

Übertragungsvereinbarungen

gem. § 13 KMG 2019

Präambel

(i) Die Finanzmarktaufsicht (idF FMA) ist gemäß § 13 Abs 1 KMG 2019 die in Österreich zuständige Behörde nach der **Verordnung (EU) 2017/1129 („PVO“)**. Art 31 Abs 2 PVO gestattet den Mitgliedstaaten, **Aufgaben im Zusammenhang mit der elektronischen Veröffentlichung gebilligter Prospekte und zugehöriger Dokumente** an Dritte zu übertragen. Der österreichische Gesetzgeber hat von dieser Ermächtigung in § 13 Abs 3 KMG 2019 Gebrauch gemacht und die FMA zur Übertragung dieser Aufgaben an die Oesterreichische Kontrollbank AG (idF OeKB) in ihrer Funktion als Meldestelle gemäß KMG (idF Meldestelle) ermächtigt. **Teil 1** der vorliegenden Vereinbarung regelt den Umfang und die Bedingungen dieser Aufgabenübertragung. Die bisherige zwischen den Parteien bestehende Übertragungsvereinbarung vom 3. Juli 2019 tritt mit Inkrafttreten der vorliegenden Übertragungsvereinbarung außer Kraft.

(ii) Die FMA ist gemäß Art 21a Abs 3 PVO als zuständige Behörde nach der PVO auch Sammelstelle gemäß Art 2 Nr 2 der **Verordnung (EU) 2023/2859 („ESAP-VO“)**. Die Sammelstelle kann bestimmte, in Art 5 Abs 8 ESAP-VO festgelegte Aufgaben an eine dem Recht eines Mitgliedstaats unterliegende juristische Person oder an eine Einrichtung oder sonstige Stelle der Union („Befugnisempfänger“) übertragen. Die Meldestelle gemäß KMG ist gemäß § 13 Abs 3a KMG über die in Abs. 3 leg cit genannten Aufgaben hinaus berechtigt, Aufgaben als Befugnisempfänger im Rahmen ihrer gesetzlichen Tätigkeit nach dem KMG zu übernehmen. **Teil 2** der vorliegenden Vereinbarung regelt für die nach der PVO an den European Single Access Point (ESAP) zu übermittelnden Informationen den Umfang und die Bedingungen dieser Aufgabenübertragung.

Soweit sich Tätigkeiten aus den beiden oben genannten Übertragungsverhältnissen insofern überschneiden, als sie unter den Anwendungsbereich beider Rechtsgrundlagen subsumierbar sind oder Zweifel bestehen, welchen der beiden Rechtsgrundlagen sie zuzurechnen sind, gehen die Regelungen des Teils 1 vor.

(iii) Die Parteien bekunden das gemeinsame Verständnis, auch künftige Aufgabenübertragungen bzw.-übernahmen nach Art 5 Abs 8 ESAP-VO, möglichst im Rahmen und gemäß der Regelungsstruktur der vorliegenden Vereinbarung vorzunehmen. Zu diesem Zweck ist der vorliegenden Vereinbarung ein Muster der in diesen Fällen standardmäßig aufzunehmenden Mindestregelungen als **Anlage 3** angefügt.

Die vorliegende Vereinbarung wird zwischen der

Finanzmarktaufsichtsbehörde

Otto-Wagner-Platz 5

1090 Wien

als übertragende Behörde und Sammelstelle einerseits

und der

Oesterreichischen Kontrollbank AG in ihrer Funktion als Meldestelle gemäß KMG 2019

Strauchgasse 3

1010 Wien

als ausführende Stelle und Befugnisempfänger andererseits geschlossen.

Übertragungsvereinbarung (Teil I)

gemäß § 13 Abs 3 Z 3 KMG 2019

§ 1 Begriffsbestimmungen

Im Sinne von Teil I dieser Vereinbarung bezeichnet der Ausdruck

1. **Prospektverordnung:** die Verordnung (EU) 2017/1129 des Europäischen Parlaments und des Rates vom 14. Juni 2017 („PVO“) in der zuletzt geänderten Fassung;
2. **Kapitalmarktgesetz 2019:** Bundesgesetz über das öffentliche Anbieten von Wertpapieren und anderen Kapitalveranlagungen („KMG 2019“) in der geltenden Fassung;
3. **Datenschutz-Grundverordnung:** die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 („DSGVO“) in der geltenden Fassung;
4. **Prospekt:** einen Prospekt gemäß der PVO, der von der FMA gebilligt wird;
5. **Endgültige Bedingungen:** emissionsspezifische Bedingungen von Emissionen, die unter einem Basisprospekt nach Art 2 lit s der PVO begeben werden („Final Terms“) und gemäß Art 8 Abs 5 PVO originär bei der FMA (siehe aber § 24 Abs 1 KMG 2019) zu hinterlegen sind;
6. **Endgültiger Emissionskurs und Endgültiges Emissionsvolumen:** die Angaben nach Art 17 Abs 1 PVO; sofern nicht im Prospekt genannt, sind sie gemäß Art 17 PVO originär bei der FMA (siehe aber § 24 Abs 1 KMG 2019) zu hinterlegen;
7. **Prospektnachtrag:** einen Nachtrag zum Prospekt gemäß Art 23 PVO, der von der FMA gebilligt wird;
8. **Registrierungsformular:** ein einheitliches Registrierungsformular nach Art 9 PVO oder ein Registrierungsformular nach Art 10 PVO, das von der FMA gebilligt oder dort hinterlegt wird;
9. **Ausgehende Notifizierung:** Bescheinigung der FMA als Billigungsbehörde (via „Certificate of Approval“) an die zuständige Behörde im Aufnahmemitgliedstaat, dass der/das Prospekt/Nachtrag/Registrierungsformular von ihr im Einklang mit der PVO gebilligt wurde sowie Übermittlung einer elektronischen Kopie (ausgehendes Passporting) gemäß Art 25 PVO;
10. **Eingehende Notifizierung:** Bescheinigung einer anderen Billigungsbehörde im EWR (via „Certificate of Approval“) an die FMA als Behörde im Aufnahmemitgliedstaat, dass der/das Prospekt/Nachtrag/Registrierungsformular von ihr im Einklang mit der PVO gebilligt wurde sowie Übermittlung einer elektronischen Kopie (eingehendes Passporting) gemäß Art 25 PVO;
11. **TOM:** Technische und organisatorische Maßnahmen nach DSGVO;
12. **Dokument nach Anhang IX:** Informationen, die in das Dokument nach Art 1 Abs 4 UntAbs 1 lit da und db und nach Art 1 Abs 5 UntAbs 1 lit ba PVO, das gleichzeitig mit seiner Veröffentlichung originär bei der FMA zu hinterlegen ist, aufzunehmen sind.

§ 2 Gegenstand der Aufgabenübertragung

(1) **Veröffentlichungen nach Art 21 Abs 5 PVO:** Die Meldestelle hat alle von der FMA gebilligten oder an diese notifizierten Prospekte und Prospektnachträge sowie alle von der FMA gebilligten, an diese notifizierten oder bei dieser hinterlegten Registrierungsformulare samt deren Änderungen auf ihrer **Website** unter dem Navigationspfad zum Online-Meldestelle-Portal samt Angabe der Aufnahmemitgliedstaaten (ein- und ausgehende Notifizierungen) **zu veröffentlichen**, sofern und soweit

ihr diese Dokumente zuvor zu diesem Zwecke von der FMA auf elektronischem Wege übermittelt wurden.

(2) **Datenaufbereitung für Veröffentlichungen im ESMA Speichermechanismus (Prospektregister) gemäß Art 21 Abs 6 und Notifizierungsportal gemäß Art 25 Abs 6 PVO:** Die FMA überträgt für die Zwecke des Hochladens im ESMA-Notifizierungsportal und der Veröffentlichung im ESMA-Speichermechanismus die Entgegennahme der endgültigen Bedingungen (siehe auch § 24 Abs 1 Satz 5 KMG 2019), des endgültigen Emissionskurses und des endgültigen Emissionsvolumens („FOPA-Dok“; siehe auch § 24 Abs 1 Satz 6 KMG 2019) sowie des Dokuments nach Anhang IX auf die Meldestelle. Die Meldestelle hat die Prospekte, die Prospektnachträge, die Registrierungsformulare, deren Änderungen, die endgültigen Bedingungen, das FOPA-Dokument, das Dokument nach Anhang IX und die für die Klassifizierung gemäß dem technischen Regulierungsstandard der Europäischen Kommission VO (EU) 2019/979 relevanten begleitenden Daten für die FMA zum Zwecke des Hochladens im **ESMA-Notifizierungsportal** und der Veröffentlichung im **ESMA-Speichermechanismus in technischer Hinsicht aufzubereiten**. Sie greift dabei insbesondere auf die ihr im Zuge von Meldungen zum Emissionskalender und/oder von der FMA zur Verfügung gestellten Dokumente und Daten zu.

(3) Die nähere, für die Zwecke des Abs 2 erforderliche IT-Aufbereitung wird zwischen der FMA und der Meldestelle gemäß den jeweiligen Erfordernissen, wie sie sich aus den Datenspezifikationen des ESMA-Notifizierungsportals und des ESMA-Speichermechanismus ergeben, periodisch und anlassbedingt einvernehmlich schriftlich festgelegt und in einer **Anlage 1** zu dieser Übertragungsvereinbarung nach jeweils aktuellem Stand dokumentiert.

§ 3 Übermittlungen an die Meldestelle

Für die Zwecke der Aufgabenerfüllung durch die Meldestelle gemäß der vorliegenden Übertragungsvereinbarung übermittelt die FMA der Meldestelle die in § 2 Abs 1 genannten Dokumente samt den von ihr im Zuge der Billigung erhobenen Metadaten gemäß der VO (EU) 2019/979, den jeweiligen mit der Amtssignatur der FMA versehenen Billigungsbescheid oder gegebenenfalls eine Notifizierungsbestätigung der Herkunftslandbehörde („Certificate of Approval“). Die technische Art und Weise der Übermittlung sowie die zu übermittelnden Metadaten werden in Anlage 1 zu dieser Übertragungsvereinbarung von den Parteien näher festgelegt.

§ 4 Fristen

Sämtliche Übermittlungen der FMA nach § 3 sowie die darauf basierenden Aufgaben der Meldestelle nach den §§ 1 u 2 dieser Vereinbarung haben möglichst ohne unnötigen Aufschub zu erfolgen.

§ 5 Interessenkonflikte- und Wettbewerbsklausel

Die OeKB in ihrer Funktion als Meldestelle verpflichtet sich aufgrund ihres Handelns und durch ihre Organisationsstruktur zu gewährleisten, dass Interessenkonflikte vermieden werden und Informationen, die sie bei Ausführung der ihr gemäß dieser Vereinbarung übertragenen Aufgaben erhält, nicht missbräuchlich oder wettbewerbswidrig zu verwenden.

§ 6 Haftung

(1) Die Haftung der Vertragsparteien für Schäden aus oder im Zusammenhang mit dem gegenständlichen Vertragsverhältnis wird – mit Ausnahme von Personenschäden – auf Fälle der groben Fahrlässigkeit und des Vorsatzes beschränkt.

(2) Die OeKB haftet nicht für unmittelbare bzw. mittelbare Folgeschäden. Eine Haftung der OeKB für Schäden Dritter ist ausgeschlossen. Die Haftung der OeKB für Schäden aus dem gegenständlichen Vertragsverhältnis ist im Kalenderjahr insgesamt der Höhe nach mit jenem Betrag begrenzt, welcher der von ihr in dem Schadenseintritt vorangegangenen Kalenderjahr für ihre Tätigkeit als Meldestelle aus dem gegenständlichen Vertragsverhältnis eingehobenen Vergütung entspricht.

(3) Ein Ersatzanspruch besteht nicht, sofern und soweit der geltend gemachte Schaden durch die Einlegung von Rechtsmitteln, durch die Erhebung einer Beschwerde an ein Verwaltungsgericht und Revision an den Verwaltungsgerichtshof oder durch sonstige gesetzlich begründete Maßnahmen hätte abgewendet werden können.

§ 7 Datenschutz

(1) Die Meldestelle verarbeitet personenbezogene Daten zum Zweck des Empfangens, Kennzeichnens und Rückübermittels für das ESMA Notifikationsportal. Gegenstand der Verarbeitung sind Prospekte, Prospektnachträge, Registrierungsformulare und das Anhang IX Dokument samt der Metadaten nach Art 21 Abs 5 PVO (im PDF-Format) sowie die darin enthaltenen personenbezogenen Daten; betroffen sind die darin ausgewiesenen natürlichen Personen. Die Dauer der Verarbeitung entspricht der Laufzeit dieser Vereinbarung.

(2) Unbeschadet der Verarbeitung aufgrund ihrer gesetzlichen Verpflichtungen nach dem KMG verarbeitet die Meldestelle die Daten für die Zwecke der vorliegenden Vereinbarung ausschließlich auf dokumentierte Weisung der FMA – auch im Falle einer Drittlandübermittlung, soweit sie hierzu nicht gesetzlich verpflichtet ist – und informiert die FMA unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Sie gewährleistet die Vertraulichkeit der befugten Personen, trifft sämtliche Maßnahmen nach Art 32 DSGVO (gemäß TOM, s. Anlage 4), wahrt die Voraussetzungen für die Beiziehung weiterer Auftragsverarbeiter nach Art 28 Abs 2 und 4 DSGVO und unterstützt die FMA bei der Erfüllung von Betroffenenanträgen (Art 12-22 DSGVO) sowie bei ihren Pflichten nach Art 32-36 DSGVO. Nach Leistungsende gemäß Anlage 2 löscht sie sämtliche Daten und löscht vorhandene Kopien, soweit keine gesetzliche Speicherpflicht entgegensteht oder keine Speicherung aufgrund der Funktion der Meldestelle nach dem KMG erfolgt. Sie stellt der FMA alle erforderlichen Nachweise zur Verfügung und ermöglicht Überprüfungen und Inspektionen.

(3) Die Meldestelle darf weitere Auftragsverarbeiter nach Maßgabe der DSGVO beiziehen, sofern sie diesen die gegenständlichen datenschutzrechtlichen Pflichten vollumfänglich überbindet.

§ 8 Inkrafttreten und Beendigung

(1) Teil 1 der vorliegenden Übertragungsvereinbarung ersetzt die zwischen der FMA und der Meldestelle abgeschlossene Übertragungsvereinbarung vom 3. Juli 2019.

(2) Die vorliegende Übertragungsvereinbarung wird auf unbestimmte Zeit geschlossen und kann von jeder der Parteien durch schriftliche Erklärung gegenüber der jeweils anderen Partei unter Einhaltung einer Frist von zumindest sechs Monaten zum Ende eines jeden Kalenderhalbjahres beendet werden. Das Recht jeder der Parteien auf sofortige Beendigung im Falle eines außerordentlichen Beendigungsgrundes bleibt hierdurch unberührt. Als außerordentlicher Kündigungsgrund gilt für die Meldestelle insbesondere, wenn die ihr übertragenen Aufgaben nicht mehr im Rahmen der zum Zeitpunkt des Abschlusses bestehenden gesetzlichen Regelungen erbracht werden können (somit insb. im Falle einer Änderung der §§ 13, 23 u. 24 KMG 2019).

Übertragungsvereinbarung (Teil II)

gemäß § 13 Abs 3a KMG 2019

§ 1 Begriffsbestimmungen

Im Sinne von Teil II dieser Vereinbarung bezeichnet der Ausdruck

1. **Prospektverordnung:** die Verordnung (EU) 2017/1129 des Europäischen Parlaments und des Rates vom 14. Juni 2017 („PVO“) in der zuletzt geänderten Fassung;
2. **Kapitalmarktgesetz 2019:** das Bundesgesetz über das öffentliche Anbieten von Wertpapieren und anderen Kapitalveranlagungen („KMG 2019“) in der geltenden Fassung;
3. **Datenschutzgrundverordnung:** die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 („DSGVO“) in der geltenden Fassung;
4. **Prospekt:** einen Prospekt gemäß der PVO;
5. **Endgültige Bedingungen:** emissionsspezifische Bedingungen von Emissionen, die unter einem Basisprospekt nach Art 2 lit s der PVO begeben werden („Final Terms“) und gemäß Art 8 Abs 5 PVO originär bei der FMA (siehe aber § 24 Abs 1 KMG 2019) zu hinterlegen sind;
6. **Endgültiger Emissionskurs und Endgültiges Emissionsvolumen:** die Angaben nach Art 17 Abs 1 PVO; sofern nicht im Prospekt genannt, sie sind gemäß Art 17 PVO originär bei der FMA (siehe aber § 24 Abs 1 KMG 2019) zu hinterlegen;
7. **Prospektnachtrag:** einen Nachtrag zum Prospekt gemäß Art 23 PVO;
8. **Prospektersetzende Dokumente:** Informationen, die bei Inanspruchnahme der Ausnahmen nach Art 1 Abs 4 lit f und g und Artikel 1 Abs 5 UntAbs 1 lit e und f PVO vom Emittenten zu veröffentlichen und gemäß Art 21a Abs 1 PVO originär an die FMA zu übermitteln sind;
9. **Unternehmen:** Gemäß Art 21a Abs 1 PVO übermittlungspflichtige Emittenten, Anbieter bzw. die eine Zulassung zum Handel an einem geregelten Markt beantragenden Personen;
10. **ESAP:** European Single Access Point;
11. **ESAP-VO:** die Verordnung (EU) 2023/2859 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 in der geltenden Fassung;
12. **TOM:** Technische und organisatorische Maßnahmen nach DSGVO;
13. **Befugnisempfänger:** die im Sinne von Art 5 Abs 8 PVO von der FMA beauftragte Meldestelle.

§ 2 Gegenstand der Aufgabenübertragung

(1) Sammlung von Informationen nach Art 5 Abs 1 lit a ESAP-VO

Die FMA überträgt der Meldestelle die Entgegennahme der prospektersetzenden Dokumente inklusive der ESAP-spezifischen Metadaten gemäß Art 21a Abs 1 PVO.

Die Meldestelle nützt hierfür gegebenenfalls ihre bestehenden Meldeverfahren und Infrastrukturen im Rahmen ihrer Tätigkeit nach dem KMG 2019.

(2) Speicherung von Informationen nach Art 5 Abs 1 lit b und lit g ESAP-VO

Die FMA überträgt der Meldestelle die Speicherung sämtlicher der ihr aufgrund einer Übertragung nach § 13 Abs 3 KMG 2019 oder nach Art 5 Abs 8 ESAP-VO iVm 21a Abs 1 PVO von Unternehmen übermittelten Informationen.

Für die in Abs 3 lit a und b genannten Informationen gelten Speicherfristen, nach deren Ablauf die Meldestelle die Informationen nicht mehr für die Zwecke der vorliegenden Übertragung (i.e. ESAP-Funktionalitäten) für die FMA zur Verfügung zu halten hat (Speicherfristen-Tabelle Anlage 2).

Die Meldestelle nützt hierfür gegebenenfalls ihre bestehenden Meldeverfahren und Infrastrukturen im Rahmen ihrer Tätigkeit nach dem KMG.

(3) Technische Validierung von Informationen nach Art 5 Abs 1 lit c ESAP-VO

Die FMA überträgt der Meldestelle die technische automatisierte Validierung der von Unternehmen übermittelten Informationen im nachstehend angeführten Umfang:

(a) Prospekte, Prospektnachträge und Registrierungsformulare, die von Unternehmen inklusive der Metadaten nach Art 21a Abs 1 lit b PVO bei der FMA im PDF-Format oder einem anderen nach der PVO oder der Durchführungsverordnung (EU) 2025/1339 der Kommission vom 10. Juli 2025 vorgeschriebenen datenextrahierbaren Format zur Billigung eingereicht und von dieser an die Meldestelle zur Validierung übermittelt werden, sind von der Meldestelle darauf zu prüfen, ob der Dokumenteninhalt datenextrahierbar ist. Ergibt die Prüfung, dass das Dokument nicht gescannt ist (Vorhandensein extrahierbarer Zeichen), kann von einer Verarbeitbarkeit des Textinhalts ausgegangen werden und ist das Dokument von der Meldestelle als datenextrahierbar mit dem Vermerk „formatvalidiert“ (oder einem gleichsinnigen Vermerk) an die FMA zurückzusenden. Andernfalls ist das Dokument als nicht datenextrahierbar mit dem Vermerk „fehlerhaft“ (oder einem gleichsinnigen Vermerk) zurückzusenden.

Eine (etwaige) gegenüber dem Unternehmen zu setzende Maßnahme nach Art 5 Abs 3 ESAP VO (Verwerfen übermittelter Informationen) fällt nicht in den an die Meldestelle übertragenen Aufgabenbereich.

(b) Endgültige Bedingungen nach Art 8 Abs 5 PVO, prospektersetzende Dokumente nach Art 1 Abs 4 lit f u. g und nach Art 1 Abs 5 UAbs 1 lit e u. f PVO, Dokumente mit endgültigen Emissionskursen sowie endgültigen Emissionsvolumina nach Art 17 Abs 2 PVO, die von Unternehmen an die Meldestelle aufgrund des § 24 KMG u./od. einer Übertragungskundmachung der FMA übermittelt werden, sind von der Meldestelle auf Datenextrahierbarkeit (s. lit. a) sowie auf das Vorhandensein der erforderlichen Metadaten nach Art 21a Abs 1 lit b PVO zu prüfen.

(c) Die Meldestelle nützt für die ihr übertragenen Validierungen gegebenenfalls ihre bestehenden Meldeverfahren und Infrastruktur und sieht im Falle fehlerhafter Übermittlungen durch Unternehmen Maßnahmen gemäß Art 5 Abs 3 u 4 ESAP-VO zur Übermittlung berechtigter Informationen vor (zB durch entsprechend konfigurierte Meldefelder).

Soweit ESMA-Vorgaben zur Datenaufbereitung für das Notifikationsportal nach Art 21 Abs 6 (Prospectus Register) oder für die Funktionalitäten des ESAP vorsieht (insb. PRIII Reporting

Instructions, Business Requirements Document der ESMA), werden diese für die Zwecke der Aufgabenübertragung nach lit a und b von der FMA nach Möglichkeit umgehend der Meldestelle mitgeteilt und sind diese, sofern sie im Rahmen der vorliegenden Aufgabenübertragung Deckung finden, zu berücksichtigen.

(4) Unterstützungsleistungen an Unternehmen nach Art 5 Abs 1 lit f ESAP-VO

Die FMA überträgt der Meldestelle, sofern dies im Bereich ihrer technischen Zuständigkeit liegt und soweit es die technische Validierung nach Absatz 3 lit b u. c betrifft, die Aufgabe, den Unternehmen, die die Informationen übermitteln, in Bezug auf das Übermittlungs-, Verwerfungs- und Neuübermittlungsverfahren Unterstützung zu leisten.

§ 3 Bedingungen nach Art 5 Abs 8 ESAP-VO

Die Oesterreichische Kontrollbank nimmt in ihrer Funktion als Meldestelle und Befugnisempfänger zustimmend zur Kenntnis, dass

(a) die von ihr als Befugnisempfänger gemäß der vorliegenden Übertragungsvereinbarung zu erfüllenden Aufgaben keinen Interessenkonflikt zu ihrer sonstigen Geschäftstätigkeit erzeugen dürfen und dass potenzielle künftige Interessenkonflikte nach Möglichkeit zu vermeiden, andernfalls umgehend offenzulegen sind und einen Grund zur außerordentlichen Auflösung der vorliegenden Übertragungsvereinbarung bilden würden;

(b) ausschließlich aufgrund der vorliegenden Übertragungsvereinbarung erlangte Informationen nicht in unangemessener oder wettbewerbswidriger Weise oder für einen anderen als den in der Übertragungsvereinbarung genannten Zweck verwendet werden dürfen;

(c) sie für ein angemessenes Maß an Authentizität, Verfügbarkeit, Integrität und Nichtabstreitbarkeit der an die FMA für Zwecke des ESAP zugänglich gemachten Informationen und ein angemessenes Schutzniveau für personenbezogene Daten zu sorgen hat (Cybersicherheit);

(d) sie die FMA als Sammelstelle regelmäßig über ihre Gesamtbilanz bei der Erfüllung der übertragenen Aufgaben und unverzüglich über jede Verfehlung bei der Erfüllung einer übertragenen Aufgabe zu unterrichten hat.

§ 4 Vergütung

Die aufgrund der vorliegenden Übertragungsvereinbarung erbrachten Aufgaben werden der OeKB als Meldestelle gemäß KMG 2019 übertragen und sind im Rahmen der nach § 23 Abs 1 KMG vorgesehenen Vergütung zu verrechnen. Eine darüberhinausgehende Vergütung durch die FMA findet nicht statt.

§ 5 Haftung

(1) Die Haftung der Vertragsparteien für Schäden aus oder im Zusammenhang mit dem gegenständlichen Vertragsverhältnis wird – mit Ausnahme von Personenschäden – auf Fälle der groben Fahrlässigkeit und des Vorsatzes beschränkt.

(2) Die OeKB haftet nicht für unmittelbare, bzw. mittelbare Folgeschäden. Eine Haftung der OeKB für Schäden Dritter ist ausgeschlossen. Die Haftung der OeKB für Schäden aus dem gegenständlichen Vertragsverhältnis ist im Kalenderjahr insgesamt der Höhe nach mit jenem Betrag begrenzt, welcher der von ihr in dem Schadenseintritt vorangegangenen Kalenderjahr für ihre Tätigkeit als Meldestelle aus dem gegenständlichen Vertragsverhältnis eingehobenen Vergütung entspricht.

(3) Ein Ersatzanspruch besteht nicht, sofern und soweit der geltend gemachte Schaden durch die Einlegung von Rechtsmitteln, durch die Erhebung einer Beschwerde an ein Verwaltungsgericht und Revision an den Verwaltungsgerichtshof oder durch sonstige gesetzlich begründete Maßnahmen hätte abgewendet werden können.

§ 6 Datenschutz

(1) Die Meldestelle verarbeitet personenbezogene Daten zum Zweck des Empfangens, technischen Prüfens, Kennzeichnens und Rückübermittels im Rahmen der Validierung der Datenextrahierbarkeit. Gegenstand der Verarbeitung sind Prospekte, Prospektnachträge, Registrierungsformulare und prospektersetzende Dokumente samt der Metadaten nach Art 21a Abs 1 lit b PVO (im PDF-Format) sowie die darin enthaltenen personenbezogenen Daten; betroffen sind die darin ausgewiesenen natürlichen Personen. Die Dauer der Verarbeitung entspricht der Laufzeit dieser Vereinbarung.

(2) Unbeschadet der Verarbeitung aufgrund ihrer gesetzlichen Verpflichtungen nach dem KMG verarbeitet die Meldestelle die Daten ausschließlich auf dokumentierte Weisung der Sammelstelle – auch im Falle einer Drittlandübermittlung, soweit sie hierzu nicht gesetzlich verpflichtet ist – und informiert die Sammelstelle unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Sie gewährleistet die Vertraulichkeit der befugten Personen, trifft sämtliche Maßnahmen nach Art 32 DSGVO (gemäß TOM; Anlage 4), wahrt die Voraussetzungen für die Beiziehung weiterer Auftragsverarbeiter nach Art 28 Abs 2 und 4 DSGVO und unterstützt die Sammelstelle bei der Erfüllung von Betroffenenanträgen (Art 12-22 DSGVO) sowie bei ihren Pflichten nach Art 32-36 DSGVO. Nach Leistungsende gemäß Anlage 2 löscht sie sämtliche Daten und löscht vorhandene Kopien, soweit keine gesetzliche Speicherpflicht entgegensteht oder keine Speicherung aufgrund der Funktion der Meldestelle nach dem KMG erfolgt. Sie stellt der Sammelstelle alle erforderlichen Nachweise zur Verfügung und ermöglicht Überprüfungen und Inspektionen.



(3) Die Meldestelle darf weitere Auftragsverarbeiter nach Maßgabe der DSGVO beiziehen, sofern sie diesen die gegenständlichen datenschutzrechtlichen Pflichten vollumfänglich überbindet.



§ 7 Inkrafttreten und Beendigung

(1) Die vorliegende Übertragungsvereinbarung tritt mit 10. Juli 2026 in Kraft.

(2) Die vorliegende Übertragungsvereinbarung wird auf unbestimmte Zeit geschlossen und kann von jeder der Parteien durch schriftliche Erklärung gegenüber der jeweils anderen Partei unter Einhaltung einer Frist von zumindest sechs Monaten zum Ende eines jeden Kalenderhalbjahres beendet werden. Das Recht jeder der Parteien auf sofortige Beendigung im Falle eines außerordentlichen Beendigungsgrundes bleibt hierdurch unberührt. Als außerordentlicher Kündigungsgrund gilt für die Meldestelle insbesondere, wenn die ihr übertragenen Aufgaben nicht mehr im Rahmen der zum

Zeitpunkt des Abschlusses bestehenden gesetzlichen Regelungen erbracht werden können (somit insb. im Falle einer Änderung der §§ 13, 23 u. 24 KMG 2019).

Für die Oesterreichische Kontrollbank AG (Meldestelle gem. KMG 2019)	
Mag. Angelika Sommer-Hemetsberger	 25./06/2026
Mag. Maria Kucera	 25./06/2026

Für die Finanzmarktaufsicht FMA	
Mag.a Mariana Kühnel, M.A	 27./7/2026
Mag. Helmut Ettl	 27./7/2026

Anlagen:

- Datenaufbereitung für Veröffentlichungen im ESMA-Notifizierungsportal Vers. 5 samt Anhang (/1)
- Speicherfristen-Tabelle (/2)
- Muster Übertragungsvereinbarung (ad Präambel Pkt iii) (/3)
- OeKB Technische und organisatorische Maßnahmen („TOM“) (/4)

Version 5 (Juli 2026)

**Datenaufbereitung für Veröffentlichungen im ESMA-Notifizierungsportal
gemäß Art 21 Abs 6 und Art 25 Abs 6 PVO**

Allgemeine Vorbemerkung:

Die vorliegenden Festlegungen und Spezifizierungen zur IT Datenaufbereitung basieren auf § 2 Abs 3 der zwischen der Finanzmarktaufsichtsbehörde (idF FMA) und der Oesterreichischen Kontrollbank in ihrer Funktion als Meldestelle gemäß KMG 2019 (idF Meldestelle oder MSt) geschlossenen Übertragungsvereinbarung nach § 13 Abs 3 KMG 2019. Unbeschadet der von der Meldestelle nach den §§ 23 und 24 KMG gesetzlich zu erfüllenden Aufgaben stellen die vorliegenden Festlegungen und Spezifizierungen weder eine Übertragung aufsichtsbehördlicher oder sonstiger hoheitlicher Zuständigkeiten auf die Meldestelle dar, noch fungiert diese als Erfüllungsgehilfe von Meldern gegenüber der FMA. Nicht rechtzeitig oder sonst nicht ordnungsgemäß erfolgende Meldungen nach § 24 KMG liegen daher weiterhin in der alleinigen Verantwortung des jeweiligen Melders bzw. in der ausschließlichen aufsichtsbehördlichen Ermittlungs- und Vollziehungskompetenz der FMA.

Grundlegendes zur Datenaufbereitung durch die Meldestelle

Auslöser eines Datentransfers ist im Falle eines STDA die vollständig eingelangte Meldung zum Emissionskalender nach § 24 KMG 2019, im Falle eines Basisprospekts die vollständig eingelangte Meldung zum Emissionskalender nach § 24 KMG 2019 samt den jeweiligen Endgültigen Bedingungen (FT).

1. Zeitpunkt des Datentransfers und Schnittstellenspezifikationen

1.1 Grundsatz: Ein Datensatz wird, sobald er vollständig bei der MSt vorliegt (dh alle Pflichtfelder (M) befüllt sind) taggleich, spätestens aber am Folgetag (Bankarbeitstag) von MSt an FMA übermittelt.

1.2 DT STDA (Idealfall): 1T nach Erhalt des STDA inkl. NIP bzw. am Tag der Meldung nach § 24 KMG.

Anmerkung: Voraussetzung dafür ist, dass die FMA-Billigung einen Tag vor Angebotsbeginn erfolgt ist und der Melder spätestens am Angebotstag seine Meldung vollständig übermittelt hat.

1.3 DT BP: DT unter einem BP erfolgen mit Einlangen der jeweiligen FT bei der MSt bzw. am Tag der Meldung nach § 24 KMG 2019

Anmerkung: ESMA benötigt KD/FT spätestens 5 Tage nach FT-Hinterlegung.

1.4 Vollständigkeit des Datensatzes: Ein Datensatz gilt als vollständig, sobald zumindest alle Pflichtfelder gemäß Anhang zur vorliegenden Anlage (s. dort jeweils die Kennzeichnung [M]) befüllt sind. Im Falle von Angeboten, die mit der Hinterlegung von Endgültigen Bedingungen einhergehen, müssen auch diese bei der MSt hochgeladen sein, damit der Datensatz als vollständig gilt und an die FMA übermittelt wird.

1.5 Weitere Schnittstellenspezifikationen

Weitere künftige durch ESMA vorgegebene oder sonstige IT-Spezifikationen können erforderlichenfalls, d.h. wenn diese für die FMA u/od MSt nicht selbsterklärend bzw. nicht ohne nähere Festlegung ohne weiteres umzusetzen sind, nach gemeinsamer Abstimmung in den Anhang zu dieser Anlage (Tabelle Annex VII RTS 979) aufgenommen werden.

2. Zu Klassifizierungsdaten

Die Aufbereitung von E-KD durch die MSt umfasst grundsätzlich keine Überprüfung der vom Melder selbst vorgenommenen Zuordnungen (zB Zuordnung einer ISIN zum NIP). Hiervon unberührt bleiben jedoch im Einzelfall ausdrücklich festgelegte Plausibilisierungen gemäß Punkt 4 (s. dort näher die Möglichkeit von Fehlermeldungen, Informationsmeldungen und Auffälligkeiten).

Nähere Auslegungen und Abgrenzungen zu den spezifischen KD enthalten die Anmerkungen zur Tabelle nach Annex VII RTS 979 (siehe Anhang).

3. Zu Emissionskalender-Daten und zur Online-Maske

Neben emissionsbezogenen KD nach RTS 979 erhält die MSt auch weitere auf Grundlage des § 24 KMG gemeldete Daten. Diese überschneiden sich teilweise mit den für das ESMA Notifikationsportal aufzubereitenden Daten, teils handelt es sich aber um eigenständige Angaben. Zum besseren Gesamtverständnis enthalten die nachstehenden Punkte Hinweise zu diesen weiteren Meldefeldern des EmKal.

3.1 Angaben zum Zeitpunkt der Emission nach § 24 Abs 1 KMG

- (i) Angebotsbeginn (M)
- (ii) Zeichnungsbeginn (M)
- (iii) Zeichnungsende (O)
- (iv) Laufzeitbeginn (MR)
- (v) Laufzeitende (MR; Anknüpfung an ESMA-KDs: warning mandatory field)

3.2 Öffentliches/nicht-öffentliches Angebot

Dieses Meldedatum wird nicht mehr (wie noch nach KMG 1992) erhoben, weil es bloß für Prospektpflicht-Prüfung (FMA-Anzeige) erforderlich gewesen ist. Die ESMA-Meldeschieden (Option 1 u. 3) setzen Prospekterstellung voraus, weshalb auch kein Prüferfordernis der MSt mehr besteht. Ferner besteht das E-KD Feld Nr 27, worin nähere Angaben zur Art des Angebots zwingend aufzunehmen sind (s. Anhang)

Meldungen nach Option 2 haben weiterhin die bisherige Angabe zur Öffentlichkeit/Nicht-Öffentlichkeit des Angebots zu enthalten.

3.3 Emissionsvolumen

Die nach § 24 Abs 1 Satz 1 KMG 2019 (neben den KD) geforderte Angabe des Gesamtvolumens wird in Option 1 durch das Feld Nr 25 erfüllt. Soweit das Gesamtvolumen nach § 24 Abs 1 Satz 1 KMG 2019 neben dem Kurswert auch als Nominale verstanden werden kann, lässt es sich aus anderen Angaben nach Option 1 errechnen (Feld 20 und/oder Feld 23).

3.4 Online-Meldemaske

Den Meldefeldern werden, wo zweckmäßig, „mousecovers“ hinzugefügt, die Erläuterungen im Sinne des

Anh VII zum RTS 979 und seiner Spalten „zu meldender Inhalt“ und „Formate und Standards für die Meldung“ ersichtlich machen.

4. Plausibilisierungen von E-KD

Plausibilisierungen von E-KD erfolgen durch die Meldestelle, wenn und soweit solche in einer Anmerkung zu einem Meldefeld der Anlage ausdrücklich als eine der nachstehend bezeichneten Arten von Plausibilisierungen festgelegt werden. Der ausdrücklichen Bezeichnung gleichgestellt ist die Kennzeichnung eines E-KD Datenfeldes als zwingendes Meldefeld „[M]“ (s. näher Punkt 4.1).

Als Arten von Plausibilisierungen kommen in Betracht:

4.1 „Fehlermeldungen“

Alle KD Datenfelder, zu denen eine Fehlermeldung in den Anmerkungen ausdrücklich festgelegt ist oder die mit der Bezeichnung [M] gekennzeichnet sind (s. Anhang) und vom Melder (E-KD) oder für diesen von der OeKB (OeKB-KD) nicht ordnungsgemäß befüllt werden bzw befüllt werden können, führen zu einer Fehlermeldung. Im Falle einer Fehlermeldung kann der Datensatz bei der MSt nicht hochgeladen werden. Die Fehlermeldung wird dem Melder zur Kenntnis gebracht. Die Meldung gilt, solange der Datensatz in der Folge nicht aufgrund der Fehlermeldung vervollständigt wurde, als bei der MSt nicht eingelangt und kann nicht zum Zwecke des Notifikationsportals weitergeleitet werden.

Ausgenommen von der Fehlermeldung sind die zwingenden, aber gemäß FMA-Rechtsansicht nachmeldbaren Angaben des FISN (s. Anhang Feld 16), des CFI (s. Anhang 18) und der FT; dies weil, FISN, CFI und FT nicht notwendiger Weise bereits vor Angebotsbeginn gemäß KMG 2019 feststehen. Der Melder wird bei einer in diesem Sinne unvollständigen Meldung auf die bestehende Nachmeldepflicht hingewiesen (i.e. Fall einer InfoMeldung (s. Pkt 4.2) und es erfolgt für die Zwecke der FMA eine Kennzeichnung als Auffälligkeit (s. Punkt 4.3).

4.2 Informationsmeldungen („InfoMeldung“)

Im Falle einer „InfoMeldung“ zu einem Meldefeld kann der Datensatz ungeachtet der InfoMeldung bei der MSt hochgeladen und an die FMA bzw ESMA weitergeleitet werden. Der Melder wird von der InfoMeldung in Kenntnis gesetzt.

4.3 „Auffälligkeiten“

Im Falle von „Auffälligkeiten“ erfolgt eine Kennzeichnung des hiervon betroffenen Meldefeldes, die von der FMA zum Zwecke allenfalls erforderlicher weiterer Klärungen eingesehen werden kann.

Ob und welche Auffälligkeiten im System der MSt zu implementieren sind, wird im Anhang zu dieser Anlage festgelegt (dies, unbeschadet der bereits gemäß Punkt 4.1 vorgesehenen Kennzeichnung fehlender FT).

Anhang: Tabelle Annex VII RTS 979 (kommentiert).

Legende, Erläuterungen:

BP: Basisprospekt (base prospectus)

DT: Datentransfer MSt an FMA

EmKal alt Emissionskalender in der Konfiguration vor dem 1.12.2020

EmKal Emissionskalender ab dem 1.12.2020

FT:	Endgültige Bedingungen
FTWS	Endgültige Bedingungen einschl. Summary (Feld 5)
MS	Mitgliedstaat
MSt	Meldestelle
KD:	Erforderliche Klassifizierungsdaten nach Art 21 Abs 13 PVO
E-KD:	Emissionsspezifische Klassifizierungsdaten; die vom Melder nach § 24 Abs 1 KMG 2019 zu übermittelnden KD
FMA-KD	Von FMA generierte, an die OeKB übermittelte KD
OeKB-KD	Von OeKB generierte KD
NI:	Nationale Kennung (national identifier);
NIP:	Nationale Kennung des Prospekts
NIS:	Nationale Kennung des Nachtrags
NIFT	Nationale Kennung der endgültigen Bedingungen
Option 1	Meldungen von Angeboten nach Option 1 = FMA-PVO Prospekte
Option 2	Meldungen von Angeboten nach Option 2 = FMA-KMG Pp/Sonst. PVO-Pp/prospfreie Ang/VA
Option 3	Meldungen von Angeboten nach Option 3 = FMA-PVO Prospekte (i) in ausschl. anderen MS (ii) für Zweit-od. Folgeangebote im Inland (iii) für Börszulassungen ohne erstm. inl. Ang
RTS 979	Delegierte Verordnung (EU) 2019/979 der Kommission vom 14. März 2019 zur Ergänzung der Verordnung (EU) 2017/1129 idgF
STDA:	Einzelprospekt (stand alone prospectus)
ToF	ESMA Table of Fields

Erläuterungen:

Die nachstehende Tabelle basiert auf Anhang 7 der DelVO (EU) 2019/979. Den Feldern gemäß DelVO sind Anmerkungen angefügt, die das gemeinsame Verständnis von FMA und OeKB in ihrer Funktion als Meldestelle gem. KMG (idF MSt) bei der Auslegung und Behandlung der Datenfelder kommentieren bzw. festhalten. Der englischen Feldbezeichnung ist jeweils die deutsche Feldbezeichnung in **Fettdruck** hinzugefügt. Die für Melder zum EmKal relevante Feldbezeichnung ist daran anschließend in **Fett-Kursivdruck** angeführt.

Der Nummer des Feldes sind – je nach Quelle (FMA, OeKB oder Melder/Emittent) der von der MSt aufzubereitenden Klassifizierungsdaten (KD) und je nach zwingender oder freiwilliger Übermittlung – Kennzeichnungen hinzugefügt wie folgt:

- Klassifizierungsdaten / Bezeichnung nach Quelle: **FMA-KD, OeKB-KD** oder **E-KD**
- Zwingende Angaben, ohne die keine Meldung abgegeben werden kann bzw. ohne die der XML-Datensatz der FMA nicht in Bearbeitung genommen werden kann (**M [mandatory]**); hierfür sehen die Systeme der MSt technische Vorgaben zur Vollständigkeitsprüfung der Meldung vor.
- Zwingende Angaben, wenn vorhanden (**MR [mandatory, if relevant]**); das Vorhandensein dieser Datenkategorie wird von der MSt nicht geprüft.
- Freiwillige Angaben (**O [optional]**)

Sofern KD zunächst als FMA-KD oder OeKB-KD und sodann auch als E-KD einlangen können, ist beim betreffenden Feld angemerkt, ob die E-KD gegenüber den FMA-KD / OeKB-KD vorgehen (prävalieren) und/oder ob es zu einer Plausibilisierung kommen soll.

Tabelle nach ANNEX VII

MACHINE-READABLE DATA TO BE PROVIDED TO ESMA

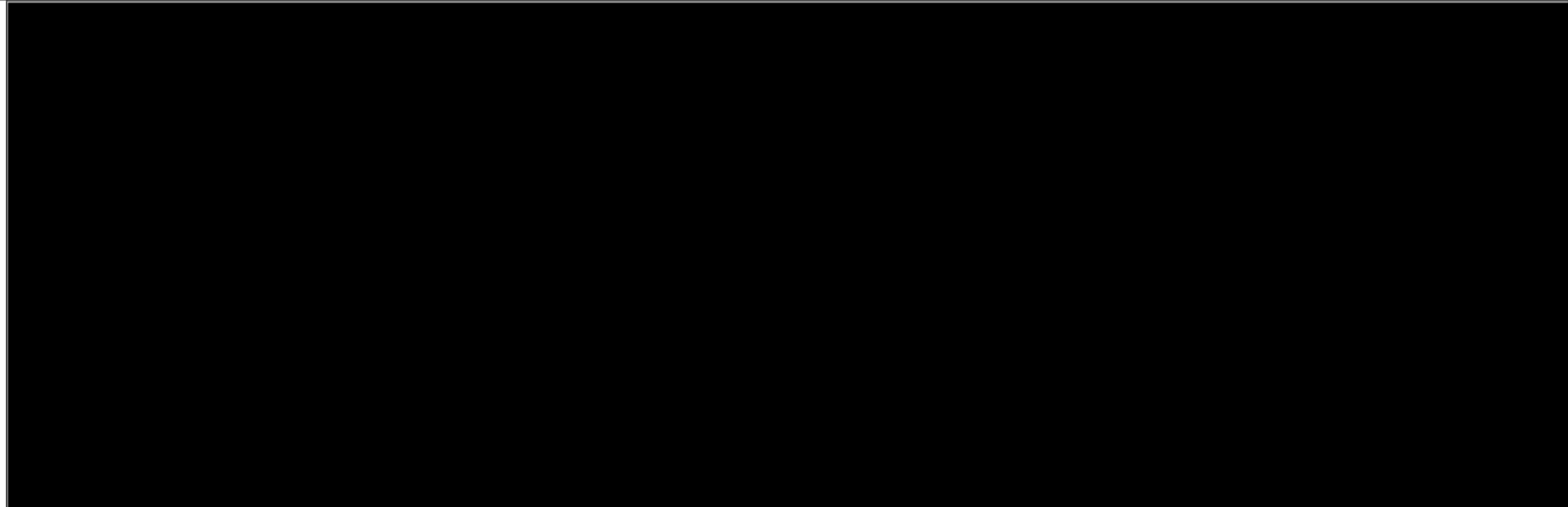
Number	Field	Content to be reported	Format and Standard to be used for reporting
1. [M] FMA-KD [M] OeKB-KD [MR]	National identifier Nationale Kennung	Unique identifier of the uploaded record, assigned by the sending NCA	{ALPHANUM-50}
2. [M] FMA-KD [MR] E-KD [M]	Related national identifier Verbundene nationale Kennung	Unique identifier of the record to which the uploaded record relates, assigned by the sending NCA Not reported in case the related national identifier is not applicable	{ALPHANUM-50}
3. FMA-KD [M] OeKB-KD [MR]	Sending Member State Übermittlender MS	Country code of the Member State which approved the uploaded record or with which the uploaded record was filed	{COUNTRYCODE_2}

4. FMA-KD [MR] E-KD [MR]	<i>Receiving Member State(s)</i> Empfangender MS <i>Empfangender MS</i>	Country code of the Member State(s) to which uploaded record is to be notified or communicated When multiple Member States shall be communicated, field 4 shall be reported as many times as necessary	{COUNTRYCODE_2}

5.[M] FMA-KD [M] OeKB-KD [MR]	Document type Art des Dokuments	The type of uploaded document(s)	Choice from list of predefined fields: — ‘BPFT’ — Base prospectus with final terms — ‘BPWO’ — Base prospectus without final terms — ‘STDA’ — Standalone prospectus — ‘REGN’ — Registration document — ‘URGN’ — Universal registration document — ‘SECN’ — Securities note — ‘FTWS’ — Final terms, including the summary of the individual issue annexed to them — ‘SMRY’ — Summary — ‘SUPP’ — Supplement — ‘SUMT’ — Translation of summary — ‘COAP’ — Certificate of Approval — ‘AMND’ — Amendment — ‘APPT’ — Translation of Appendix (zu RTS-Liste von ESMA ergänzter Dok-Typ) When multiple documents shall be communicated, field [5] shall be reported as many times as necessary to describe each document composing the record
6. FMA-KD [MR]	Structure type Struktur	The format chosen for the prospectus	Choice from list of predefined fields: — ‘SNGL’ — Single document prospectus — ‘SPWS’ — Prospectus consisting of separate documents with summary — ‘SPWO’ — Prospectus consisting of separate documents without summary

7. FMA-KD [M] OeKB_KD [MR]	Approval or filing date Datum der Billigung oder Hinterlegung	The date on which the uploaded record was approved or filed Datum, an dem der hochgeladene Datensatz gebilligt oder hinterlegt wurde	{DATEFORMAT}
8. FMA-KD [M] E-KD [MR]	Language Sprache <i>Sprache</i>	The EU language in which the uploaded record is drafted	{LANGUAGE}
9. FMA-KD [MR] E-KD [MR]	Offeror standardised name Standardisierte Bezeichnung des Anbieters <i>Anbieter, Name</i>	Name and surname of the offeror in case the offeror is a natural person When multiple offerors shall be communicated, field [9] shall be reported as many times as necessary	{ALPHANUM-280}

10. FMA-KD [MR] E-KD [MR]	Guarantor standardised name Standardisierte Bezeichnung des Garantiegebers <i>Garantiegeber</i>	Name and surname of the guarantor in case the guarantor is a natural person When multiple guarantors shall be communicated, field [10] shall be reported as many times as necessary	{ALPHANUM-280}
11. FMA-KD [M] E-KD [M]	Issuer LEI LEI des Emittenten <i>LEI des Emittenten</i>	Legal Entity Identifier of the issuer When multiple issuers shall be communicated, field [11] shall be reported as many times as necessary	{LEI}
12. FMA-KD [MR] E-KD [MR]	Offeror LEI LEI des Anbieters <i>LEI des Anbieters</i>	Legal Entity Identifier of the offeror When multiple offerors shall be communicated, field [12] shall be reported as many times as necessary	{LEI}



13. FMA-KD [MR] E-KD [MR]	Guarantor LEI LEI des Garantiegebers <i>LEI des Garantiegebers</i>	Legal Entity Identifier of the guarantor When multiple guarantors shall be communicated, field [13] shall be reported as many times as necessary	{LEI}
---------------------------------------	---	--	-------



14. FMA-KD [MR]	Offeror residency Wohnsitz des	Offeror's residency in case the offeror is a natural person	{COUNTRYCODE_2}
-----------------------	--	--	-----------------

E-KD [MR]	Anbieters <i>Anbieter, Land</i>	When multiple offerors shall be communicated, field [14] shall be reported as many times as necessary	
15. FMA-KD [MR] E-KD [MR]	Guarantor residency Wohnsitz des Garantiegebers <i>Garantiegeber, Land</i>	Guarantor's residency in case the guarantor is a natural person When multiple guarantors shall be communicated, field [15] shall be reported as many times as necessary	{COUNTRYCODE_2}
Anm: ---			
16.[M] OeKB-KD [MR] E-KD [MR]	FISN	Financial Instrument Short Name of the security This field should be repeated for each ISIN	{FISN}

17. [M] FMA-KD [MR] E-KD [M]	ISIN	International Securities Identification Number	{ISIN}
18 [M]. OeKB-KD [MR] E-KD [MR]	CFI	Classification of Financial Instrument code Klassifizierungscode für Wertpapiere This field should be repeated for each ISIN	{CFI_CODE}
19.[M] OeKB-KD [MR] E-KD [MR]	Issuance currency Währung der Emission	Code representing the currency in which the nominal or notional value is denominated This field should be repeated for each ISIN	{CURRENCYCODE_3}

20. E-KD [M]	Denomination per unit Stückelung <i>Stückelung</i>	Nominal value or notional value per unit in the issuance currency This field should be repeated for each ISIN Field applicable to securities with defined denomination	{DECIMAL-18/5}
21. E-KD [MR]	Identifier or name of the underlying	ISIN code of the underlying security/index or name of the underlying security/index if an ISIN does not exist	For unique underlying: — In case of security or index with existing ISIN: {ISIN} — In case the index has no ISIN: {INDEX} — Otherwise: {ALPHANUM-50}

	Kennung oder Name des Basiswerts	When basket of securities, to be identified accordingly Field applicable to securities with defined underlying. This field should be repeated for each ISIN of such securities	For multiple underlyings (more than one): 'BSKT'
22. E-KD [MR]	Maturity or expiry date Fälligkeitstermin oder Verfalldatum	Date of maturity or expiry date of the security, when applicable This field should be repeated for each ISIN Field applicable to securities with defined maturity	{DATEFORMAT} For perpetual debt securities field 22 should be populated with the value 9999-12-31.
22a.	<i>Laufzeit unbefristet</i>		

23. E-KD [M]	Volume offered Angebotenes Volumen <i>Anzahl der Stücke (bei DW)</i> <i>Nominale in Währung (bei NDW)</i>	Number of securities offered Field applicable only to equity This field should be repeated for each applicable ISIN	{INTEGER-18} Either as single value, range of values, maximum
23a. E-KD [O]	Volume raised Platziertes Volumen		
23b. [MR]	Endgültig angebotenes Emissions-		

	volumen nach Art 17 PVO		
24. E-KD [M]	Price offered Angebotspreis <i>Angebotspreis pro Wertpapier (Erstausgabe- preis)</i>	Price per security offered, in monetary value. The currency of the price is the issuance currency Preis pro angebotenem Wertpapier Field applicable only to equity This field should be repeated for each applicable ISIN	{DECIMAL-18/5} Either as single value, range of values, maximum 'PNDG' in case the price offered is not available but pending 'NOAP' in case the price offered is not applicable



24a. Endgültiger Emissionspreis/-kurs nach Art 17 PVO
Final Offer Price
E-KD
[M]



24b. [O]	Price raised Platzierter Preis		
-------------	--	--	--

25. OeKB-KD [M] E-KD [O]	Consideration offered Angebotener Gegenwert <i>[Gesamtvolumen (Kurswert)]</i>	Total amount offered, in monetary value of the issuance currency This field should be repeated for each ISIN	{DECIMAL-18/5} Either as single value, range of values, maximum ‘PNDG’ in case the consideration offered is not available but pending ‘NOAP’ in case the consideration offered is not applicable
25a. [O]	Consideration raised Platzierter Gegenwert (Kurswert)		

26. E-KD [M]	Type of security Art des Wertpapiers <i>Art des Wertpapiers</i>	Classification of categories of equity and non-equity securities This field should be repeated for each ISIN	Choice from list of predefined fields: Equity — ‘SHRS’: Share — ‘UCEF’: Unit or share in closed end funds — ‘CVTS’: Convertible security — ‘DPRS’: Depository receipt — ‘OTHR’: Other equity Debt —‘DWLD’: Debt with denomination per unit of less than EUR 100 000 —‘DWHD’: Debt with denomination per unit of at least EUR 100 000 —‘DLRM’: Debt with denomination per unit of less than EUR 100 000 traded on a regulated market to which only qualified investors have access to ‘ABSE’: ABS ‘DERV’: Derivative security
--------------------	--	---	--

27. E-KD [M]	Type of offer/admission Art des Angebots / der Zulassung <i>Art des Angebots / der Zulassung</i>	Taxonomy according to PR and MiFID/MIFIR	Choice from list of predefined fields: — ‘IOWA’: Initial offer without admission to trading/listing — ‘SOWA’: Secondary offer without admission to trading/listing — ‘IRMT’: Initial admission to trading on regulated market — ‘IPTM’: Initial admission to trading on regulated market from previously being traded on MTF — ‘IMTF’: Initial admission to trading on MTF with offer to the public — ‘SIRM’: Secondary issuance on a regulated market or MTF
28. E-KD [MR]	Characteristics of the trading venue where the security is initially admitted to trading Merkmale des Handelsplatzes, an dem das Wertpapier erstmals zum Handel zugelassen ist.	Taxonomy according to PR and MiFID/MIFIR	Choice from list of predefined fields: — ‘RMKT’: RM open to all investors — ‘RMQI’: RM, or segment thereof, limited to qualified investors — ‘MSGM’: MTF which is a SME growth market — ‘MLTF’: MTF which is not a SME growth market

29. FMA-KD [MR]	Disclosure regime Offenlegungs- regelung	The annex number in accordance with which the prospectus is drafted under the Commission Delegated Regulation (EU) [] When multiple annexes shall be communicated, field 29 shall be reported as many times as necessary	{INTEGER-2} From 1 to [29]
30. FMA-KD [MR]	EU Growth prospectus category Kategorie des EU- Wachstums- prospekts	Reason based on which an EU Growth prospectus has been used	Choice from list of predefined fields: — ‘S15A’: SME under PR Article 15(1)(a) — ‘I15B’: Issuer other than SME under PR Article 15(1)(b) — ‘I15C’: Issuer other than SME under PR Article 15(1)(c) — ‘O15D’: Offeror of securities under PR Article 15(1)(d)
31. Bail-in ability [E-KD] [M]			

Anlage 2

zur Übertragungsvereinbarung FMA/OeKB

Speicherfristen-Tabelle

Dokumentenart	Frist	zu berechnen ab
Einzelprospekt	10 Jahre gem PVO	ab Veröffentlichung durch Meldestelle nach Art 21 Abs 5 PVO (entspricht Hinterlegungstag FMA an Meldestelle)
Basisprospekt	10 Jahre gem PVO	ab Veröffentlichung durch Meldestelle nach Art 21 Abs 5 PVO (entspricht Hinterlegungstag FMA an Meldestelle)
Einheitliches Registrierungsformular (URD)	mind. 10 Jahre gem PVO	ab Veröffentlichung durch Meldestelle nach Art 21 Abs 5 PVO (entspricht Hinterlegungstag FMA an Meldestelle) mind. 10 Jahre (evtl Verlängerung durch spätere SecNote)
Registrierungsformular (RD)	mind. 10 Jahre gem PVO	ab Veröffentlichung durch Meldestelle nach Art 21 Abs 5 PVO (entspricht Hinterlegungstag FMA an Meldestelle) mind. 10 Jahre (evtl Verlängerung durch spätere SecNote)
Wertpapierbeschreibung	10 Jahre gem PVO	ab Veröffentlichung durch Meldestelle nach Art 21 Abs 5 PVO (entspricht Hinterlegungstag FMA an Meldestelle)
Nachtrag	max. 10 Jahre gem PVO	Rest-Veröffentlichungszeit des zugehörigen Prospekts (zwischen 9 und 10 Jahren)
Final Terms	max. 10 Jahre gem PVO	Rest-Veröffentlichungszeit des zugehörigen Basisprospekts (zwischen 9 und 10 Jahren)
FOPA	max. 10 Jahre gem PVO	Rest-Veröffentlichungszeit des zugehörigen(Basis-)Prospekts (zwischen 9 und 10 Jahren)
EXMP	10 Jahre gem PVO	ab Hinterlegungstag bei Meldestelle

Übertragungsvereinbarung (Teil [●])

gemäß § 13 Abs 3a KMG 2019 iVm Art 5 Abs 8 der Verordnung (EU) 2023/2859 des Europäischen Parlaments und des Rates v. 13.12.2023

§ 1 Begriffsbestimmungen

Im Sinne von Teil [●] dieser Vereinbarung bezeichnet der Ausdruck

1. **ESAP-VO:** Verordnung (EU) 2023/2859 des europäischen Parlaments und des Rates vom 13. Dezember 2023 zur Einrichtung eines zentralen europäischen Zugangsportals für den zentralisierten Zugriff auf öffentlich verfügbare, für Finanzdienstleistungen, Kapitalmärkte und Nachhaltigkeit relevante Informationen.
2. *[Angabe des zur Anwendung kommenden sektoralen Rechtsaktes nach Art 1 Abs 1 lit a ESAP-VO]*
3. *[Angabe zur anwendbaren nationalen Umsetzungs- bzw. Begleitgesetzgebung]*
4. *[Angabe der von der Aufgabenübertragung umfassten Informationen/Dokumente]*
5. **Unternehmen:** Gemäß Artikel *[Bestimmung des sektoralen Rechtsaktes]* übermittlungspflichtige *[Bezeichnung gem. sekt. Rechtsakt, zB Emittenten, Fondsgesellschaft]*
6. **ESAP:** European Single Access Point
7. **Befugnisempfänger:** die im Sinne von Art 5 Abs 8 PVO von der FMA beauftragte Meldestelle
8. **DSGVO:** Datenschutz-Grundverordnung; Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 („DSGVO“) in der geltenden Fassung;

§ 2 Gegenstand der Aufgabenübertragung

(1) Sammlung von Informationen nach Art 5 Abs 1 lit a ESAP-VO

[n.a.]

[Angabe der entgegenzunehmenden Informationen / Metadaten]

[Ggf Angabe der zu nutzenden bestehenden Erhebungsverfahren und -infrastrukturen]

(2) Speicherung von Informationen nach Art 5 Abs 1 lit b und lit g ESAP-VO

[n.a.]

[Angabe der zu speichernden Informationen / Metadaten]

[Spezifikation Speicherfristen / Ablauf der Frist/en, die für die Zurverfügunghaltung der Informationen/Metadaten von der Meldestelle einzuhalten sind]

[Ggf Angabe der zu nutzenden bestehenden Erhebungsverfahren und -infrastrukturen]

(3) Technische Validierung von Informationen nach Art 5 Abs 1 lit c ESAP-VO

[n.a.]

[Die FMA überträgt der Meldestelle die technische automatisierte Validierung der von den Unternehmen übermittelten Informationen im nachstehend angeführten Umfang:]

[Angabe der technischen Validierungen pro Informationsart im Hinblick auf (i) Formatvorgaben (Datenextrahierbarkeit / Maschinenlesbarkeit) und/oder (ii) Metadaten]

[Etwaige gegenüber dem Unternehmen zu setzende Maßnahmen nach Art 5 Abs 3 ESAP-VO (Verwerfen übermittelter Informationen) fallen nicht in den an die Meldestelle übertragenen Aufgabenbereich.]

[Im Falle fehlerhafter Übermittlung durch Unternehmen sieht die Meldestelle Maßnahmen gemäß Art 5 Abs 3 u 4 ESAP-VO zur Übermittlung berichtigter Informationen vor. *Evtl. nähere Spezifikationen*]

[Ggf Angabe der zu nutzenden bestehenden Erhebungsverfahren und -infrastrukturen]

[Ggf Berücksichtigung weiterer ‚Level III Reporting Instructions‘]

(4) Unterstützungsleistungen an Unternehmen nach Art 5 Abs 1 lit f ESAP-VO

[n.a.]

[Die FMA überträgt der Meldestelle, sofern dies im Bereich ihrer technischen Zuständigkeit liegt und soweit es die technische Validierung nach Absatz 3 betrifft, die Aufgabe, den Unternehmen, die die Informationen übermitteln, in Bezug auf das Übermittlungs-, Verwerfungs- und Neuübermittlungsverfahren Unterstützung zu leisten.]

§ 3 Bedingungen nach Art 5 Abs 8 ESAP-VO

Die Oesterreichische Kontrollbank nimmt in ihrer Funktion als Meldestelle und Befugnisempfänger zustimmend zur Kenntnis, dass

- a) die von ihr als Befugnisempfänger gemäß der vorliegenden Übertragungsvereinbarung zu erfüllenden Aufgaben keinen Interessenkonflikt zu ihrer sonstigen Geschäftstätigkeit erzeugen dürfen und dass potenzielle künftige Interessenkonflikte nach Möglichkeit zu vermeiden, andernfalls umgehend offenzulegen sind und einen Grund zur außerordentlichen Auflösung der vorliegenden Übertragungsvereinbarung bilden würden;
- b) ausschließlich aufgrund der vorliegenden Übertragungsvereinbarung erlangte Informationen nicht in unangemessener oder wettbewerbswidriger Weise oder für einen anderen als den in der Übertragungsvereinbarung genannten Zweck verwendet werden dürfen;
- c) sie für ein angemessenes Maß an Authentizität, Verfügbarkeit, Integrität und Nichtabstreitbarkeit der an die FMA für Zwecke des ESAP zugänglich gemachten Informationen und ein angemessenes Schutzniveau für personenbezogene Daten zu sorgen hat (Cybersicherheit);

d) sie die FMA als Sammelstelle regelmäßig über ihre Gesamtbilanz bei der Erfüllung der übertragenen Aufgaben und unverzüglich über jede Verfehlung bei der Erfüllung einer übertragenen Aufgabe zu unterrichten hat.

§ 4 Vergütung

Die aufgrund der vorliegenden Übertragungsvereinbarung erbrachten Aufgaben werden der OeKB als Meldestelle gemäß KMG übertragen und sind im Rahmen der nach § 23 Abs 1 KMG vorgesehenen Vergütung zu verrechnen. Eine darüberhinausgehende Vergütung durch die FMA findet nicht statt.

§ 5 Haftung

(1) Die Haftung der Vertragsparteien für Schäden aus oder im Zusammenhang mit dem gegenständlichen Vertragsverhältnis wird – mit Ausnahme von Personenschäden – auf Fälle der groben Fahrlässigkeit und des Vorsatzes beschränkt.

(2) Die OeKB haftet nicht für unmittelbare, bzw. mittelbare Folgeschäden. Eine Haftung der OeKB für Schäden Dritter ist ausgeschlossen. Die Haftung der OeKB ist im Kalenderjahr insgesamt der Höhe nach mit jenem Betrag begrenzt, welcher der von ihr in dem Schadenseintritt vorangegangenen Kalenderjahr für ihre Tätigkeit als Meldestelle nach dem KMG eingehobenen Vergütung entspricht.

(3) Ein Ersatzanspruch besteht nicht, sofern und soweit der geltend gemachte Schaden durch die Einlegung von Rechtsmitteln, durch die Erhebung einer Beschwerde an ein Verwaltungsgericht und Revision an den Verwaltungsgerichtshof oder durch sonstige gesetzlich begründete Maßnahmen hätte abgewendet werden können.

§ 6 Datenschutz

Die Meldestelle verarbeitet personenbezogene Daten zum Zweck *[des Empfangens, technischen Prüfens, Kennzeichnens und Rückübermittels im Rahmen der Validierung der Datenextrahierbarkeit.]* Gegenstand der Verarbeitung sind [] sowie die darin enthaltenen personenbezogenen Daten; betroffen sind die darin ausgewiesenen natürlichen Personen. Die Dauer der Verarbeitung entspricht der Laufzeit dieser Vereinbarung.

Unbeschadet der Verarbeitung aufgrund ihrer gesetzlichen Verpflichtungen nach dem KMG verarbeitet die Meldestelle die Daten für die Zwecke der vorliegenden Vereinbarung ausschließlich auf dokumentierte Weisung der Sammelstelle – auch im Falle einer Drittlandübermittlung, soweit sie hierzu nicht gesetzlich verpflichtet ist – und informiert die Sammelstelle unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Sie gewährleistet die Vertraulichkeit der befugten Personen, trifft sämtliche Maßnahmen nach Art 32 DSGVO (gemäß TOM Anlage 4) wahrt die Voraussetzungen für die Beiziehung weiterer Auftragsverarbeiter nach Art 28 Abs 2 und 4 DSGVO und unterstützt die Sammelstelle bei der Erfüllung von Betroffenenanträgen (Art 12-22 DSGVO) sowie bei ihren Pflichten nach Art 32-36 DSGVO. Nach Leistungsende löscht oder retourniert sie nach Wahl der Sammelstelle sämtliche Daten und löscht vorhandene Kopien, soweit keine gesetzliche Speicherpflicht entgegensteht oder keine Speicherung aufgrund der Funktion der Meldestelle nach dem KMG erfolgt. Sie stellt der Sammelstelle alle erforderlichen Nachweise zur Verfügung und ermöglicht Überprüfungen und Inspektionen.

Die Meldestelle darf weitere Auftragsverarbeiter nach Maßgabe der DSGVO beiziehen, sofern sie diesen die gegenständlichen datenschutzrechtlichen Pflichten vollumfänglich überbindet.

§ 7 Inkrafttreten und Beendigung

(1) Die vorliegende Übertragungsvereinbarung tritt mit [●] in Kraft.

(2) Die vorliegende Übertragungsvereinbarung wird auf unbestimmte Zeit geschlossen und kann von jeder der Parteien durch schriftliche Erklärung gegenüber der jeweils anderen Partei unter Einhaltung einer Frist von zumindest sechs Monaten zum Ende eines jeden Kalenderhalbjahres beendet werden. Das Recht jeder der Parteien auf sofortige Beendigung im Falle eines außerordentlichen Beendigungsgrundes bleibt hierdurch unberührt. Als außerordentlicher Kündigungsgrund gilt für die Meldestelle insbesondere, wenn die ihr übertragenen Aufgaben nicht mehr im Rahmen der zum Zeitpunkt des Abschlusses bestehenden gesetzlichen Regelungen erbracht werden können (somit insb. im Falle einer Änderung der §§ 13, 23 u. 24 KMG 2019).

Wien, am

Technische und organisatorische Maßnahmen gemäß DSGVO¹

Organisationen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, sind in der gesetzlichen Pflicht, technische und organisatorische Maßnahmen zu treffen, um die Einhaltung der EU-Datenschutzgrundverordnung [DSGVO] sowie anderer Gesetze, welche datenschutzrelevante Vorgaben machen, zu gewährleisten. Für alle Maßnahmen gilt das Prinzip der Verhältnismäßigkeit, d.h. dass ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Zu diesem Zweck werden die nachfolgenden technischen und organisatorischen Maßnahmen (TOMs) zur Prüfung bei den Lieferanten angefragt und deren Antworten einer qualitativen Risiko- und Vollständigkeitsanalyse – auch unter dem Prinzip der Verhältnismäßigkeit der jeweiligen Leistung - unterzogen:

1. Zutrittskontrollen

Es sind folgende Maßnahmen umgesetzt, um den Zutritt Unbefugter zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden, einzuschränken bzw. zu unterbinden. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, (Chipkarten und Transponder), Kontrolle des Zutritts durch Portierdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikation, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken und -räumen zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.:

Technische Maßnahmen	Organisatorische Maßnahmen
- Alarmanlage	- Geregelt Schlüsselverwaltung
- Automatisches Zugangskontrollsystem	- Protokollierung der Zugangsberechtigungen
- Manuelles Schließsystem	- Besucherbuch /Protokollierung der Besucher

¹ In der DSGVO finden sich zentrale Stellen zu den technischen und organisatorischen Maßnahmen (TOMs), insbesondere im Art. 32 DSGVO, welcher die Pflicht beschreibt, TOMs zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus zu treffen. Zudem Art. 28 DSGVO, der festlegt, dass Auftragsverarbeiter technische und organisatorische Maßnahmen umzusetzen und nachzuweisen haben. Und schließlich Art. 25 DSGVO (Privacy by design & Privacy by default), welcher die Umsetzung von Maßnahmen bereits bei der Gestaltung von Verarbeitungsvorgängen vorschreibt, um datenschutzfreundliche Voreinstellungen zu gewährleisten.

Technische Maßnahmen	Organisatorische Maßnahmen
- Sicherheitsschlösser	- Mitarbeiter- /Besucherausweise
Schließsystem mit Codesperre	- Portier / Empfang / Rezeption
Biometrische Zugangssperren	- Zutrittsprotokollierung Mitarbeiter und Besucherkarten
- Chipkarten, Transpondersysteme	- Sorgfalt bei Auswahl des Wachpersonals
Absicherung der Gebäudeschächte	- Sorgfalt bei Auswahl der Reinigungsdienste
- Klingelanlage mit Kamera	- Mind. Jährl. Review der RZ-Zutrittsberechtigungen
- Videoüberwachung bzw. Videoüberwachung der Eingänge (24/7)	- Externe Besuchen/Techniker dürfen sich nur mit Begleitung in den Serverräumen aufhalten!!!
Rechenzentrum: Zutrittsbeschränkung ua. durch Videoüberwachungsanlagen, Alarmanlagen und Sicherheitstüren, Zutritt ausschließlich für autorisierte Personen, Zutrittsprotokollierung, 2 Faktor Authentifizierung	- Zonenkonzept der unterschiedlichen sicherheitsezogenden Levels im Facility Management
- Vereinzelungsanlagen an den jeweiligen Eingangs- und Zutrittspunkten des Gebäudes	
Automat. On-/Off Boarding von Mitarbeitenden	

2. Zugangskontrollen

Es sind folgende Maßnahmen umgesetzt, die verhindern, dass Datenverarbeitungssysteme von Unbefugten benutzt werden können

Mit Zugangskontrolle auf Applikationen und dessen Daten erfolgt in erster Linie über das zentral implementierte Active Directory. Mittels IDM sind Applikationsberechtigungen hierzu anzufordern und müssen durch den verantwortlichen Applikationsowner frei gegeben werden. Mit dieser Implementierung wird die Umsetzung des need-to-know-Prinzips gewährleistet.

Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts):

Technische Maßnahmen	Organisatorische Maßnahmen
- Login mit Benutzername und Passwort	- Berechtigungskonzept und Authentifizierungsverfahren für personenbezogene Benutzererkennung
- Login mit biometrischen Daten	- Richtlinie zur Passwortsicherheit, Benutzerverhalten und Code-of-Conduct für Systemadministratoren
- MFA Login Verwendung	- Zentrale Berechtigungs- und Passwortvergabe
- Firewall	- Passwort-Richtlinie
- IDS, IPS	- Richtlinie Clean Desk
- Netzwerksegmentierung	- Accepted Use Policy (Endgeräte, Mobile Devices, Software)
- Antivirusschutz auf Endgeräten	- Patch Management
- Antivirusschutz auf mobilen Endgeräten	- Richtlinie zur Aktualisierung der Schutzsysteme
- Antivirusschutz auf Server	- Richtlinie zur Desktopsperre bei Abwesenheit
- Anti Malware Systeme auf Endgeräten & Servern	- Unverzögliche Sperre der Berechtigung ausgeschiedener Benutzer
- Schwachstellenmanagement	- Änderungen von Benutzerrechten bei internen Organisationswechsel
- Log Management (Protokollierung der Zugänge (An- und Abmeldung) zu Datenverarbeitungssystemen)	- Kontosperre bei fehlerhaften Zugangsversuchen,
- SIEM/Event Detection & Event Management	- Privacy by Design and Default
- Mobile Device Management	- Security Awareness Schulungen
- Einsatz VPN bei Remote Zugriffen	- Least Privileged und need-to-know
- Verschlüsselung Datenträger	- Wiederkehrende Review der Berechtigungen durch Data-Owner der Fachbereiche
- Verschlüsselung Smartphones	- 24x7 SOC Monitoring und Reaktion
- Bitlocker auf Endgeräten	
- Sperre externer Schnittstellen (USB)	
- Software Whitelisting	
- ID-Austria Verwendung	

3. Zugriffskontrollen

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
- Aktenschredder	- Berechtigungskonzept und Authentifizierungsverfahren für personenbezogene Benutzererkennung
- Einsatz von Dokumentenentsorgungs-Services und externer Aktenvernichter - Versperrte Container	- Prozess zur Beantragung, Genehmigung, Vergabe, Prüfung und Rückgabe von Zugriffsberechtigungen
- Physische Löschung von Datenträgern anhand Verfahren die Nichtwiederherstellbarkeit garantieren	- Differenzierte Berechtigungen (Lesen, Ändern, Profile, Rollen, Transaktionen, Objekte)
- Protokollierung von Zugriffen auf Anwendungen (Eingabe, Änderung, Zugriff und Löschung)	- Meldung und Auswertung erfolgter/versuchter Sicherheitsverletzungen
- Awareness Trainings (zB Phishing Simulation)	- Protokollierung von Datenvernichtung
- Netzwerksegmentierung	- Verpflichtende Schulungen von Mitarbeitenden (zB. zu Information Security, Datenschutz), - Kommunikation geltender Richtlinien an Mitarbeitende. - Audits und Sicherheitsüberprüfungen (zB. Penetration Tests) - Awareness Trainings

4. Trennungskontrollen

Es sind folgende Maßnahmen umgesetzt, die gewährleisten, dass zu unterschiedlichen Zwecken Unternehmensdaten getrennt verarbeitet werden:

Technische Maßnahmen	Organisatorische Maßnahmen
- Trennung von Produktiv- und Test- und Entwicklungsumgebungen	- Steuerung über Berechtigungskonzept - Rollentrennung zwischen Administratoren und Standardusern,

Technische Maßnahmen	Organisatorische Maßnahmen
- Physikalische Trennung (Systeme, DBs, Datenträger)	- Steuerung über Berechtigungskonzept - Berechtigungskonzept für Zugriff auf Daten
- Mandantenfähigkeit relevanter Anwendungen	- Steuerung über Berechtigungskonzept - Festlegung von Datenbankrechten
- Netzwerksegmentierung	- Datensätze sind mit Zweckattributen versehen
	- keine Mitbenutzung der Büroräume und Archive durch Fremdfirmen
	- getrennte Speicherung besonders sensibler Daten (Personalbereich),

5. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

5.1 Weitergabekontrollen

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
- Email-Verschlüsselungen	- Dokumentation der Datenempfänger, sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Email-Signatur	- Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- Einsatz von VPN	- Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
- Datenübertragung über verschlüsselte Verbindungen (VPN; HTTPS, SFTP, etc.	- Persönliche Übergabe mit Protokoll
- Protokollierung der Zugriffe und Abrufe	- Grundsätzliche Protokollierung und Überwachung von Datenübertragungen
- Sichere Transportbehälter	- Getrennte Übergabe der Credential-Bestandteile
- Bereitstellung über verschlüsselte Verbindungen	
- Nutzung von Signaturverfahren	

-
- MFA für Externe bei personenbezogenen Remote-Zugriff in das OeKB Netzwerk
-
- MFT für sicheren Datenaustausch an Berechtigte
-
- Verwendung ID-Austria für
-

5.2 Eingabekontrollen

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"> - Technische Protokollierung der Eingabe, Änderung, Ansicht und Löschung von Daten 	<ul style="list-style-type: none"> - Berechtigungskonzept und Authentifizierungsverfahren für personenbezogene Benutzererkennung
<ul style="list-style-type: none"> - Speicherung der Audit-Logs der Anwendungen 	<ul style="list-style-type: none"> - Risikobasiertes 4-Augen-Prinzip bei Datenänderungen, -lösungen
<ul style="list-style-type: none"> - Pflichtfelder bei der Eingabe von Daten inkl. der Vorgabe von Feldformaten bzw. Bandbreiten der Eingabewerte 	<ul style="list-style-type: none"> - Übersicht der Datenklassifizierung und Anwendungskatalog
	<ul style="list-style-type: none"> - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitung übernommen wurden
	<ul style="list-style-type: none"> - Klare Zuständigkeiten für Datenowner

6. Verfügbarkeits- und Belastbarkeitskontrollen (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Beispielsweise Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
- Feuer- und Rauchmeldeanlagen	- Backup- und Recovery Konzept vorliegend
- Feuerlöscher/System RZ/Serverraum	- Kontrolle des Sicherungsvorgangs
- Serverraumüberwachung – Temperatur & Feuchtigkeit	- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Serverraum klimatisiert	- Geschäftskontinuitätspläne für Krisen- und Notfallsituationen
- Einsatz eines 7x24h Security Operation Centers	- Krisen-/Notfallprozesse und Systeme werden regelmäßig nach dem Back-up und Recovery Konzepten getestet,
- Einsatz von regelmäßige Backup-Mechanismen zur Wiederherstellung von Daten und Services,	- Belastbarkeit der Systeme wird durch mindestens jährlich durchgeführte Tests (zB. penetration, portscan, stress) verifiziert
- Einsatz von USV & Generatoren	- Security Hardening Prozesse
- Redundante Netzwerkverbindungen	-
- Videoüberwachung Serverräume	-
- Monitoring-Framework für die Überwachung des Betriebs von Applikationen und Infrastruktur	-

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Die Wirksamkeit der festgelegten Maßnahmen zur dauerhaften Gewährung der Sicherheit für die Datenverarbeitung personenbezogener Daten wird durch laufende Überprüfungen, Bewertungen, Kontrollen/Monitoring und Evaluierungen sichergestellt.

7.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
- Software-Lösungen für Datenschutz-Management im Einsatz	- Interner/externer Datenschutzbeauftragter

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"> - Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf und Berechtigung 	<ul style="list-style-type: none"> - Mitarbeiter geschult und auf Vertraulichkeit und Geheimhaltung verpflichtet
<ul style="list-style-type: none"> - Sicherheitszertifizierungen nach ISO 27001, BSI IT-Grundschutz, CISIS12 oder ähnliche Bzw. alternatives Informationssicherheitskonzept 	<ul style="list-style-type: none"> - Regelmäßige Sensibilisierung der Mitarbeiter (mindestens einmal jährlich)
<ul style="list-style-type: none"> - Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens einmal jährlich durchgeführt 	<ul style="list-style-type: none"> - Interner/externer Informationssicherheitsbeauftragter
	<ul style="list-style-type: none"> - Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt nach Art. 35 EU-DSGVO
	<ul style="list-style-type: none"> - Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	<ul style="list-style-type: none"> - Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
	<ul style="list-style-type: none"> - Unternehmensrichtlinien zum Datenschutz

7.2 IT Security Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"> - Einsatz von Firewalls 	<ul style="list-style-type: none"> - Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen vorhanden
<ul style="list-style-type: none"> - Einsatz von IDS 	<ul style="list-style-type: none"> - Dokumentierter Prozess zur Vorgehensweise zum Umgang mit Sicherheitsvorfällen vorhanden
<ul style="list-style-type: none"> - Einsatz von IPS 	<ul style="list-style-type: none"> - Dokumentation von Sicherheitsvorfällen via ITSM/Ticket Tools
<ul style="list-style-type: none"> - Einsatz von Malware und Antivirenscoannern 	<ul style="list-style-type: none"> - Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen
<ul style="list-style-type: none"> - Einsatz von EDR Systemen 	
<ul style="list-style-type: none"> - Einsatz von SOC 	

7.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design/ Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
<ul style="list-style-type: none"> - Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen 	<ul style="list-style-type: none"> - Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

7.4 Auftragskontrollen (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	<ul style="list-style-type: none"> - Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation im Rahmen des Lieferantenmanagements
	<ul style="list-style-type: none"> - Sorgfältige Auswahl von (Sub-)Auftragsverarbeitern nach Datensicherheitsgarantien,
	<ul style="list-style-type: none"> - Dienstleister werden vertraglich umfassend zur Geheimhaltung verpflichtet,
	<ul style="list-style-type: none"> - Abschluss von Auftragsverarbeitungsverträgen bzw. zur notwendigen Vereinbarungen nach EU Standard Vertragsklauseln
	<ul style="list-style-type: none"> - Regelungen zum Einsatz von Subunternehmern,
	<ul style="list-style-type: none"> - Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	<ul style="list-style-type: none"> - Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	<ul style="list-style-type: none"> - Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
	<ul style="list-style-type: none"> - Verpflichtung zur Vernichtung von Daten nach Vertragsbeendigung