datum vom 31.03.2025 auch für Institute außerhalb von AT bzw. der EU?
    Der Stichtag 31.3.2025 bezieht sich sämtliche Meldeinhalte, die auf (teil-/konsolidierter) Basis an die FMA zu übermitteln sind.

40. Gilt das nur für das Informationsregister oder sind die Tochtergesellschaften z.b in der Schweiz auch von der kompletten DORA-Verordnung betroffen?
    Tochtergesellschaften in der Schweiz sind gs. nicht im DORA-Anwendungsbereich umfasst. Siehe dazu aber auch Folie 20.

41. Konsolidierung InfoRegister: ist lt. der Präsentation nun ein MUSS dass das konsolidiert zu melden ist, korrekt?
    Siehe Folie 44

42. Könnte man davon ausgehen, dass die TLPT-Tests nicht gleich im 2025 vorzunehmen sind und die FMA entsprechend Zeit zwischen Bekanntgabe und Durchführung gewährleisten wird?
    TLPT ist ab Jänner 2025 für bestimmte Finanzunternehmen verpflichtend und jene Finanzunternehmen, die diese durchführen müssen, werden rechtzeitig informiert.

43. IKT-System: Dienstleister nutzt ein System für seine Prozesse und a) übermittelt das Ergebnis via Excel und Mail an die Bank -> kein IKT-Service? b) übermittelt das Ergebnis mittels einer automatischen Schnittstelle an Bank, die über Schnittstellen in die Banksysteme eingespielt werden - kein IKT-Service? c) stellt der Bank eine Plattform zur Verfügung, wo die Bank die Ergebnisse downloaden kann - kein IKT-Service?
    Über welche konkrete elektronische Schnittstelle/Medium – eine Übertragung per Brief/Telefon ist ausgeklammert – der Dienstleister Daten übermittelt, ist an sich kein Entscheidungskriterium. Wenn ein Bezug zur Geschäftstätigkeit, eine dauerhafte Leistung und ein IKT-Bezug nach Annex III des ITS vorliegen, liegen Hinweise für eine DORA IKT-DL vor.

44. Wenn es ein einheitliches Template für das Register geben wird für alle EU-Länder, wieso wird diese Einheitlichkeit nicht auch für die Meldung von Major IT Incidents sichergestellt, um die Heterogenität zu verhindern?
    Mit dem Final Report draft ITS on incident reporting wird die Verwendung eines einheitlichen Meldeformulars vorgeschrieben.

45. Müssen Headoffice Institute an die FMA die Incidents von Töchterunternehmen in anderen EU Ländern konsolidiert melden? Das wäre wieder eine Doppelmeldung da die Meldung an die lokale Behörde ja auch erfolgen muss.
    Die Meldeverpflichtung bezieht sich gem. Art. 19 Abs. 1 DORA-VO gs. auf Finanzunternehmen. Darüber hinaus besteht die Möglichkeit der Auslagerung der Meldeverpflichtung an einen Drittdienstleister (Art. 19 Abs. 5 DORA-VO). Auch aggregiertes Reporting durch einen Drittdienstleister für mehrere Finanzunternehmen ist möglich (Art 7 Final report draft ITS on incident reporting).

46. Sollte eine konsolidierte Meldung der Incidents von Auslandstöchtern an die FMA erfolgen müssen, können hierfür die erweiterten Meldefristen außerhalb von Wochenende und Feiertag auch für SI

angewendet werden? Ansonsten müsste ein AT Headoffice ein 24/7 Team für die Weiterleitung von Meldungen von Incidents von Auslandtöchtern haben.
Siehe auch Beantwortung der vorhergehenden Frage.
Die verlängerten Wochenend- und Feiertagsfristen gelten voraussichtlich nicht für credit institutions, central counterparties, operators of trading venues, and other financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, or financial entities declared as significant or systemic by the competent authority.

47. Also sind von einer regulierten Tochtergesellschaft einer Bank erbrachten IKT-Dienstleistungen auch keine IKT-Dienstleistungen?
Unternehmen, die Teil einer Finanzgruppe sind und IKT-Dienstleistungen vorwiegend für ihr Mutterunternehmen oder für Tochterunternehmen oder Zweigniederlassungen ihres Mutterunternehmens erbringen, sowie Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen erbringen, gelten ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung. (Siehe Erwägungsgrund 63 DORA-VO).
Die Frage, ob Dienstleistungen eines regulierten Finanzunternehmens nicht als IKT-Dienstleistung betrachtet werden, wird in Gremien noch abgestimmt. Die endgültige Beantwortung wird dann auf der FMA-DORA-Website veröffentlicht.

48. Bedeutet Frage 13 auf Folie 54, dass ein System zur Abwicklung von Überweisungen, das durch ein Bankinstitut zur Verfügung gestellt wird, nicht darunter zu verstehen ist?
Siehe dazu auch Erwägungsgrund 63 DORA-VO: *Angesichts der zunehmenden Abhängigkeit des sich entwickelnden Marktes für Zahlungsdienste von komplexen technischen Lösungen sowie angesichts neu entstehender Arten von Zahlungsdiensten und zahlungsbezogenen Lösungen sollten diejenigen Teilnehmer des Ökosystems für Zahlungsdienste, die Zahlungsabwicklungstätigkeiten durchführen oder Zahlungsinfrastrukturen betreiben, ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung gelten, mit Ausnahme von Zentralbanken, die Zahlungs- oder Wertpapierliefer- und -abrechnungssysteme betreiben, und von staatlichen Behörden, die IKT- bezogene Dienste im Zusammenhang mit Funktionen des Staates bereitstellen.*

49. Werden Sie wie angekündigt neben Ihren Ausführungen zum Informationsregister auch noch zu den notwendigen Vertragsänderungen berichten? Wie streng reagiert die Aufsicht ab Jänner, wenn es uns mit einzelnen Dienstleistern nicht gelingt, unsere Verträge DORA-konform anzupassen?
Ist die volle Überarbeitung aller Verträge bis zur Deadline in der Praxis nicht möglich, könnte es ggf. sinnvoll sein, die für das Unternehmen wichtigsten Verträge zu priorisieren. Da keine Übergangsfrist vorgesehen ist, muss die FMA grundsätzlich die volle Einhaltung der Mindestvertragsvorgaben ab 17.1.2025 beaufsichtigen.

50. Sind die Meldeplattformen der OeNB als IKT-Dienstleistungen im Sinne der DORA-Verordnung einzustufen? Wäre die OeNB in diesem Fall als IKT-Dienstleister zu betrachten?
OeNB gilt nicht als DORA-IKT-Dienstleister.

51. Ich war immer der Ansicht, der Dry Run sollte genau dafür genutzt werden, um die kritischen IKT DL zu identifizieren?
Die 2025 zu übermittelnden Informationsregister dienen als Basis für die Bestimmung der kritischen IKT-Drittdienstleister.

52. Banken im öffentlichen Eigentum müssen Daten (inklusive Sujet- und Videodaten) gemäß MedientransparenzG einmelden. Diese müssen in einer eigens von RTR (Rundfunk und Telekom Regulierungs-GmbH) zur Verfügung gestellten Plattform hochgeladen werden. Fällt die RTR als GmbH daher unter die DORA und muss als IKT DDL klassifiziert werden oder kann sie als Behörde gewertet werden?
Siehe Frage 33.

53. Im Template des Dry-Run mussten unter anderem Informationen aus dem Jahresabschluss der beinhalteten Gesellschaften angegeben werden. Diese werden formal zu diesem Zeitpunkt (Anfang

April) für das Vorjahr (2024) noch nicht final vorhanden sein. Sollen hier dann geschätzte Werte herangezogen werden …
Das Informationsregister ist vorrangig kein Finanzreporting. Gs. sind die zum verlangten Stichtag eingeforderten Daten heranzuziehen. Liegen diese begründet nicht vor, kann eine bestmögliche Schätzung, ausgehend von den aktuellsten Daten, vorgenommen werden.

54. According to the letter from ECB (as of 12 September 2024), it is stated that no Outsourcing Register will be required in 2025.

    "Consequently, the current ECB collection of outsourcing registers will be discontinued in 2025 and replaced by the new DORA RoI."

    Usually, we must provide in 2025 the Outsourcing Register with data as of 31.12.2024.

    So, can you help us to get clarification, if we need to provide an Outsourcing Register beginning of 2025 with data as of 2024?
    Diesbezüglich definiert EZB die relevanten Erfordernisse.

55. Werden die Prüfregeln der FMA bezüglich des Registers of Information veröffentlicht, damit sich die Institute vorbereiten können?
    Den beaufsichtigten Unternehmen werden diese Prüfregeln voraussichtlich zur Verfügung gestellt werden.

56. Wie sind Dienstleistungen einzumelden, die gem. EBA keine Auslagerung (weil sie unter eine taxativ genannte Ausnahme fallen) darstellen, aber gem. DORA als IKT-Dienstleistung, die kritische und wichtige Funktionen unterstützen, einzustufen sind (zB PSA)?
    DORA-Bestimmungen sind für das Meldeerfordernis relevant.

57. Gibt es/wird es eine Übersicht über die Meldungen und Abgabefristen geben?
    Schwerwiegende IKT-bezogene Vorfälle: Siehe insb. Final report draft RTS and ITS on incident reporting.
    Informationsregister: Siehe Frage 4.

58. Folie 29 ⇨ möglicher inhaltlicher Fehler
    Ziehen Sie Delegierte Verordnung (EU) 2024/1772 zur Nachvollziehung heran. Gehen Sie dabei insb. von Art. 8 aus.

59. Folie 37 ⇨ was ist mit Open Source Analysen genau gemeint?
    Diese könnten sich auf Open-Source-Software beziehen (Vgl. Erwägungsgrund 56 DORA-VO).

60. Wie soll ein Unternehmen mit nicht änderbaren Abhängigkeiten umgehen?
    Die Finanzunternehmen sollten bei der Überwachung der Risiken, die auf Ebene der IKT-Drittdienstleister entstehen, einen verhältnismäßigen Ansatz verfolgen, indem Art, Umfang, Komplexität und Bedeutung ihrer IKT-bezogener Abhängigkeiten und die Kritikalität oder Bedeutung der Dienste, Prozesse oder Funktionen, die den vertraglichen Vereinbarungen unterliegen, letztlich je nach Sachlage anhand einer sorgfältigen Bewertung jeglicher potenzieller Auswirkungen auf die Kontinuität und Qualität von Finanzdienstleistungen auf Einzel- und Gruppenebene gebührend berücksichtigt werden. (Siehe Erwägungsgrund 64 DORA-VO)

61. Was ist einzutragen, wenn ein IKT DL außerhalb EU keinen LEI hat? Kann das Feld freigelassen werden?
    Das finale Template wird die Möglichkeit enthalten, alternative Codes anzugeben.

62. Sind Zweigniederlassungen welche in der Schweiz tätig sind, von der DORA betroffen, wenn in AT der Hauptsitz ist?
    Diese sind gs. nicht im DORA-Anwendungsbereich umfasst. Siehe dazu auch Folie 20.

63. Welches Excel-Template für das Inforegister ist zu verwenden?
    Finales Template existiert noch nicht, da der ITS zum Template noch nicht final ist. Erwartungsgemäß wird es sehr ähnlich zum Dry Run Template gestaltet sein (+ zusätzliche Spalten in 05.01, ev. geänderte Spaltenbezeichnungen).

64. Wird es noch Informationen/Inputs zur Definition der kritischen oder wichtigen Funktionen geben?
    Siehe Frage 22. Darüber hinaus sind weitere Fragen zu diesem Thema an die ESAs herangetragen worden.

65. Für Versicherungen mit einer Composit-Lizenz - wie sind hier die Funktionen/Verträge abzubilden? Einen eigenen Eintrag unter Lizenzen hierfür gibt es nicht.
    Bitte richten Sie Ihre Frage – unter Anführung weiterer Details – an die FMA.

66. Softwarewartung ist lt Vortrag eine IKTDDL. Welcher Code wäre lt. Annex III heranzuziehen?
    Derzeit wäre der Code S14.

67. Eine Funktion wird als kritische und wichtige eingestuft. Ein IKT-Dienstleister liefert hierzu Leistungen. Ein Ausfall dieser Leistungen hat aber KEINE materielle Auswirkung auf die Funktion. Ist diese IKT-DL als unterstützend für eine kritische und wichtige Funktion einzustufen? Welcher Funktion ist dieser IKT-DL im Inforegister zuzuordnen?
    Siehe Frage 22.

68. Wenn die Datensicherung eines KI an ein externes Rechenzentrum ausgelagert ist, ist dann gem Art 12 trotzdem ein Datensicherungs-/Datenwiedergewinnungskonzept zu erstellen, oder reicht ein Audit im Rechenzentrum?
    Ja. Die Letztverantwortung liegt beim Finanzunternehmen.

69. Es gibt die Meinung, dass im Register nur kritische/wichtige Funktionen erfasst werden müssen. Ist dies der Fall?
    Nein. Siehe insb. Art 3 ITS Informationsregister.

70. Fallen Dienstleister, die Meldungen an Trade Repositories vornehmen (EMIR, MiFIR) auch unter DORA?
    Siehe Frage 33.
    Im Übrigen ist festzuhalten, dass die FMA nicht für die Aufsicht von Transaktionsregistern zuständig ist, sondern diese der direkten Aufsicht durch die ESMA unterliegen.