| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ide írja be a bejegyzett jogi személy nevét | | | | | | | |
| Dokumentumszám:<br>PII17 | | | | | Dokumentum címe:<br>**PIMS dokumentált információk és bizonyító anyagok kezelésére vonatkozó szabályzat** | | | | | | | |
| Verzió:<br>1.0 | | Hatálybalépés dátuma:<br>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 6.1.3 | Both | Supporting | SoA dokumentált információ |
| ISO/IEC 27701:2025 | Clause 7.5 | Both | Primary | PIMS dokumentált információ |
| ISO/IEC 27701:2025 | Clause 8.1 | Both | Primary | Operatív bizonyítóanyag-kezelés |
| ISO/IEC 27701:2025 | Clause 9.1 | Both | Supporting | Nyomonkövetési bizonyító anyagok |
| ISO/IEC 27701:2025 | Clause 9.2 | Both | Supporting | Auditbizonyíték |
| ISO/IEC 27701:2025 | Clause 9.3 | Both | Supporting | Vezetőségi felülvizsgálati bizonyító anyagok |
| ISO/IEC 27701:2025 | Clause 10.2 | Both | Supporting | Meg nem felelésre és helyesbítő intézkedésre vonatkozó bizonyító anyagok |
| ISO/IEC 27701:2025 | Annex A.1.2.9 | Controller | Primary | Adatkezelői adatkezelési nyilvántartások |
| ISO/IEC 27701:2025 | Annex A.2.2.2 | Processor | Supporting | Adatfeldolgozói megállapodásokra és utasításokra vonatkozó bizonyító anyagok |
| ISO/IEC 27701:2025 | Annex A.3.14 | Both | Primary | Nyilvántartások védelme |
| GDPR | Article 5(2) | Controller | Supporting | Elszámoltathatósági bizonyító anyagok |
| GDPR | Article 24 | Controller | Supporting | Adatkezelői intézkedések és bizonyító anyagok |
| GDPR | Article 28 | Both | Supporting | Adatfeldolgozói dokumentáció |
| GDPR | Article 30 | Both | Supporting | Adatkezelési nyilvántartások |
| GDPR | Article 32 | Both | Supporting | Bizonyító anyagok védelme |

| | | | | |
|---|---|---|---|---|
| ISO/IEC 29100:2020 | Clause 5.12 | Both | Supporting | Adatvédelmi megfelelési bizonyító anyagok |
| ISO/IEC 29151:2022 | Clause 18.1.4 | Both | Supporting | Nyilvántartások védelme |
| ISO/IEC 27001:2022 | Clause 7.5 | Both | Supporting | Dokumentált információk kezelése |
| ISO/IEC 27002:2022 | Control 5.33 | Both | Supporting | Nyilvántartások védelme |
| ISO/IEC 27002:2022 | Control 5.34 | Both | Supporting | A magánszféra és a PII védelme |

## 1. Hatály

1.1 Ez a szabályzat kötelező követelményeket határoz meg a PIMS dokumentált információk létrehozására, jóváhagyására, verziókezelésére, védelmére, megőrzésére, visszakeresésére, fordítására, visszavonására és bizonyító anyagokkal való alátámasztására.

1.2 Ez a szabályzat a PIMS-megfelelés igazolására használt PIMS-szabályzatokra, nyilvántartásokra, dokumentált jóváhagyásokra, bizonyítékul szolgáló feljegyzésekre, auditbizonyítékokra, vezetőségi felülvizsgálati feljegyzésekre, helyesbítő intézkedések bizonyító anyagaira és kontrollált fordításokra alkalmazandó.

1.3 Ez a szabályzat az adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói kontextusokra alkalmazandó.

1.4 Ez a szabályzat nem hoz létre külön dokumentumkezelési nyilvántartást. A dokumentált információk kezelésére vonatkozó bizonyító anyagok fenntartása a REG01–REG12 kanonikus PIMS bizonyítékobjektumokon keresztül történik, a REG03 és REG12 felhasználásával a kontrollok alkalmazhatóságára, auditra, meg nem felelésre, helyesbítő intézkedésre és fejlesztésre vonatkozó bizonyító anyagokhoz.

## 2. Cél

2.1 A szabályzat célja annak biztosítása, hogy a PIMS dokumentált információk pontosak, kontrolláltak, a jogosult felhasználók számára hozzáférhetők legyenek, védettek legyenek a jogosulatlan módosítással vagy közzététellel szemben, auditálhatóság céljából megőrzésre kerüljenek, és elavulás esetén visszavonásra kerüljenek.

2.2 Ez a szabályzat támogatja a tanúsításra való felkészültséget annak biztosításával, hogy a PIMS-megfelelés igazolásához szükséges bizonyító anyagok megtalálhatók, ellenőrizhetők, visszakereshetők, valamint az alkalmazandó szabályzatokhoz, kontrollokhoz, adatkezelési tevékenységekhez, kockázatokhoz, auditokhoz és helyesbítő intézkedésekhez kapcsolhatók legyenek.

## 3. Célkitűzések

### 3.1 A szabályzat célkitűzései a következők:

3.1.1 a PIMS dokumentált információk kezelésére vonatkozó követelmények meghatározása;

3.1.2 a bizonyítékok sértetlenségének fenntartása a REG01–REG12 körében;

3.1.3 a szabályzat- és bizonyítóanyag-jóváhagyás visszakövethetőségének biztosítása;

3.1.4 a verzióelőzmények és a visszavonási döntések dokumentálásának biztosítása;

3.1.5 a PIMS-bizonyító anyagok összekapcsolása az alkalmazhatósági nyilatkozattal és a szabályzati megfeleltetésekkel;

3.1.6 a PIMS-dokumentumokhoz és bizonyítékul szolgáló feljegyzésekhez való hozzáférés szabályozása;

3.1.7 a többnyelvű szabályzatok és bizonyító anyagok verziókezelésének támogatása;

3.1.8 az auditbizonyíték időben történő visszakeresésének lehetővé tétele;

3.1.9 a szükségtelen dokumentumkezelési bürokrácia megelőzése;

3.1.10 az auditra való felkészültséget biztosító nyilvántartások megőrzése tanúsítás, ügyfélbizonyosság és folyamatos fejlesztés céljából.

## 4. Szabályzati előírások

### 4.1 PIMS dokumentált információk kezelése

4.1.1 [All] The Privacy Lead / PIMS Manager MUST a kezdeti PIMS-közzététel előtt, majd ezt követően negyedévente köteles fenntartani a PIMS dokumentált információk jegyzékét a REG12-ben.

4.1.2 [All] The Process Owner / Business Owner MUST minden általa birtokolt PII adatkezelési tevékenységhez köteles az adatkezelési tevékenység megkezdése előtt, majd ezt követően évente azonosítani a szükséges dokumentált információkat a REG02-ben.

4.1.3 [All] The Privacy Lead / PIMS Manager MUST minden szabályzatkiadás előtt, valamint a kontrollok alkalmazhatóságát érintő bármely lényeges változást követő 15 munkanapon belül köteles az alkalmazandó PIMS-szabályzatokat, kontrollokat és bizonyítóanyag-kötelezettségeket a REG03-hoz kapcsolni.

4.1.4 [All] The Privacy Lead / PIMS Manager MUST az adott kategória használata előtt köteles hozzáférési szintet és bizonyítóanyag-érzékenységi besorolást rendelni minden PIMS dokumentált információs kategóriához a REG12-ben.

### 4.2 Létrehozás, jóváhagyás, verziókezelés és közzététel

4.2.1 [All] The Privacy Lead / PIMS Manager MUST PIMS dokumentált információ közzététele előtt köteles dokumentumazonosítót, tulajdonost, verziószámot, jóváhagyási státuszt, hatálybalépés dátumát és felülvizsgálati dátumot rögzíteni a REG12-ben.

4.2.2 [All] Top Management MUST a közzététel előtt köteles jóváhagyni az alapvető PIMS-szabályzatokat és a lényeges szabályzatmódosításokat a REG12-ben.

4.2.3 [All] The Privacy Lead / PIMS Manager MUST operatív használat előtt köteles jóváhagyni a PIMS bizonyítóanyag-sablonokat vagy a beágyazott nyilvántartási szakaszokat a REG12-ben.

4.2.4 [All] The Privacy Lead / PIMS Manager MUST frissített PIMS dokumentált információ kiadása előtt köteles rögzíteni a verzióelőzményeket és a változtatás indokolását a REG12-ben.

4.2.5 [All] The Privacy Lead / PIMS Manager MUST a közzétételt követő 30 napon belül köteles rögzíteni a jóváhagyott PIMS dokumentált információs változások kommunikálását a REG11-ben.

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

## 9. Kivételek

9.1.1 [All] The Process Owner / Business Owner MUST a szabályzattól való eltérés előtt köteles dokumentált információs vagy bizonyítóanyag-kezelési kivételt kérni a REG12-ben.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST a kérelemtől számított 10 munkanapon belül köteles értékelni minden dokumentált információs vagy bizonyítóanyag-kezelési kivételt a REG12-ben.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST a PII bizonyító anyagok kiadását, fordítási eltérést, megőrzési konfliktust vagy auditbizonyíték-korlátozást érintő bármely kivétel jóváhagyása előtt köteles tanácsot rögzíteni a REG12-ben.

9.1.4 [All] Top Management MUST a kivétel hatálybalépése előtt köteles jóváhagyni a 30 napot meghaladó vagy tanúsítást, magas kockázatú adatkezelést, illetve külső bizonyosságot érintő dokumentált információs kivételeket a REG12-ben.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST minden jóváhagyott dokumentált információs vagy bizonyítóanyag-kezelési kivételhez legfeljebb 90 napos lejárati dátumot köteles meghatározni a REG12-ben.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST a lejárattól számított öt munkanapon belül köteles lezárni vagy újraértékelni minden dokumentált információs vagy bizonyítóanyag-kezelési kivételt a REG12-ben.

## 10. Betartatás

10.1.1 [All] The Privacy Lead / PIMS Manager MUST az azonosítástól számított öt munkanapon belül köteles meg nem felelésként rögzíteni a hiányzó, pontatlan, kontrollálatlan, elavult vagy visszakereshetetlen PIMS dokumentált információkat a REG12-ben.

10.1.2 [All] The Privacy Lead / PIMS Manager MUST köteles megakadályozni a PIMS dokumentált információk közzétételét, ha a szükséges jóváhagyási, verzió-, tulajdonosi vagy hatálybalépési dátumra vonatkozó bizonyító anyagok hiányoznak a REG12-ből.

10.1.3 [All] The Process Owner / Business Owner MUST köteles megakadályozni az adatkezelési bizonyító anyagok auditcélú benyújtását, ha a szükséges tulajdonosi, dátum-, státusz- vagy jóváhagyási bizonyító anyagok hiányoznak a REG02-ből.

10.1.4 [All] The System Owner / Application Owner MUST az azonosítástól számított egy munkanapon belül köteles eltávolítani a PIMS dokumentált információs adattárakhoz való jogosulatlan hozzáférést, és rögzíteni az eltávolítást a REG12-ben.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST a következő ütemezett audit során vagy a lezárástól számított 60 napon belül – amelyik előbb bekövetkezik – köteles ellenőrizni a dokumentált információs meg nem felelésekhez kapcsolódó helyesbítő intézkedések eredményességét a REG12-ben.

## 11. Felülvizsgálat és karbantartás

11.1.1 [All] The Privacy Lead / PIMS Manager MUST évente és a PIMS dokumentált információs követelményeket érintő lényeges változástól számított 30 napon belül köteles felülvizsgálni ezt a szabályzatot.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST jelentős auditmegállapítást, tanúsítási meg nem felelést, adattárplatform-változást vagy többnyelvű közzétételi folyamatváltozást követő 30 napon belül köteles felülvizsgálni ezt a szabályzatot.

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

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

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

## 12. Kapcsolódó szabályzatok

12.1 Ezt a szabályzatot a következő kapcsolódó szabályzatok támogatják:

12.2 PII01 - Adatvédelmi információkezelési rendszer szabályzata

12.3 PII02 - Adatvédelmi szerepkörök, felelősségek és elszámoltathatóság szabályzata

12.4 PII03 - PII adatkezelési tevékenységek nyilvántartásának és jogalapjának szabályzata

12.5 PII04 - Adatvédelmi tájékoztató és átláthatósági szabályzat

12.6 PII05 - Hozzájárulás- és preferenciakezelési szabályzat

12.7 PII06 - PII-alanyi jogok kezelésére vonatkozó szabályzat

12.8 PII07 - Adatvédelmi kockázatértékelési és DPIA szabályzat

12.9 PII08 - Beépített és alapértelmezett adatvédelem szabályzata

12.10 PII09 - PII gyűjtésére, felhasználására, közzétételére és megosztására vonatkozó szabályzat

12.11 PII10 - PII megőrzési, törlési és megsemmisítési szabályzata

12.12 PII11 - PII pontossági és minőségi szabályzata

12.13 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik felek adatvédelmi kezelésére vonatkozó 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 PII18 - PIMS nyomonkövetési, audit- és fejlesztési szabályzata

## 13. Hivatkozott szabványok és keretrendszerek

13.1 Ez a szabályzat a következő szabványokhoz és jogszabályokhoz van hozzárendelve. 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 6.1.3** - A PIMS alkalmazhatósági nyilatkozatának, a kontrollok alkalmazhatósági nyilvántartásainak és a szabályzat–bizonyítóanyag kapcsolatoknak a fenntartásához kapcsolódik. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - A dokumentált információk azonosításához, jóváhagyásához, verziókezeléséhez, hozzáféréséhez, visszakereséséhez, megőrzéséhez, visszavonásához, fordítási verziókapcsolatához és megőrzési metaadataihoz kapcsolódik. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Az adatkezelési nyilvántartásokhoz, bizonyítóanyag-sablonokhoz, operatív bizonyítóanyag-minőséghez és külső forrásból származó bizonyító anyagokhoz kapcsolódó operatív tervezési és kontrollbizonyítékokhoz kapcsolódik. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - A mérésre, visszakeresési teljesítményre, bizonyítóanyag-hiányosságokra, fordítási eltérésekre és adattári hozzáférési felülvizsgálatok teljesítésére vonatkozó dokumentált bizonyító anyagok fenntartásához kapcsolódik. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Az auditbizonyíték visszakereséséhez, auditmintavételhez, auditbizonyíték-visszakövethetőséghez és a dokumentált információk kezelésével kapcsolatos auditmegállapításokhoz kapcsolódik. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - A vezetőségi felülvizsgálati bizonyító anyagokhoz, a dokumentált információk kezelésének vezetőségi felülvizsgálat során történő figyelembevételéhez és a bizonyítóanyag-kezelési teljesítmény Top Management általi felülvizsgálatához kapcsolódik. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - A dokumentált információs meg nem felelésekhez, helyesbítő intézkedésekhez, kivételkezeléshez, lezáráshoz és eredményesség-ellenőrzéshez kapcsolódik. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Az adatkezelői adatkezelési nyilvántartásokhoz, elszámoltathatósági nyilvántartásokhoz, adatkezelési bizonyítóanyag-minőséghez és az adatkezelői kötelezettségeket alátámasztó bizonyító anyagok megőrzéséhez kapcsolódik. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Az adatfeldolgozói megállapodáshoz, ügyfélutasításhoz, külső forrásból származó bizonyító anyagokhoz és az adatfeldolgozói kapcsolatra vonatkozó bizonyítóanyag-kezeléshez kapcsolódik. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - A PIMS-nyilvántartások elvesztéssel, jogosulatlan módosítással, jogosulatlan hozzáféréssel, jogosulatlan kiadással és nem megfelelő megsemmisítéssel

szembeni védelméhez kapcsolódik. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

**13.3 GDPR**

13.3.1 **Article 5(2)** - Az elszámoltathatósági bizonyító anyagokhoz, a bizonyító anyagok visszakövethetőségéhez, a bizonyító anyagok visszakereséséhez, a meg nem felelési nyilvántartásokhoz és a megfelelést igazoló, auditra való felkészültséget biztosító nyilvántartásokhoz kapcsolódik. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Az adatkezelői irányítás bizonyító anyagaihoz, jóváhagyási nyilvántartásokhoz, szabályzatkezeléshez, elszámoltathatósági intézkedésekhez, dokumentált felülvizsgálathoz és Top Management felügyeletéhez kapcsolódik. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Az adatfeldolgozói és al-adatfeldolgozói dokumentációhoz, ügyfélutasítási bizonyító anyagokhoz, külső forrásból származó folyamatbizonyító anyagokhoz és bizonyítóanyag-kiadási kontrollhoz kapcsolódik. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Az adatkezelési nyilvántartási bizonyító anyagokhoz, bizonyítóanyag-minőségi követelményekhez, adatkezelési tevékenység hivatkozásaihoz és adatkezelési bizonyítóanyag-tulajdonosi/státusz metaadatokhoz kapcsolódik. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - A bizonyítóanyag-adattárak védelméhez, hozzáférési korlátozásokhoz, hozzáférési jóváhagyásokhoz, adattárvédelmi felülvizsgálathoz és jogosulatlan hozzáférés eltávolításához kapcsolódik. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.12** - Az adatvédelmi megfelelési bizonyító anyagokhoz, auditbizonyíték visszakereséséhez, bizonyítóanyag-visszakövethetőséghez, független felülvizsgálat támogatásához és helyesbítő intézkedési bizonyító anyagokhoz kapcsolódik. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Clause 18.1.4** - A PII-hez kapcsolódó nyilvántartások védelméhez, a nyilvántartások megőrzéséhez, valamint a bizonyítóanyag-adattárak hozzáférési és törlési kontrolljaihoz kapcsolódik. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

**13.6 ISO/IEC 27001:2022**

13.6.1 **Clause 7.5** - A dokumentált információk azonosításához, jóváhagyásához, rendelkezésre állásához, védelméhez, verziókezeléséhez, megőrzéséhez, selejtezéséhez és külső követelmény alapján szükséges dokumentált információk kezeléséhez kapcsolódik. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

**13.7 ISO/IEC 27002:2022**

13.7.1 Control 5.33 - A PIMS-nyilvántartások elvesztéssel, megsemmisüléssel, meghamisítással, jogosulatlan hozzáféréssel, jogosulatlan kiadással és nem megfelelő megsemmisítéssel szembeni védelméhez kapcsolódik. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - A magánszféra és a PII védelméhez kapcsolódik dokumentált információkban, bizonyítóanyag-adattárakban, közzétételekben és hozzáférés-szabályozott nyilvántartásokban. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].