

				Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII18				Dokumentum címe: PIMS nyomon követési, audit- és fejlesztési szabályzat							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025		A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Úrlap		Nyilvántartás		Egyéb

Felülvizsgálati előzmények				
Felülvizsgálat száma	Felülvizsgálat dátuma	Változások	Felülvizsgálta	A folyamat tulajdonosa

Jóváhagyások			
Név	Beosztás	Dátum	Aláírás

<p>Jogi nyilatkozat (szerzői jog és felhasználási korlátozások) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Ez a dokumentum a Clarysec LLC szellemi tulajdona. A dokumentum semmilyen része nem másolható, nem használható fel újra, nem terjeszthető és nem módosítható kereskedelmi vagy bevezetési célból előzetes, kifejezett írásbeli engedély nélkül.</p> <p>A jogosulatlan felhasználás szigorúan tilos, és jogi eljárást vonhat maga után. Licenccel kapcsolatban keresse: info@clarysec.com</p>

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/kontroll/cikk	Alkalmazhatóság	Lefedettségtípusa	Megjegyzés
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Adatvédelmi célkitűzések mérése
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	A nyomon követéshez, audíthoz és fejlesztéshez kapcsolódó dokumentált információ
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Működéstervezés és -szabályozás nyomon követése
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Nyomon követés, mérés, elemzés 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.1.2.9	Controller	Supporting	Audit céljára használt adatkezelői adatkezelési nyilvántartások
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Adatfeldolgozói megállapodás és audit-együtműködési bizonyítékok
GDPR	Article 5(2)	Controller	Supporting	Elszámoltathatósági bizonyítékok
GDPR	Article 24	Controller	Supporting	Adatkezelői intézkedések és eredményességük felülvizsgálata
GDPR	Article 28	Both	Supporting	Adatfeldolgozói audit és együtműködés irányítása

GDPR	Article 30	Both	Supporting	Audit céljára használt adatkezelési nyilvántartások
GDPR	Article 32	Both	Supporting	Biztonsági intézkedések tesztelése és értékelése
GDPR	Article 39	Conditional	Supporting	DPO általi nyomon követés és audittanácsadás, ahol alkalmazandó
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Adatvédelmi megfelelés, audit és független felügyelet
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	PII-védelem felülvizsgálata és megfelelőségi ellenőrzések
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Információbiztonsági nyomon követés és értékelés
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	ISMS belső audit támogatása
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	ISMS vezetőségi felülvizsgálat támogatása
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	ISMS folyamatos fejlesztés támogatása
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	ISMS meg nem felelés és helyesbítő intézkedés támogatása
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Az információbiztonság független felülvizsgálata
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Szabályzatoknak és szabványoknak való megfelelés felülvizsgálata
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Irányítási rendszer auditálási alapelvei, programja,

				lefolytása és kompetenciája
--	--	--	--	-----------------------------

1. Hatály

1.1 Ez a szabályzat meghatározza a szervezet PIMS nyomon követésére, mérésére, elemzésére, értékelésére, belső auditjára, vezetőségi felülvizsgálatára, a meg nem felelések kezelésére, a helyesbítő intézkedésekre és a folyamatos fejlesztésre vonatkozó követelményeit.

1.2 Ez a szabályzat az alábbiakra alkalmazandó:

1.2.1 a PIMS alkalmazási területén belüli valamennyi PIMS-folyamatra, kontrollra, szabályzatra, nyilvántartásra, bizonyítékobjektumra, rendszerre, beszállítóra, adatfeldolgozóra, al-adatfeldolgozóra és adatmegosztási megállapodásra;

1.2.2 a szervezet adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói kontextusaira;

1.2.3 a PIMS-teljesítmény, az adatvédelmi célkitűzések, a kontrollok bevezetési állapota, az auditmegállapítások, a meg nem felelések, a helyesbítő intézkedések, a vezetőségi felülvizsgálati intézkedések és a fejlesztési intézkedések összevont nyomon követésére;

1.2.4 a REG12-ben megőrzött bizonyítékokra és a REG01-től REG11-ig megőrzött támogató forrásbizonyítékokra.

1.3 Ez a szabályzat nem váltja fel az egyéb PIMS-szabályzatokban meghatározott operatív nyomon követési követelményeket. A PIMS összevont teljesítményértékelési, audit-, felülvizsgálati és fejlesztési ciklusát hozza létre.

1.4 E szabályzat alkalmazásában jelentős PIMS meg nem felelésnek minősül az olyan hiba, amely lényegesen érinti a PIMS alkalmazási területét, az adatvédelmi célkitűzéseket, a PII-kezelés elszámoltathatóságát, az adatvédelmi kockázatkezelést, a PII-alany jogait, az adatkezelés biztonságát, az adatfeldolgozói vagy al-adatfeldolgozói irányítást, az adatsértésre való felkészültséget, a dokumentált bizonyítékok sértetlenségét, a tanúsítási hatókört, vagy ugyanazon követelmény 12 hónapos időszakon belüli ismételt megsértését.

1.5 E szabályzat alkalmazásában lényeges változás minden olyan változás, amely érinti a PIMS alkalmazási területét, a PII-kezelési célokat, a PII-kategóriákat, a PII-alanyok kategóriáit, az adatkezelési helyszíneket, az adatkezelői vagy adatfeldolgozói szerepek kiosztását, a rendszerarchitektúrát, a beszállítói vagy al-adatfeldolgozói megállapodásokat, az adatvédelmi kockázati profilt, az alkalmazandó jogi vagy szerződéses kötelezettségeket, az audit hatókörét, a nyomon követési módszert vagy a tanúsítási hatókört.

2. Cél

2.1 E szabályzat célja annak biztosítása, hogy a szervezet objektív bizonyítékok alapján értékelje a PIMS teljesítményét, ellenőrizze a PIMS megfelelőségét, azonosítsa a meg nem feleléseket, helyesbítse a kontrollgyengeségeket, és folyamatosan fejlessze a PIMS-et.

2.2 Ez a szabályzat lehetővé teszi a szervezet számára annak igazolását, hogy a PIMS nyomon követési, audit-, vezetőségi felülvizsgálati és fejlesztési tevékenységei tervezettek, szükség esetén függetlenek, bizonyítékalapúak, időszerűek, valamint visszakövethetők az elszámoltatható szerepkörökhöz és a kanonikus bizonyítékobjektumokhoz.

3. Célkitűzések

3.1 E szabályzat célkitűzései a következők:

3.1.1 összevont PIMS nyomon követési és mérési folyamat meghatározása;

3.1.2 annak biztosítása, hogy az adatvédelmi célkitűzések és a PIMS kontrollteljesítménye dokumentált bizonyítékok alapján kerüljön mérésre;

3.1.3 kockázatalapú belső auditprogram létrehozása a PIMS számára;

3.1.4 a függetlenség és objektivitás megőrzése a PIMS audittevékenységeiben;

- 3.1.5 annak biztosítása, hogy a vezetőségi felülvizsgálat teljes körű és aktuális PIMS-teljesítménybemeneteket kapjon;
- 3.1.6 annak biztosítása, hogy a meg nem felelések rögzítése, értékelése, helyesbítése és ellenőrzése megtörténjen;
- 3.1.7 annak biztosítása, hogy a helyesbítő intézkedések lezárásig nyomon követhetők legyenek, és eredményességüket felülvizsgálják;
- 3.1.8 visszatérő gyengeségek és fejlesztési lehetőségek azonosítása;
- 3.1.9 a tanúsításra való felkészültség és az elszámoltatható bizonyítékezelés támogatása;
- 3.1.10 az operatív mutatók megkettőződésének elkerülése, amennyiben azokat kapcsolódó PIMS-szabályzatok már meghatározzák.

4. Szabályzati rendelkezések

4.1 PIMS nyomon követési és mérési keretrendszer

- 4.1.1 [Both] The Privacy Lead / PIMS Manager MUST köteles a REG12-ben meghatározni az összevont PIMS nyomon követési programot a PIMS kezdeti működése előtt, majd azt követően évente.
- 4.1.2 [Both] The Privacy Lead / PIMS Manager MUST köteles a REG12-ben meghatározni az egyes PIMS-mutatók mérési módszerét, gyakoriságát, bizonyítékforrását, célértékét és felelős szerepkörét a mérési ciklus megkezdése előtt.
- 4.1.3 [Both] The Process Owner / Business Owner MUST köteles negyedévente PII adatkezelési tevékenységre vonatkozó nyomon követési bemeneteket szolgáltatni a REG02-ből a Privacy Lead / PIMS Manager részére.
- 4.1.4 [Both] The Information Security Lead MUST köteles negyedévente PII-biztonsági kontrollállapot-bemeneteket szolgáltatni a REG03-ból a Privacy Lead / PIMS Manager részére.
- 4.1.5 [Both] The Vendor / Procurement Owner MUST köteles negyedévente adatfeldolgozói, al-adatfeldolgozói, harmadik féllel történő megosztási és szállítói bizonyossági státusz-bemeneteket szolgáltatni a REG08-ból a Privacy Lead / PIMS Manager részére.
- 4.1.6 [All] The Incident Response Coordinator MUST köteles havonta, továbbá jelentős incidens lezárását követő 10 munkanapon belül adatvédelmi incidens- és adatsértési trendbemeneteket szolgáltatni a REG10-ből a Privacy Lead / PIMS Manager részére.
- 4.1.7 [Both] The Privacy Lead / PIMS Manager MUST köteles negyedévente összevonni a PIMS nyomon követési eredményeit a REG12-ben.

4.2 PIMS belső auditprogram

- 4.2.1 [All] The Internal Audit / Compliance Reviewer MUST köteles évente, az első tervezett PIMS auditciklus előtt kockázatalapú PIMS belső auditprogramot készíteni a REG12-ben.
- 4.2.2 [All] The Internal Audit / Compliance Reviewer MUST köteles az audit terepmunkájának megkezdése előtt a REG12-ben meghatározni az egyes PIMS auditok célját, kritériumait, hatókörét, módszerét, mintavételi alapját és jelentéstételi határidejét.
- 4.2.3 [All] The Internal Audit / Compliance Reviewer MUST köteles minden auditmegbízás előtt rögzíteni az auditori függetlenségre és összeférhetetlenségre vonatkozó ellenőrzéseket a REG12-ben.
- 4.2.4 [All] The Privacy Lead / PIMS Manager MUST köteles jóváhagyott auditkérelem esetén 10 munkanapon belül a REG12-n keresztül elérhetővé tenni a kért, szabályozott PIMS dokumentált információkat és nyilvántartási bizonyítékokat.
- 4.2.5 [Both] The Internal Audit / Compliance Reviewer MUST köteles minden PIMS audit során a REG03 alapján tesztelni az alkalmazandó PIMS kontrollok bevezetési állapotát.

- 4.2.6 [Both] The Internal Audit / Compliance Reviewer MUST köteles minden PIMS audit során rögzíteni a kiválasztott PII-kezelési bizonyítékmintát a REG12-ben.
- 4.2.7 [All] The Internal Audit / Compliance Reviewer MUST köteles az audit befejezését követő 15 munkanapon belül rögzíteni a PIMS audit eredményeit a REG12-ben.
- 4.2.8 [All] The Privacy Lead / PIMS Manager MUST köteles az audit eredményeinek elfogadásától számított 10 munkanapon belül helyesbítő intézkedési felelősöket kijelölni az elfogadott PIMS auditmegállapításokhoz a REG12-ben.

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

9. Kivételek

9.1 Nyomon követési, audit- és fejlesztési kivételek

- 9.1.1 [All] The Process Owner / Business Owner MUST köteles a szabályzattól való bármely kivételt az eltérés bekövetkezése előtt kérelmezni a REG12-ben.
- 9.1.2 [All] The Privacy Lead / PIMS Manager MUST köteles a kérelemtől számított 10 munkanapon belül értékelni minden kért kivétel adatvédelmi, tanúsítási, audit- és helyesbítő intézkedési hatását a REG12-ben.
- 9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST köteles tanácsát rögzíteni a REG12-ben minden olyan kivétel jóváhagyása előtt, amely jogi kötelezettségeket, PII-alanyi jogokat, DPIA-vállalásokat, ügyfélaudit-kötelezettségeket vagy magas kockázatú adatkezelést érint.
- 9.1.4 [All] Top Management MUST köteles a kivétel hatálybalépése előtt jóváhagyni a REG12-ben az auditütemezés teljesítését, a vezetőségi felülvizsgálatot, jelentős meg nem feleléseket, tanúsítási hatókört vagy magas kockázatú adatkezelést érintő kivételeket.
- 9.1.5 [All] The Privacy Lead / PIMS Manager MUST köteles minden jóváhagyott nyomon követési, audit- vagy fejlesztési kivételhez legfeljebb 90 napos lejárat dátumot beállítani a REG12-ben.
- 9.1.6 [All] The Privacy Lead / PIMS Manager MUST köteles minden nyomon követési, audit- vagy fejlesztési kivételt a lejáratot követő öt munkanapon belül lezárni vagy újraértékelni a REG12-ben.

10. Betartás

10.1 Nyomon követési, audit- és fejlesztési követelmények betartása

- 10.1.1 [All] The Privacy Lead / PIMS Manager MUST köteles az elmulasztott nyomon követési ciklust, elmulasztott PIMS auditot, lejárt határidejű vezetőségi felülvizsgálatot, hiányzó auditbizonyítékot, lejárt határidejű helyesbítő intézkedést vagy lejárt határidejű fejlesztési intézkedést az azonosítástól számított öt munkanapon belül meg nem felelésként rögzíteni a REG12-ben.
- 10.1.2 [All] The Internal Audit / Compliance Reviewer MUST köteles az auditjelentés kiadása előtt rögzíteni az auditmegállapítás súlyosságát a REG12-ben.
- 10.1.3 [All] Top Management MUST köteles az eszkalációtól számított 10 munkanapon belül helyesbítő intézkedést előírni minden jelentős PIMS meg nem feleléshez a REG12-ben.
- 10.1.4 [All] The Process Owner / Business Owner MUST köteles megakadályozni a magas kockázatú adatkezelés éles indulását vagy külső bizonyossági benyújtását, ha a szükséges helyesbítő intézkedési bizonyítékok az éles indulás vagy benyújtás előtt hiányoznak a REG12-ből.

10.1.5 [All] The Privacy Lead / PIMS Manager MUST köteles 12 hónapos időszakon belüli második előfordulás után öt munkanapon belül eszkalálni az ismételten elmulasztott nyomon követési vagy helyesbítő intézkedési határidőket Top Management részére a REG12-ben.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST köteles a következő ütemezett audit során vagy a bejelentett lezárástól számított 60 napon belül – amelyik előbb bekövetkezik – ellenőrizni a betartatási intézkedés lezárását a REG12-ben.

11. Felülvizsgálat és karbantartás

11.1 Szabályzat felülvizsgálata és karbantartása

11.1.1 [All] The Privacy Lead / PIMS Manager MUST köteles ezt a szabályzatot évente, valamint a PIMS nyomon követési, audit-, vezetőségi felülvizsgálati, helyesbítő intézkedési vagy tanúsítási követelményeit érintő lényeges változástól számított 30 napon belül felülvizsgálni a REG12-ben.

11.1.2 [All] The Internal Audit / Compliance Reviewer MUST köteles a PIMS működési év utolsó ütemezett auditját követően évente felülvizsgálni a PIMS auditprogram eredményességét a REG12-ben.

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

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

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

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

12. Kapcsolódó szabályzatok

- 12.1 E szabályzatot az alábbi kapcsolódó szabályzatok támogatják:
- 12.2 PII01 - Adatvédelmi információirányítási rendszer szabályzat
- 12.3 PII02 - Adatvédelmi szerepkörök, felelőségek és elszámoltathatósági szabályzat
- 12.4 PII03 - PII adatkezelési tevékenységek nyilvántartása és jogalap szabályzat
- 12.5 PII04 - Adatvédelmi tájékoztató és átláthatósági szabályzat
- 12.6 PII05 - Hozzájárulás- és preferenciakezelési szabályzat
- 12.7 PII06 - PII-alanyi jogok kezelésének szabályzata
- 12.8 PII07 - Adatvédelmi kockázatértékelési és DPIA szabályzat
- 12.9 PII08 - Beépített és alapértelmezett adatvédelmi szabályzat
- 12.10 PII09 - PII gyűjtési, felhasználási, adatközlési és megosztási szabályzat
- 12.11 PII10 - PII megőrzési, törlési és megsemmisítési szabályzat
- 12.12 PII11 - PII pontossági és minőségi szabályzat
- 12.13 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik fél adatvédelmi kezelési szabályzat
- 12.14 PII13 - Nemzetközi PII-továbbítási szabályzat
- 12.15 PII14 - PII biztonsági és hozzáférés-szabályozási szabályzat
- 12.16 PII15 - PII incidens- és adatsértés-kezelési szabályzat
- 12.17 PII16 - Adatvédelmi képzési, tudatossági és kompetenciaszabályzat
- 12.18 PII17 - PIMS dokumentált információk és bizonyítékkezelési szabályzat

13. Hivatkozott szabványok és keretrendszerek

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Megfeleltetve a PIMS-célkitűzések és PIMS teljesítménymutatók meghatározásának, mérésének, jelentésének és felülvizsgálatának. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Megfeleltetve a nyomon követési eredményekhez, auditprogramokhoz, auditeredményekhez, vezetőségi felülvizsgálati bizonyítékokhoz, meg nem felelésekhez, helyesbítő intézkedésekhez és fejlesztési intézkedésekhez kapcsolódó dokumentált információk fenntartásának. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Megfeleltetve a tervezett PIMS nyomon követési, audit-, helyesbítő intézkedési és fejlesztési ciklus PIMS operatív kontroll részeként történő működtetésének. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Megfeleltetve annak meghatározásának, hogy mit kell nyomon követni és mérni, a nyomon követési eredmények összevonásának, a PIMS-teljesítmény értékelésének és a mérési bizonyítékok fenntartásának. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Megfeleltetve a belső auditprogram fenntartásának, az audittervezésnek, az auditori függetlenségi ellenőrzéseknek, a bizonyítékmintavételnek, az auditeredményeknek és az auditmegállapítások nyomon követésének. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Megfeleltetve a vezetőségi felülvizsgálat tervezésének, a PIMS-teljesítmény áttekintésének, az audit- és helyesbítő intézkedési trendek áttekintésének, a kimenetek jóváhagyásának és az erőforrás-döntéseknek. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Megfeleltetve a PIMS alkalmasságát, megfelelőségét és eredményességét szolgáló folyamatos fejlesztési lehetőségek azonosításának, jóváhagyásának, végrehajtásának és nyomon követésének. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Megfeleltetve a meg nem felelések rögzítésének, a gyökérok-elemzésnek, a helyesbítő intézkedések tervezésének, a helyesbítő intézkedések végrehajtásának, az eredményesség ellenőrzésének, az eskalációnak és a betartatásnak. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Megfeleltetve az adatkezelői adatkezelési nyilvántartásoknak, amelyeket bizonyítékforrásként használnak a nyomon követéshez, az auditmintavételhez és az adatkezelési tevékenységek nyilvántartásának naprakészégi mutatóihoz. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Megfeleltetve a beszállítói és ügyfélbizonyossági folyamatokon keresztül nyomon követett adatfeldolgozói megállapodási, ügyfélaudit-, bizonyossági válasz- és adatfeldolgozói együttműködési bizonyítékoknak. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Megfeleltetve a nyomon követéshez, audithoz, vezetőségi felülvizsgálathoz, helyesbítő intézkedéshez és folyamatos fejlesztéshez kapcsolódó elszámoltathatósági bizonyítékoknak. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

- 13.3.2 **Article 24** - Megfeleltetve az adatkezelői irányítási intézkedéseknek, az eredményesség felülvizsgálatának, a vezetőségi felülvizsgálatnak, a helyesbítő intézkedésnek és a dokumentált fejlesztési bizonyítékoknak. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].
- 13.3.3 **Article 28** - Megfeleltetve az adatfeldolgozói, al-adatfeldolgozói, ügyfélaudit-, harmadik fél bizonyossági és beszállítói együttműködési bizonyítékoknak. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].
- 13.3.4 **Article 30** - Megfeleltetve az adatkezelési nyilvántartásoknak, amelyeket nyomon követési, auditmintavételi, bizonyítékobjektum-teljességi és adatkezelési tevékenységek nyilvántartásának naprakészégi bizonyítékokként használnak. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].
- 13.3.5 **Article 32** - Megfeleltetve a PII-biztonsági kontrollállapot, a technikai kontrollbizonyítékok és a biztonsággal kapcsolatos eredményességi bizonyítékok nyomon követésének és értékelésének. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].
- 13.3.6 **Article 39** - Megfeleltetve a Data Protection Officer / Privacy Advisor által – ahol alkalmazandó – adott adatvédelmi tanácsadásnak, nyomon követési észrevételeknek, audittámogatásnak és adatvédelmi megfelelési trendek felülvizsgálatának. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.12** - Megfeleltetve az adatvédelmi megfelelés ellenőrzésének, a belső vagy független auditoknak, a belső kontrolloknak, a felügyeleti mechanizmusoknak és az adatvédelmi kockázatértékelési bizonyítékoknak. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Megfeleltetve a PII-hez kapcsolódó információbiztonság független felülvizsgálatának, a szabályzatoknak és szabványoknak való megfelelésnek, valamint a PII-védelem technikai megfeleléségi felülvizsgálatának. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

- 13.6.1 **Clause 9.1** - Megfeleltetve azoknak az információbiztonsági nyomon követési és értékelési bemeneteknek, amelyek támogatják a PIMS teljesítménymérését és a PII-biztonsági kontrollállapotot. Addressed by clauses [4.1.4; 8.1.2].
- 13.6.2 **Clause 9.2** - Megfeleltetve a PIMS audittervezést, auditbizonyítékokat, auditeredményeket és auditprogram-teljesítést támogató ISMS belső audit támogatásnak. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].
- 13.6.3 **Clause 9.3** - Megfeleltetve az integrált PIMS- és információbiztonsági teljesítményfelügyelet vezetőségi felülvizsgálati bemeneteinek és kimeneteinek. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].
- 13.6.4 **Clause 10.1** - Megfeleltetve a PIMS és a támogató információbiztonsági kontrollkörnyezet folyamatos fejlesztésének. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].
- 13.6.5 **Clause 10.2** - Megfeleltetve a meg nem felelések kezelésének, a helyesbítő intézkedések tervezésének, a helyesbítő intézkedések végrehajtásának és az eredményesség ellenőrzésének. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

- 13.7.1 Control 5.35 - Megfeleltetve a független felülvizsgálatnak, az auditori függetlenségi ellenőrzéseknek, az auditbizonyítékok tesztelésének és a helyesbítő intézkedések eredményessége független ellenőrzésének. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].
- 13.7.2 Control 5.36 - Megfeleltetve a PIMS- és információbiztonsági szabályzatok, a kontrollbevezetési állapot és a szabványoknak való megfelelési bizonyítékok megfelelőségi felülvizsgálatának. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

- 13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Megfeleltetve az auditalapelveknek, az auditprogram irányításának, az audit lefolytatásának, a bizonyítékalapú auditjelentésnek, az audit nyomon követésének és a PIMS auditokra vonatkozó auditori kompetenciaelvárásoknak. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].