					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII01					Dokumentum címe: **Adatvédelmi információkezelési rendszer szabályzata**							
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 4.1	Both	Primary	Kontextus és PIMS-szerepkör meghatározása
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Érdekelt felek és követelmények
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS alkalmazási területe
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	A PIMS létrehozása és fejlesztése
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Vezetői szerepvállalás és elkötelezettség
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Adatvédelmi szabályzat
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Szerepkörök és hatáskörök
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	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
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Adatvédelmi célkitűzések
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Tervezett PIMS-változtatások
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Erőforrások
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetencia
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Tudatosság
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Kommunikáció
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentált információk
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	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	Primary	Nyomon követés és értékelés
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Belső audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Vezetőségi felülvizsgálat
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Folyamatos fejlesztés
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Meg nem felelés és helyesbítő intézkedés
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Adatkezelői irányítási nyilvántartások
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Adatfeldolgozói megállapodás és célok
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Kapcsolódás a PII biztonsági szabályzatához
GDPR	Article 5(2)	Controller	Supporting	Elszámoltathatósági bizonyítékok
GDPR	Article 24	Controller	Supporting	Adatkezelői intézkedések és szabályzat
GDPR	Article 26	Joint Controller	Supporting	Közös adatkezelői megállapodások
GDPR	Article 28	Both	Supporting	Adatfeldolgozói irányítás
GDPR	Article 30	Both	Supporting	Adatkezelési nyilvántartások
GDPR	Article 32	Both	Supporting	Az adatkezelés biztonsága
GDPR	Article 35	Controller	Supporting	DPIA irányítás
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Adatvédelmi kontrollok és alapelvek
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA-folyamat és előkészítés

ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	PII-védelmi program és szabályzat
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Szervezeti adatvédelmi kockázatok integrálása

1. hatály

1.1 Ez a szabályzat létrehozza a szervezet PIMS-ét a PII kezelésére adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói környezetekben.

1.2 Ez a szabályzat az alábbiakra alkalmazandó:

1.2.1 a PIMS alkalmazási területe, kontextusa, érdekelt felei és szervezeti határai;

1.2.2 PIMS-szerepkör meghatározása a PII-kezelési tevékenységekhez;

1.2.3 adatvédelmi szabályzat, adatvédelmi célkitűzések, adatvédelmi kockázatértékelés, adatvédelmi kockázatkezelés és a PIMS alkalmazhatósági nyilatkozata;

1.2.4 PIMS-irányítás, nyomon követés, belső audit, vezetőségi felülvizsgálat, meg nem felelés, helyesbítő intézkedés és folyamatos fejlesztés;

1.2.5 a PIMS-megfelelés és az elszámoltathatóság bizonyításához szükséges dokumentált információk és bizonyítékok.

1.3 E szabályzat alkalmazásában lényeges változásnak minősül minden olyan változás, amely érinti a PIMS alkalmazási területét, a PII-kezelés céljait, a PII-kategóriákat, a PII-alanyok kategóriáit, az adatkezelés helyszíneit, az adatkezelői vagy adatfeldolgozói szerepek kiosztását, a rendszerarchitektúrát, a beszállítói vagy al-adatfeldolgozói megállapodásokat, az adatvédelmi kockázati profilt, az alkalmazandó jogi vagy szerződéses kötelezettségeket, illetve a tanúsítási alkalmazási területet.

2. cél

2.1 Ez a szabályzat meghatározza a PIMS létrehozására, bevezetésére, fenntartására, nyomon követésére és folyamatos fejlesztésére vonatkozó kötelező irányítási követelményeket.

2.2 A szabályzat célja annak biztosítása, hogy a szervezet bizonyítani tudja a PII-kezelés elszámoltatható, kockázatalapú és bizonyítékvezérelt irányítását az alkalmazandó PIMS-szerepkörökben.

3. célkitűzések

3.1 A jelen szabályzat célkitűzései a következők:

3.1.1 a PIMS alkalmazási területének, kontextusának, határainak és szerepkör szerinti alkalmazhatóságának meghatározása;

3.1.2 a PIMS irányítási elszámoltathatóságának kijelölése a kanonikus PIMS-szerepkörök használatával;

3.1.3 adatvédelmi célkitűzések és mérhető PIMS-teljesítményelvárások kialakítása;

3.1.4 a kiválasztott és kizárt kontrollokra vonatkozó PIMS alkalmazhatósági nyilatkozat fenntartása;

3.1.5 az adatvédelmi kockázatértékelés, az adatvédelmi kockázatkezelés és a DPIA irányítás integrálása a PIMS működésébe;

3.1.6 annak biztosítása, hogy az adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói kötelezettségek az adatkezelés megkezdése előtt azonosításra kerüljenek;

3.1.7 auditra alkalmas bizonyítékok fenntartása a tanúsításra való felkészültség és a folyamatos fejlesztés érdekében;

3.1.8 szükségtelen szerepkörök, nyilvántartások, űrlapok és duplikált operatív kontrollok elkerülése.

4. szabályzati előírások

4.1 A PIMS létrehozása, kontextusa és alkalmazási területe

4.1.1 [Both] Top Management KÖTELES jóváhagyni a PIMS alkalmazási területét a REG01-ben a PIMS első bevezetése előtt, valamint bármely lényeges változástól számított 30 napon belül.

4.1.2 [Both] Privacy Lead / PIMS Manager KÖTELES évente, valamint bármely lényeges változástól számított 30 napon belül dokumentálni a külső és belső adatvédelmi kontextushoz kapcsolódó kérdéseket a REG01-ben.

4.1.3 [Both] Privacy Lead / PIMS Manager KÖTELES évente, valamint bármely lényeges változástól számított 30 napon belül dokumentálni a releváns érdekelt feleket és PIMS-követelményeiket a REG01-ben.

4.1.4 [Both] Privacy Lead / PIMS Manager KÖTELES minden vezetőségi felülvizsgálat előtt fenntartani a PIMS-folyamatok kapcsolódási összefoglalóját a REG01-ben.

4.2 PIMS-szerepkör meghatározása

4.2.1 [Both] Process Owner / Business Owner KÖTELES minden PII-kezelési tevékenység esetében az adatkezelési tevékenység megkezdése előtt besorolni a szervezet PIMS-szerepkörét a REG02-ben.

4.2.2 [Joint Controller] Vendor / Procurement Owner KÖTELES a közös adatkezelés megkezdése előtt dokumentálni a közös adatkezelői felelősségek megosztását a REG08-ban.

4.2.3 [Processor] Vendor / Procurement Owner KÖTELES a szolgáltatás bevezetése előtt dokumentálni az adatfeldolgozói tevékenységekre vonatkozó ügyfél-utasításokat a REG08-ban.

4.2.4 [Subprocessor] Vendor / Procurement Owner KÖTELES az al-adatfeldolgozás megkezdése előtt dokumentálni a feljebb lévő ügyfél utasításait és a jóváhagyott al-adatfeldolgozói megállapodásokat a REG08-ban.

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

9. kivételek

9.1 Kivétel kérése és jóváhagyása

9.1.1 [All] Process Owner / Business Owner KÖTELES az eltérés bekövetkezése előtt dokumentálni a jelen szabályzat alóli bármely kért kivételt a REG12-ben.

9.1.2 [Both] Privacy Lead / PIMS Manager KÖTELES jóváhagyás előtt értékelni minden kért kivétel adatvédelmi kockázatát a REG04-ben.

9.1.3 [Both] Top Management KÖTELES a végrehajtás előtt jóváhagyni az elfogadott adatvédelmi kockázati küszöbértékeket meghaladó kivételeket a REG12-ben.

9.1.4 [Both] Privacy Lead / PIMS Manager KÖTELES a lezárásig negyedévente felülvizsgálni az aktív PIMS-kivételeket a REG12-ben.

9.2 Kivétel lezárása

9.2.1 [All] Process Owner / Business Owner KÖTELES a jóváhagyott kivétel lejárati dátumáig dokumentálni a kivétel lezárásának bizonyítékait a REG12-ben.

9.2.2 [Both] Internal Audit / Compliance Reviewer KÖTELES a következő tervezett belső audit során ellenőrizni a lejárt kivételek lezárási bizonyítékait a REG12-ben.

10. betartatás

10.1 Meg nem felelések kezelése

10.1.1 [All] Privacy Lead / PIMS Manager KÖTELES az azonosítástól számított öt munkanapon belül rögzíteni a jelen szabályzattal kapcsolatos feltételezett meg nem feleléseket a REG12-ben.

10.1.2 [All] Process Owner / Business Owner KÖTELES a meg nem felelés jóváhagyását követően a kijelölt határidőig végrehajtani a jóváhagyott helyesbítő intézkedéseket a REG12-ben.

10.1.3 [All] Top Management KÖTELES minden vezetőségi felülvizsgálat során felülvizsgálni a megoldatlan jelentős PIMS meg nem feleléseket a REG12-ben.

10.1.4 [All] Internal Audit / Compliance Reviewer KÖTELES a bejelentett lezárástól számított 30 napon belül ellenőrizni a helyesbítő intézkedés eredményességét a REG12-ben.

10.2 Eszkaláció

10.2.1 [All] Privacy Lead / PIMS Manager KÖTELES a határidőt követő öt munkanapon belül eszkalálni a lejárt határidejű jelentős helyesbítő intézkedéseket Top Management felé a REG12-ben.

10.2.2 [All] Top Management KÖTELES az eszkalációtól számított 15 munkanapon belül rögzíteni a lejárt határidejű jelentős helyesbítő intézkedésekre vonatkozó döntéseket a REG12-ben.

11. felülvizsgálat és karbantartás

11.1 Szabályzat felülvizsgálata

11.1.1 [All] Privacy Lead / PIMS Manager KÖTELES évente, valamint bármely lényeges jogi, szervezeti, adatkezelési, technológiai vagy tanúsítási alkalmazásiterület-változástól számított 30 napon belül felülvizsgálni ezt a szabályzatot a REG12-ben.

11.1.2 [All] Data Protection Officer / Privacy Advisor KÖTELES a szabályzat jóváhagyása előtt dokumentált tanácsot adni a REG12-ben, ha a lényeges adatvédelmi kötelezettségek változnak.

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

11.1.4 [All] Privacy Lead / PIMS Manager KÖTELES a PIMS alkalmazási területét vagy a kontrollok alkalmazhatóságát módosító jóváhagyott szabályzatváltozásokat követő 15 munkanapon belül frissíteni a REG01-et és a REG03-at.

11.1.5 [All] Privacy Lead / PIMS Manager KÖTELES a közzétételtől számított 30 napon belül rögzíteni a jóváhagyott szabályzatváltozások kommunikálását a REG11-ben.

12. kapcsolódó szabályzatok

12.1 Ezt a szabályzatot az alábbi kapcsolódó szabályzatok támogatják:

12.2 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.3 PII03 - PII Processing Inventory and Lawful Basis Policy

12.4 PII07 - Privacy Risk Assessment and DPIA Policy

12.5 PII08 - Privacy by Design and Default Policy

12.6 PII12 - Processor, Subprocessor and Data Sharing Policy

12.7 PII14 - PII Security and Access Control Policy

12.8 PII15 - PII Incident and Breach Management Policy

12.9 PII16 - Privacy Training, Awareness and Competence Policy

12.10 PII17 - PIMS Documented Information and Evidence Management Policy

12.11 PII18 - PIMS Monitoring, Audit and Improvement Policy

13. hivatkozott szabványok és keretrendszerek

13.1 Ez a szabályzat az alábbi szabványokhoz és jogszabályokhoz van hozzárendelve. A megfeleltetés bemutatja, hogy a szabályzat hogyan támogatja a hivatkozott követelményeket, és azonosítja az azokat végrehajtó vagy támogató belső pontokat.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - A szervezeti kontextus, az adatvédelmi kontextuskérdések, valamint az adatkezelői vagy adatfeldolgozói szerep PIMS-tevékenységekre vonatkozó alkalmazhatóságának meghatározásához rendelve. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Az érdekelt felek, PII-alanyok, ügyfelek, felügyeleti hatóságok, adatfeldolgozók, al-adatfeldolgozók és releváns PIMS-követelményeik azonosításához rendelve. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - A dokumentált PIMS alkalmazási terület meghatározásához, jóváhagyásához, fenntartásához és módosításához rendelve. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - A PIMS-folyamatok és kapcsolódásaik létrehozásához, bevezetéséhez, fenntartásához és fejlesztéséhez rendelve. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Top Management jóváhagyásához, az erőforrásokhoz, az irányítási felülvizsgálathoz, valamint a PIMS eredményességével és fejlesztésével kapcsolatos vezetői szerepvállaláshoz rendelve. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - A jelen adatvédelmi szabályzat jóváhagyott dokumentált információként való fenntartásához és a szabályzatváltozások kommunikálásához rendelve. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - A PIMS-szerepkörök, felelősségek és hatáskörök kijelöléséhez és kommunikálásához rendelve. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - A PIMS kockázataira és lehetőségeire vonatkozó intézkedések tervezéséhez rendelve, a kontextus, az érdekelt felek követelményei, a célkitűzések és a fejlesztési bemenetek felhasználásával. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Az új vagy lényegesen módosított adatkezelés előtti adatvédelmi kockázatértékelés megkövetéséhez és az adatvédelmi kockázati bizonyítékok fenntartásához rendelve. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Az adatvédelmi kockázatkezeléshez, a kontrollkiválasztáshoz, az információbiztonsági programhoz való kapcsolódáshoz és az alkalmazhatósági nyilatkozat fenntartásához rendelve. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - A PIMS-célkitűzések kialakításához, méréséhez, nyomon követéséhez, kommunikálásához és frissítéséhez rendelve. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - A tervezett PIMS-változtatásokhoz, valamint az alkalmazási területet, szerepeket, kontrollokat és dokumentált információkat érintő változtatások szabályozásához rendelve. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - A PIMS létrehozásához, működtetéséhez, fenntartásához és fejlesztéséhez szükséges erőforrások meghatározásához és biztosításához rendelve. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - A PIMS-felelősségeket és szerepkör-teljesítményt támogató kompetenciaelvárásokhoz és bizonyítékokhoz rendelve. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Az adatvédelmi szabályzat, a PIMS eredményességéhez való hozzájárulás és a meg nem felelés következményei iránti tudatossághoz rendelve. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - A PIMS-irányításhoz, szabályzatváltozásokhoz és eszkalációhoz kapcsolódó belső és külső kommunikációhoz rendelve. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - A dokumentált információk létrehozásához, fenntartásához, kezeléséhez, a bizonyítékok készenlétéhez és megőrzéséhez rendelve. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - A PIMS operatív folyamatainak és a külső fél által biztosított folyamatoknak a tervezéséhez, bevezetéséhez és szabályozásához rendelve. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Az adatvédelmi kockázatértékelések tervezett időközönkénti, valamint jelentős változások javaslata vagy bekövetkezése esetén történő elvégzéséhez rendelve. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Az adatvédelmi kockázatkezelési tervek végrehajtásához és a kezelés eredményeire vonatkozó bizonyítékok megőrzéséhez rendelve. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - A nyomon követéshez, méréshez, elemzéshez, értékeléshez, mutatókhoz és a PIMS eredményességéről szóló jelentéstételhez rendelve. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - A belső audit tervezéséhez, a bizonyítékok mintavételéhez, az audit eredményeihez és a független felülvizsgálathoz rendelve. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - A vezetőségi felülvizsgálat bemeneteihez, a teljesítmény felülvizsgálatához, a vezetőségi felülvizsgálat kimeneteihez és a fejlesztési döntésekhez rendelve. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - A vezetőségi felülvizsgálaton, mutatókon, helyesbítő intézkedések nyomon követésén és szabályzatkarbantartáson alapuló folyamatos fejlesztéshez rendelve. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - A meg nem felelések kezeléséhez, a helyesbítő intézkedéshez, az eszkalációhoz, a lezáráshoz és az eredményesség ellenőrzéséhez rendelve. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Az adatkezelői oldali adatkezelési célnyilvántartásokhoz, a jogalap-kapcsolódáshoz, a DPIA szükségességének meghatározásához, a közös adatkezelői felelősségek megosztásához és az adatkezelési bizonyítékok nyilvántartásához rendelve. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Az adatfeldolgozói ügyfélmegállapodásokhoz, dokumentált ügyfél-utasításokhoz és az adatfeldolgozói célkorlátozásokhoz rendelve. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - A PII-biztonsági szabályzathoz való kapcsolódáshoz, a PII-biztonsági kontrollalapvonal felelősségéhez és az információbiztonsági kontrollok állapotához a PIMS alkalmazhatósági nyilatkozatában rendelve. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Az elszámoltathatósági bizonyítékokhoz, a szabályzat jóváhagyásához, az adatkezelési szerep besorolásához, a kontrollalkalmazhatósághoz, a nyomon követéshez, az audithoz és a helyesbítő intézkedések nyilvántartásaihoz rendelve. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Az adatkezelői irányítási intézkedésekhez, a szabályzat jóváhagyásához, a PIMS-célkitűzésekhez, az eredményesség felülvizsgálatához és az adatkezelői elszámoltathatóság dokumentált bizonyítékaihoz rendelve. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - A közös adatkezelői felelősségek megosztásának a közös adatkezelés megkezdése előtti meghatározásához és dokumentálásához rendelve. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Az adatfeldolgozói és al-adatfeldolgozói irányítási nyilvántartásokhoz, az ügyfél adatkezelési utasításaihoz és a külső fél által biztosított folyamatok szabályozásához rendelve. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Az adatkezelési tevékenységek nyilvántartásaihoz, a szerepbesoroláshoz, az adatkezelési elszámoltathatósági nyilvántartásokhoz és az auditálhatóság érdekében megőrzött bizonyítékokhoz rendelve. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - A PII-biztonsági alapvonal irányításához, a biztonsági kontrollok felelősségi köréhez, a biztonsági végrehajtási állapothoz és az operatív kontrollok megerősítéséhez rendelve. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - A DPIA szükségességének meghatározásához és az adatvédelmi kockázatértékeléshez rendelve, mielőtt a magas kockázatú vagy lényegesen módosított adatkezelői adatkezelés folytatódna. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Az adatvédelmi kontrollok azonosításához, az adatvédelmi alapelvekhez, az információbiztonsághoz, az adatvédelmi megfeleléshez, az audithoz, a bizonyítékokhoz és a kockázatalapú adatvédelmi irányításhoz rendelve. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - A PIA-irányításhoz, a DPIA kiváltó okainak meghatározásához, a PIA előkészítéséhez, az adatvédelmi kockázati kritériumokhoz és a dokumentált adatvédelmi kockázatértékelési bizonyítékokhoz rendelve. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - A PII-védelmi program követelményeihez, a PII-védelmi követelmények azonosításához, az adatvédelmi kockázatalapú kontrollkiválasztáshoz és a PII-védelmi szabályzati irányhoz rendelve. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - A szervezeti adatvédelmi kockázati alapelvekhez, a vezetői elkötelezettséghez, az adatvédelmi kockázat PIMS-irányításba történő integrálásához és a szervezet PII-kezelésben betöltött szerepének megértéséhez rendelve. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].