					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII07					Dokumentum címe: **Adatvédelmi kockázatértékelési és DPIA-szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/kontroll/cikk	Alkalmazhatóság	Lefedettség típusa	Megjegyzés
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS-kockázatok és -lehetőségek
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Adatvédelmi kockázatértékelés
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Adatvédelmi kockázatkezelés és SoA-kapcsolódás
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Tervezett PIMS-változtatások és kockázati újraértékelés
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Adatvédelmi kockázatra és DPIA-ra vonatkozó dokumentált információk
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Működéstervezés és -szabályozás
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operatív adatvédelmi kockázatértékelés
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operatív adatvédelmi kockázatkezelés
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Adatvédelmi kockázatok nyomon követése és mérése
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Adatvédelmi kockázatok vezetőségi felülvizsgálata
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Kockázattal kapcsolatos meg nem felelés és helyesbítő intézkedés
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Adatvédelmi hatásvizsgálat
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	A kockázatértékelést támogató

				adatkezelési nyilvántartások
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Adatfeldolgozói ügyfélmegállapodás és DPIA-támogatás
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Az ügyfél megfelelését támogató adatfeldolgozói információk
GDPR	Article 5(2)	Controller	Supporting	Elszámoltathatósági bizonyítékok
GDPR	Article 24	Controller	Supporting	Az adatkezelő felelőssége és intézkedései
GDPR	Article 25	Controller	Supporting	Beépített és alapértelmezett adatvédelem
GDPR	Article 28	Both	Supporting	Adatfeldolgozói segítségnyújtás és utasítások
GDPR	Article 30	Both	Supporting	A DPIA-t támogató adatkezelési nyilvántartások
GDPR	Article 32	Both	Supporting	Biztonsági kockázatok és védelmi intézkedések
GDPR	Article 35	Controller	Primary	Adatvédelmi hatásvizsgálat
GDPR	Article 36	Controller	Primary	Előzetes konzultáció
GDPR	Article 39	Conditional	Supporting	DPO-tanácsadás és nyomon követés, ahol alkalmazandó
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Adatvédelmi kontrollok, információbiztonság és adatvédelmi megfelelés
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA hatálya, előnyei, kiváltó feltétele és előkészítése

ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII-védelmi program és követelmények azonosítása
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Szervezeti adatvédelmi kockázatkezelési integráció

1. Hatály

1.1 Ez a szabályzat meghatározza a PIMS alkalmazási területén belüli PII-kezelésre vonatkozó adatvédelmi kockázatértékelés, DPIA-előszűrés, teljes DPIA-végrehajtás, kockázatkezelés, maradványkockázat-elfogadás, konzultáció, felülvizsgálat és bizonyítékkezelés követelményeit.

1.2 Ez a szabályzat az alábbiakra alkalmazandó:

1.2.1 új és lényegesen módosított PII-kezelési tevékenységek;

1.2.2 adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói adatkezelési kontextusok;

1.2.3 rendszerek, alkalmazások, szolgáltatások, üzleti folyamatok, beszállítók, adatfeldolgozók, al-adatfeldolgozók, nemzetközi adattovábbítások és adatmegosztási megállapodások, amelyek érintik a PII-kezelést;

1.2.4 a REG04-ben fenntartott adatvédelmi kockázati és DPIA-bizonyítékok, valamint a REG02, REG03, REG08, REG09, REG10, REG11 és REG12 alatt fenntartott támogató bizonyítékok.

1.3 Ez a szabályzat nem helyettesíti az adatkezelési tevékenységek nyilvántartására, az adatvédelmi tájékoztatókra, a hozzájárulásra, a PII-alanyok jogaira, a beépített adatvédelemre, a beszállítókra, a nemzetközi adattovábbításokra, a PII-biztonságra, az incidensekre, a dokumentált információkra vagy a nyomon követésre/auditra/fejlesztésre vonatkozó kontrollokat. Ezeket a követelményeket a 12. szakaszban felsorolt kapcsolódó szabályzatok határozzák meg.

1.4 E szabályzat alkalmazásában az adatvédelmi kockázatértékelés a PII-kezelésből eredő potenciális kedvezőtlen adatvédelmi hatások dokumentált azonosítását, elemzését, értékelését, kezelését, felülvizsgálatát és nyomon követését jelenti.

1.5 E szabályzat alkalmazásában a DPIA olyan dokumentált értékelést jelent, amelyet olyan adatkezelői adatkezeléshez alkalmaznak, amely valószínűsíthetően magas kockázattal jár a PII-alanyokra nézve, és amely értékeli az adatkezelés szükségességét, arányosságát, kockázatait, védelmi intézkedéseit, maradványkockázatát, konzultációs szükségleteit és jóváhagyási feltételeit.

1.6 E szabályzat alkalmazásában a magas maradvány adatvédelmi kockázat olyan adatvédelmi kockázatot jelent, amely a javasolt vagy végrehajtott kockázatkezelés után is meghaladja a jóváhagyott elfogadási küszöbértéket.

1.7 E szabályzat alkalmazásában lényeges változásnak minősül minden olyan változás, amely érinti a PIMS alkalmazási területét, az adatkezelés célját, a jogalapot, a PII-kategóriákat, a PII-alany kategóriáit, az adatkezelés volumenét, az adatkezelési technológiát, a megfigyelést vagy profilalkotást, az automatizált döntéshozatalt, a sérülékeny PII-alanyokat, a címzetteket, az adatfeldolgozókat, az al-adatfeldolgozókat, a nemzetközi adattovábbításokat, a megőrzést, a biztonsági kontrollokat, a kockázati profilt, az ügyfélutasításokat vagy a tanúsítási hatályt.

2. Cél

2.1 E szabályzat célja annak biztosítása, hogy az adatvédelmi kockázatokat és a DPIA-kötelezettségeket azonosítsák, értékeljék, kezeljék, jóváhagyják, felülvizsgálják és bizonyítékokkal alátámasszák, mielőtt a PII-kezelés elfogadhatatlan kockázatot hozna létre a PII-alanyokra vagy a PIMS-re nézve.

2.2 Ez a szabályzat lehetővé teszi a szervezet számára a kockázatalapú adatvédelmi irányítás, az adatkezelői DPIA-elszámoltathatóság, az adatfeldolgozói DPIA-támogatás, a dokumentált kockázatkezelés, a maradványkockázat jóváhagyása, az előzetes konzultációra vonatkozó döntéshozatal és az adatvédelmi kontrollok folyamatos fejlesztésének igazolását.

3. Célkitűzések

3.1 E szabályzat célkitűzései a következők:

3.1.1 a kötelező adatvédelmi kockázati előszűrési kiváltó feltételek meghatározása;

3.1.2 annak meghatározása, hogy mikor szükséges teljes DPIA;

3.1.3 annak biztosítása, hogy az adatkezelői DPIA-döntések dokumentáltak és felülvizsgálhatók legyenek;

3.1.4 annak biztosítása, hogy az adatfeldolgozói és al-adatfeldolgozói DPIA-támogatás dokumentált legyen, ahol azt ügyfélutasítás vagy megállapodás előírja;

3.1.5 annak biztosítása, hogy az adatvédelmi kockázatokat az új vagy lényegesen módosított PII-kezelés megkezdése előtt értékeljék;

3.1.6 annak biztosítása, hogy az adatvédelmi kockázatkezeléseket kijelöljék, végrehajtsák és ellenőrizzék;

3.1.7 annak biztosítása, hogy a magas maradvány adatvédelmi kockázatokat az adatkezelés megkezdése vagy folytatása előtt eszkalálják és jóváhagyják;

3.1.8 annak biztosítása, hogy az előzetes konzultációra vonatkozó döntések dokumentáltak legyenek, ahol magas maradványkockázat áll fenn;

3.1.9 annak biztosítása, hogy az adatvédelmi kockázati és DPIA-bizonyítékokat a REG04-ben tartsák fenn, és kapcsolják a kapcsolódó bizonyítékobjektumokhoz;

3.1.10 annak elkerülése, hogy a REG04-en kívül külön DPIA-, kockázati vagy konzultációs nyilvántartások jöjjenek létre.

4. Szabályzati előírások

4.1 Adatvédelmi kockázati előszűrés

4.1.1 [Both] The Process Owner / Business Owner köteles adatvédelmi kockázati előszűrést kezdeményezni a REG04-ben, mielőtt a REG02-ben rögzített új vagy lényegesen módosított PII-kezelés megkezdődik.

4.1.2 [Both] The Privacy Lead / PIMS Manager köteles az adatvédelmi kockázati előszűrés kritériumait a REG04-ben fenntartani a PIMS első működése előtt, majd azt követően évente.

4.1.3 [Controller] The Process Owner / Business Owner köteles a DPIA-előszűrést a REG04-ben elvégezni, mielőtt az adatvédelmi kockázati előszűrési kritériumoknak megfelelő adatkezelői adatkezelés megkezdődik.

4.1.4 [Processor] The Vendor / Procurement Owner köteles az ügyfél DPIA-támogatási követelményeit a REG08-ban rögzíteni az adatfeldolgozói adatkezelés megkezdése előtt, ha az ügyfélmegállapodás vagy dokumentált utasítás DPIA-támogatást ír elő.

4.1.5 [Both] The System Owner / Application Owner köteles rendszertervezési, hozzáférési, biztonsági, naplózási és adatáramlási bizonyítékokat biztosítani a REG04-ben az új vagy lényegesen módosított, PII-t kezelő rendszerek adatvédelmi kockázatértékelésének jóváhagyása előtt.

4.1.6 [Both] The Privacy Lead / PIMS Manager köteles az előszűrés eredményét és a teljes DPIA-ra vonatkozó döntés indokolását a REG04-ben rögzíteni az adatkezelési tevékenység folytatása előtt.

4.2 DPIA-kiváltó feltételek és követelménymeghatározás

4.2.1 [Controller] The Privacy Lead / PIMS Manager köteles teljes DPIA-t előírni a REG04-ben, mielőtt a valószínűsíthetően magas kockázattal járó adatkezelői adatkezelés megkezdődik.

4.2.2 [Controller] The Process Owner / Business Owner köteles a nagy volumenű, szisztematikus megfigyeléssel, profilalkotással, automatizált döntésekkel, különleges kategóriájú PII-vel, büntetőítéletekre vagy bűncselekményekre vonatkozó adatokkal, sérülékeny PII-alanyokkal, innovatív technológiával vagy lényegesen módosított adatkezeléssel járó adatkezelést a REG04-ben a The Privacy Lead / PIMS Manager elé utalni az adatkezelés megkezdése előtt.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor köteles tanácsát a REG04-ben rögzíteni a magas kockázatú adatkezelői adatkezelésre vonatkozó teljes DPIA-követelményről szóló döntés jóváhagyása előtt.

4.2.4 [Both] The Process Owner / Business Owner köteles az adatvédelmi kockázatot a REG04-ben újra előszűrni, mielőtt a PII-t új célra használják, új címzettet adnak hozzá, új adatfeldolgozót vagy al-adatfeldolgozót vezetnek be, módosítják a rendszerarchitektúrát, vagy új nemzetközi adattovábbítást indítanak.

4.2.5 [Processor] The Privacy Lead / PIMS Manager köteles a REG08-ban dokumentálni, hogy szükséges-e adatfeldolgozói DPIA-támogatás, az ügyfél DPIA-támogatási kérelmének kézhezvételétől számított 10 munkanapon belül.

4.2.6 [Subprocessor] The Vendor / Procurement Owner köteles a REG08-ban dokumentálni az upstream DPIA-támogatási követelményeket az al-adatfeldolgozás megkezdése előtt, ha az upstream ügyfél vagy adatfeldolgozói megállapodás ilyen támogatást ír elő.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Kivételek

9.1 Adatvédelmi kockázati és DPIA-kivételek

9.1.1 [All] The Process Owner / Business Owner köteles a jelen szabályzat alóli bármely kivételt a REG12-ben kérelmezni az eltérés bekövetkezése előtt.

9.1.2 [All] The Privacy Lead / PIMS Manager köteles minden kérelmezett kivétel adatvédelmi, jogi, tanúsítási, működési és PII-alanyokra gyakorolt hatását a REG04-ben vagy a REG12-ben értékelni a kérelemtől számított 10 munkanapon belül.

9.1.3 [All] The Data Protection Officer / Privacy Advisor köteles tanácsát a REG12-ben rögzíteni minden olyan kivétel jóváhagyása előtt, amely magas kockázatú adatkezelést, teljes DPIA elvégzését, előzetes konzultációt, magas maradvány adatvédelmi kockázatot vagy ügyfél DPIA-támogatást érint.

9.1.4 [All] Top Management köteles a magas kockázatú adatkezelést, tanúsítási hatályt, előzetes konzultációt vagy megoldatlan magas maradvány adatvédelmi kockázatot érintő adatvédelmi kockázati vagy DPIA-kivételeket a REG12-ben jóváhagyni, mielőtt a kivétel hatályba lép.

9.1.5 [All] The Privacy Lead / PIMS Manager köteles minden jóváhagyott adatvédelmi kockázati vagy DPIA-kivételhez a jóváhagyás előtt legfeljebb 90 napos lejárati dátumot beállítani a REG12-ben.

9.1.6 [All] The Process Owner / Business Owner köteles minden adatvédelmi kockázati vagy DPIA-kivételt a lejárattól számított öt munkanapon belül a REG12-ben lezárni vagy újraértékelni.

10. Betartatás

10.1 Adatvédelmi kockázati és DPIA-betartatás

10.1.1 [All] The Privacy Lead / PIMS Manager köteles a hiányzó, pontatlan, hiányos, késedelmes vagy jóvá nem hagyott REG04 adatvédelmi kockázati vagy DPIA-bizonyítékot a REG12-ben meg nem felelésként rögzíteni az azonosítástól számított öt munkanapon belül.

10.1.2 [Controller] The Process Owner / Business Owner köteles felfüggeszteni az új magas kockázatú adatkezelői adatkezelést, ha a szükséges REG04 DPIA-jóváhagyási bizonyíték hiányzik az indulás előtt.

10.1.3 [Both] The System Owner / Application Owner köteles blokkolni a PII-t kezelő rendszerek éles indulását, ha a szükséges REG04 kockázatkezelési bizonyíték hiányzik az éles indulás jóváhagyása előtt.

10.1.4 [Both] The Vendor / Procurement Owner köteles blokkolni a beszállítói, adatfeldolgozói, al-adatfeldolgozói vagy adatmegosztási beléptetést, ha a szükséges REG04 adatvédelmi kockázati vagy DPIA-támogatási bizonyíték hiányzik a megállapodás jóváhagyása előtt.

10.1.5 [All] Top Management köteles a vezetőségi felülvizsgálat során a REG12-ben áttekinteni a megoldatlan jelentős adatvédelmi kockázati vagy DPIA-meg nem feleléseket.

10.1.6 [All] The Privacy Lead / PIMS Manager köteles az ismétlődően elmulasztott REG04-előszűrési, DPIA-felülvizsgálati vagy kockázatkezelési határidőket a REG12-ben Top Management felé eszkalálni a 12 hónapos időszakon belüli második előfordulást követő öt munkanapon belül.

10.1.7 [All] The Internal Audit / Compliance Reviewer köteles az adatvédelmi kockázati és DPIA-meg nem felelésekre vonatkozó helyesbítő intézkedések eredményességét a REG12-ben ellenőrizni a következő ütemezett audit során vagy a lezárástól számított 60 napon belül, attól függően, melyik következik be előbb.

11. Felülvizsgálat és karbantartás

11.1 Szabályzat felülvizsgálata és karbantartása

11.1.1 [All] The Privacy Lead / PIMS Manager köteles ezt a szabályzatot a REG12-ben évente, valamint az adatvédelmi kockázatot, DPIA-t, előzetes konzultációt, adatfeldolgozói segítségnyújtást vagy tanúsítási követelményeket érintő lényeges változástól számított 30 napon belül felülvizsgálni.

11.1.2 [All] The Privacy Lead / PIMS Manager köteles a REG04-előszűrési kritériumokat, a DPIA-kiváltó kritériumokat, a kockázati besorolási kritériumokat és a maradványkockázat-elfogadási kritériumokat a REG12-ben évente felülvizsgálni.

11.1.3 [All] The Data Protection Officer / Privacy Advisor köteles a jelen szabályzat adatvédelmi szempontból jelentős módosításait a REG12-ben felülvizsgálni a jóváhagyás előtt.

11.1.4 [All] Top Management köteles a jelen szabályzat lényeges módosításait a REG12-ben jóváhagyni a közzététel előtt.

11.1.5 [All] The Privacy Lead / PIMS Manager köteles a REG03-at és a REG04-et 15 munkanapon belül frissíteni az olyan jóváhagyott szabályzatmódosítások után, amelyek megváltoztatják a kontrollok alkalmazhatóságát, a kockázati kritériumokat vagy a DPIA-előszűrési követelményeket.

11.1.6 [All] The Privacy Lead / PIMS Manager köteles a jelen szabályzat jóváhagyott módosításainak kommunikálását a REG11-ben rögzíteni a közzétételtől számított 30 napon belül.

12. Kapcsolódó szabályzatok

12.1 E szabályzatot az alábbi kapcsolódó szabályzatok támogatják:

12.2 PII01 - Privacy Information Management System szabályzat

12.3 PII02 - Adatvédelmi szerepkörök, felelősségek és elszámoltathatóság szabályzata

12.4 PII03 - PII adatkezelési tevékenységek nyilvántartása és jogalap szabályzat

12.5 PII04 - Adatvédelmi tájékoztató és átláthatóság szabályzata

12.6 PII05 - Hozzájárulás- és preferenciakezelési szabályzat

12.7 PII06 - PII-alanyok jogainak kezelésére vonatkozó szabályzat

12.8 PII08 - Beépített és alapértelmezett adatvédelem szabályzata

12.9 PII09 - PII gyűjtési, felhasználási, közlési és megosztási szabályzata

12.10 PII10 - PII megőrzési, törlési és megsemmisítési szabályzata

12.11 PII11 - PII pontossági és minőségi szabályzata

12.12 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik fél adatvédelmi kezelési szabályzata

12.13 PII13 - Nemzetközi PII-továbbítási szabályzat

12.14 PII14 - PII-biztonsági és hozzáférés-szabályozási szabályzat

12.15 PII15 - PII incidens- és adatsértés-kezelési szabályzat

12.16 PII17 - PIMS dokumentált információk és bizonyítékkezelési szabályzat

12.17 PII18 - PIMS nyomon követési, audit- és fejlesztési szabályzat

13. Hivatkozott szabványok és keretrendszerek

13.1 Ez a szabályzat az alábbi szabványokhoz és jogszabályokhoz van hozzárendelve. A megfeleltetés bemutatja, hogy a szabályzat miként támogatja a hivatkozott követelményeket, és azonosítja azokat a belső pontokat, amelyek végrehajtják vagy támogatják azokat.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Az adatvédelmi kockázatokra és lehetőségekre vonatkozó intézkedések azonosításához és tervezéséhez kapcsolódik előszűrési kritériumok, kockázati küszöbértékek, eszkaláció és vezetőségi felülvizsgálati bemenetek alkalmazásával. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Az adatvédelmi kockázati előszűrés, adatvédelmi kockázatértékelés, kockázati besorolás, újraértékelés és DPIA-kiváltó feltételek értékelésének elvégzéséhez kapcsolódik, mielőtt az új vagy lényegesen módosított adatkezelés folytatódik. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Az adatvédelmi kockázatkezelési tervezéshez, a kontrollalkalmazhatósági frissítésekhez, a kockázatkezelés végrehajtásához, a maradványkockázat elfogadásához és az SoA-kapcsolódáshoz kapcsolódik. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - A tervezett PIMS- és adatkezelési változásokhoz kapcsolódik, amelyek adatvédelmi kockázati újraértékelést és DPIA-felülvizsgálatot váltanak ki. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Az adatvédelmi kockázati előszűrés, DPIA-bizonyítékok, kockázatkezelés, maradványkockázat-elfogadás, előzetes konzultációs döntések, kivételek, meg nem felelések és szabályzat-felülvizsgálati bizonyítékok kontrollált dokumentált információihoz kapcsolódik. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Az adatvédelmi kockázati és DPIA-kontrollok működtetéséhez kapcsolódik az éles indulás, beléptetés, adatkezelési jóváhagyás, kockázatkezelési lezárás és helyesbítő intézkedéshez kapcsolás előtt. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Az új, módosított, rendszerrel, beszállítóval, adattovábbítással és incidenssel vezérelt adatkezelési változások operatív adatvédelmi kockázatértékeléséhez kapcsolódik. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Az operatív adatvédelmi kockázatkezeléshez, a kockázatkezelés kijelöléséhez, végrehajtásához, a késedelmes kockázatkezelés eszkalációjához és az eredményesség ellenőrzéséhez kapcsolódik. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Az előszűrési lefedettség, a DPIA-státusz, a nyitott kockázatok, a lejárt határidejű kockázatkezelési intézkedések, a beszállítói intézkedések, a biztonsági kockázatkezelési intézkedések, az incidens-újraértékelési intézkedések és az

auditmegállapítások nyomon követéséhez és méréséhez kapcsolódik. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - A magas maradvány adatvédelmi kockázatok, a lejárt határidejű kockázatkezelési intézkedések, a teljes DPIA-státusz, az előzetes konzultációs döntések és a jelentős adatvédelmi kockázati kivételek vezetőségi felülvizsgálatához kapcsolódik. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Az adatvédelmi kockázati és DPIA-meg nem felelésekhez, kivételekhez, helyesbítő intézkedés megnyitásához, eszkalációhoz és eredményességi ellenőrzéshez kapcsolódik. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Az új vagy módosított adatkezelői adatkezeléshez kapcsolódó adatvédelmi hatásvizsgálat szükségességének értékeléséhez és szükség szerinti végrehajtásához kapcsolódik. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Az adatvédelmi kockázati és DPIA-értékelési bemeneteket támogató adatkezelési nyilvántartásokhoz kapcsolódik, beleértve a célt, kategóriákat, rendszereket, címzetteket, adattovábbításokat és beszállítókat. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Az adatfeldolgozói ügyfélmegállapodásokhoz és az ügyfél DPIA-támogatási kötelezettségeihez kapcsolódik. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Az ügyfél megfeleléséhez szükséges információk adatfeldolgozó általi biztosításához kapcsolódik, beleértve a DPIA-támogatást és az ügyféltámogatási bizonyítékokat. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - A DPIA-előszűrésre, a teljes DPIA-ra vonatkozó döntésekre, kockázatkezelésre, maradványkockázat-elfogadásra, előzetes konzultációs döntésekre, kivételekre, auditmegállapításokra és helyesbítő intézkedésekre vonatkozó elszámoltathatósági bizonyítékokhoz kapcsolódik. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Az adatkezelő megfelelő adatvédelmi kockázati intézkedésekért, magas maradványkockázat felülvizsgálatáért, vezetői jóváhagyásért és szabályzatkarbantartásért viselt felelősségéhez kapcsolódik. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - A kockázatértékelésben és az éles indulás jóváhagyása előtt használt beépített és alapértelmezett adatvédelmi bizonyítékokhoz kapcsolódik. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Az adatfeldolgozói és al-adatfeldolgozói DPIA-támogatáshoz, az ügyfélutasítások kezeléséhez és a beszállítói kockázatkezelési bizonyítékokhoz kapcsolódik. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Az adatvédelmi kockázatértékelési és DPIA-bemeneteket támogató adatkezelési nyilvántartásokhoz kapcsolódik. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - A PII-biztonsági kockázati bemenetekhez, védelmi intézkedések kiválasztásához, biztonsági kockázatkezeléshez és biztonsági kontrollstátusz-frissítésekhez kapcsolódik. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - A DPIA-előszűréshez, a teljes DPIA-követelmény meghatározásához, a DPIA-tartalomhoz, DPO-tanácsadáshoz, felülvizsgálathoz és a magas kockázatú adatkezelés blokkolásához kapcsolódik, ha a szükséges DPIA-jóváhagyás hiányzik. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Az előzetes konzultációra vonatkozó döntéshozatalhoz, DPO-tanácsadáshoz, Top Management jóváhagyáshoz, valamint a folytatási, felfüggesztési, újratervezési vagy konzultációs intézkedésekhez kapcsolódik, ha magas maradványkockázat marad fenn. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - A Data Protection Officer / Privacy Advisor tanácsadásához és nyomon követéséhez kapcsolódik, ahol alkalmazandó, a DPIA-döntések, magas kockázatú adatkezelés, előzetes konzultáció és szabályzatmódosítások tekintetében. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Az adatvédelmi kontrollok azonosításához, biztonsági védelmi intézkedésekhez, adatvédelmi megfeleléshez, adatvédelmi kockázati bizonyítékokhoz, nyomon követéshez és felülvizsgálathoz kapcsolódik. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - A PIA-folyamat hatályához, előnyeihez, kiváltó feltételének meghatározásához, előkészítéséhez, értékelési bemeneteihez, érdekelt felek bizonyítékaihoz és a REG04-ben fenntartott DPIA-jelentési struktúrához kapcsolódik. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - A PII-védelmi program követelményeihez, a PII-védelmi követelmények azonosításához, a kockázatalapú kontrollkiválasztáshoz és az adatvédelmi kockázatkezelési kapcsolódáshoz kapcsolódik. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - A szervezeti adatvédelmi kockázati alapelvekhez, vezetői szerepvállaláshoz, integrációhoz, kockázatértékeléshez, kockázatkezeléshez, nyomon követéshez és felülvizsgálathoz, valamint rögzítéshez és jelentéstételhez kapcsolódik. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].