					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII16					Dokumentum címe: **Adatvédelmi képzési, tudatossági és kompetenciaszabályzat**							
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 7.2; Clause 7.3	Both	Primary	Kompetencia és tudatosság
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Kommunikáció és dokumentált bizonyítékok
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operatív kontroll, mérés és fejlesztés
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	PII-kezelési tudatosság, oktatás és képzés
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Elszámoltathatóság, adatfeldolgozói irányítás, biztonság és DPO-feladatok
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetencia, tudatosság és képzés
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Tudatossági, oktatási és képzési útmutatás
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Információbiztonsági és adatvédelmi megfelelés

1. Hatály

1.1 Ez a szabályzat meghatározza a szervezet adatvédelmi képzésre, tudatosságra és kompetenciára vonatkozó követelményeit a Privacy Information Management System keretében.

1.2 Ez a szabályzat azokra a munkatársakra, vállalkozókra, ideiglenes munkatársakra, releváns harmadik felekre, adatfeldolgozókra, al-adatfeldolgozókra és egyéb érdekelt felekre vonatkozik, akiknek munkája befolyásolhatja a PII-kezelést, a PIMS teljesítményét, a PII-alanyi jogokat, az adatvédelmi kockázatot, a PII-hez kapcsolódó információbiztonságot, az adatfeldolgozói utasításokat, az adatvédelmi incidenseket, a dokumentált információkat vagy a megfelelési bizonyítékokat.

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

1.4 Ez a szabályzat kiterjed a következőkre:

1.4.1 az adatvédelmi képzési célközönség azonosítása;

1.4.2 beléptetési képzés;

1.4.3 éves frissítő képzés;

1.4.4 szerepkör-alapú és esemény által kiváltott képzés;

1.4.5 képzési teljesítési bizonyítékok;

1.4.6 a nem teljesítés eszkalációja;

1.4.7 a képzési hatékonyság felülvizsgálata;

1.4.8 adatfeldolgozói, al-adatfeldolgozói és harmadik félre vonatkozó képzési bizonyossági bizonyítékok.

1.5 Ez a szabályzat nem hoz létre külön képzési mátrixot, képzési irányítópultot, humánerőforrás-nyilvántartást, kompetencianyilvántartást, fegyelmi nyilvántartást vagy ügyfélképzési nyilvántartást. A képzési hozzárendeléseket, teljesítéseket, emlékeztetőket, kompetenciabizonyítékokat és tudatossági bizonyítékokat a REG11 tartalmazza; a kivételeket, eszkalációkat, meg nem feleléseket, helyesbítő intézkedéseket és felülvizsgálati bizonyítékokat a REG12 rögzíti. Az adatfeldolgozói, al-adatfeldolgozói és harmadik félre vonatkozó képzési bizonyossági bizonyítékokat releváns esetben a REG08 rögzíti.

1.6 Ez a szabályzat nem ismétli meg a következőket:

1.6.1 a szerepköri elszámoltathatóság hozzárendelése a PII02-ben;

1.6.2 az adatkezelési tevékenységek nyilvántartására és a jogalapra vonatkozó követelmények a PII03-ban;

1.6.3 az adatvédelmi kockázati és DPIA-módszertan a PII07-ben;

1.6.4 a beépített adatvédelmi kapuk a PII08-ban;

1.6.5 az adatfeldolgozói életciklus irányítása a PII12-ben;

1.6.6 a PII-biztonság és hozzáférés-szabályozás működtetése a PII14-ben;

1.6.7 a PII-incidens- és adatsértési munkafolyamat a PII15-ben;

1.6.8 a dokumentált információk irányítása a PII17-ben;

1.6.9 a nyomon követési, belső audit- és fejlesztési irányítás a PII18-ban.

2. Cél

2.1 A szabályzat célja annak biztosítása, hogy azok a személyek, akiknek munkája befolyásolja a PII-kezelést, megértsék adatvédelmi felelősségeiket, meghatározott ütemezés szerint elvégezzék a megfelelő képzést, fenntartsák a szerepkörükhöz kapcsolódó kompetenciát, valamint auditálható bizonyítékokat hozzanak létre a képzésről, a tudatosságról és az eszkalációról.

2.2 Ez a szabályzat a PIMS következetes végrehajtását támogatja azáltal, hogy a REG11-et elsődleges képzési és tudatossági bizonyítékobjektumként, a REG08-at, REG10-et és REG12-t pedig támogató bizonyítékobjektumként használja.

3. Célkitűzések

3.1 A szabályzat célkitűzései a következők:

3.1.1 az adatvédelmi képzési célközönségek meghatározása;

3.1.2 a beléptetési képzési követelmények meghatározása;

3.1.3 az éves frissítő képzési követelmények meghatározása;

3.1.4 a szerepkör-alapú adatvédelmi képzési követelmények meghatározása;

3.1.5 a teljesítési bizonyítékok rögzítése a REG11-ben;

3.1.6 a nem teljesítés eszkalálása a REG12-n keresztül;

3.1.7 az adatfeldolgozói, al-adatfeldolgozói és harmadik félre vonatkozó képzési bizonyossági bizonyítékok fenntartása a REG08-ban, ahol releváns;

3.1.8 a képzési hatékonyság felülvizsgálata túlzott mutatók vagy párhuzamos nyilvántartások létrehozása nélkül;

3.1.9 annak biztosítása, hogy a képzési tartalom összhangban maradjon az aktuális PIMS-szabályzatokkal és a lényeges adatvédelmi kötelezettségekkel.

4. Szabályzati rendelkezések

4.1 Képzési célközönség és hozzárendelés

4.1.1 [All] A Privacy Lead / PIMS Manager KÖTELES meghatározni a PIMS-képzési célközönségi kategóriákat a REG11-ben minden éves képzési ciklus megkezdése előtt.

4.1.2 [All] A Process Owner / Business Owner KÖTELES azonosítani a REG11-ben azokat a munkatársakat, akiknek feladatai PII-kezelést érintenek, még a beléptetés, a szerepkör-hozzárendelés vagy a lényeges feladatváltozás előtt.

4.1.3 [Conditional] A System Owner / Application Owner KÖTELES azonosítani a REG11-ben azokat a felhasználókat, akiknek PII-rendszerre, emelt jogosultságú hozzáférésre vagy adminisztratív adatvédelmi képzésre van szükségük, még a hozzáférés engedélyezése vagy lényeges módosítása előtt.

4.1.4 [Joint Controller] A Privacy Lead / PIMS Manager KÖTELES rögzíteni a közös adatkezelői képzési felelősség megosztását a REG11-ben vagy a REG08-ban a közös adatkezelési tevékenység megkezdése vagy lényeges módosítása előtt.

4.1.5 [Conditional] A Data Protection Officer / Privacy Advisor KÖTELES azonosítani a fokozott adatvédelmi képzési igényeket a REG11-ben, mielőtt képzést rendelnek azokhoz a szerepkörökhöz, amelyek magas kockázatú adatkezelést, különleges kategóriájú PII-t, PII-alanyi jogokat, DPIA-kat, nemzetközi adattovábbításokat vagy adatsértési értékelést kezelnek.

4.1.6 [All] A Privacy Lead / PIMS Manager KÖTELES rögzíteni a kijelölt képzési célközönséget, a képzés típusát, az előírt teljesítési határidőt és a bizonyíték tulajdonosát a REG11-ben minden éves képzési ciklus megkezdése előtt.

4.2 Beléptetési és éves képzési ütemezés

4.2.1 [All] A Privacy Lead / PIMS Manager KÖTELES alapszintű adatvédelmi tudatossági képzést hozzárendelni a REG11-ben a beléptetéstől számított 10 munkanapon belül azon munkatársak számára, akik hozzáférnek PII-hez vagy PIMS-felelősségekkel rendelkeznek.

4.2.2 [All] A Process Owner / Business Owner KÖTELES biztosítani, hogy a kijelölt munkatársak teljesítsék a beléptetési adatvédelmi képzést a REG11-ben, mielőtt felügyelet nélküli PII-

hozzáférés jóváhagyásra kerül, vagy a beléptetéstől számított 30 napon belül, attól függően, melyik következik be korábban.

4.2.3 [All] A Privacy Lead / PIMS Manager KÖTELES éves adatvédelmi frissítő képzést hozzárendelni a REG11-ben legalább 12 havonta egyszer.

4.2.4 [All] A Process Owner / Business Owner KÖTELES megerősíteni a kijelölt munkatársak éves frissítő képzésének teljesítési státuszát a REG11-ben a közzétett éves határidőig.

4.2.5 [Conditional] A Privacy Lead / PIMS Manager KÖTELES célzott frissítő képzést hozzárendelni a REG11-ben 30 napon belül lényeges adatvédelmi szabályzatmódosítást, lényeges PIMS-folyamatváltozást, auditmegállapítást, ismétlődő képzési sikertelenséget vagy releváns PII-incidensből származó tanulságot követően.

[... 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] A Process Owner / Business Owner KÖTELES adatvédelmi képzési kivételkérelmet rögzíteni a REG12-ben, mielőtt egy előírt teljesítési határidőt meghosszabbítanak.

9.1.2 [All] A Privacy Lead / PIMS Manager KÖTELES jóváhagyni vagy elutasítani az adatvédelmi képzési kivételkérelmeket a REG12-ben, mielőtt a kivétel aktívvá válik.

9.1.3 [Conditional] A Data Protection Officer / Privacy Advisor KÖTELES tanácsot adni a REG12-ben a képzési kivételekről a jóváhagyás előtt, ha a kivétel magas kockázatú adatkezelést, különleges kategóriájú PII-t, jogkezelést, incidenskezelést, nemzetközi adattovábbításokat vagy tanúsítási bizonyítékokat érint.

9.1.4 [Conditional] Top Management KÖTELES jóváhagyni az adatvédelmi képzési kivételeket a REG12-ben az aktiválás előtt, ha a kivétel ismétlődő nem teljesítést, emelt jogosultságú PII-hozzáférést, nagy hatású PII-kezelést vagy szabályozó hatóság felé bemutatható bizonyítékokat érint.

9.1.5 [All] A Privacy Lead / PIMS Manager KÖTELES meghatározni a kivétel tulajdonosát, lejárati dátumát, kompenzáló intézkedését és felülvizsgálati dátumát a REG12-ben bármely adatvédelmi képzési kivétel jóváhagyása előtt.

9.1.6 [All] A Process Owner / Business Owner KÖTELES lezárni vagy megújítani a jóváhagyott adatvédelmi képzési kivételeket a REG12-ben a kivétel lejárati dátuma előtt.

10. Betartatás

10.1.1 [All] A Privacy Lead / PIMS Manager KÖTELES képzési meg nem felelést rögzíteni a REG12-ben öt munkanapon belül, ha a kötelező adatvédelmi képzési bizonyíték hiányzik, hiányos, lejárt határidejű vagy nem vezethető vissza a REG11-re.

10.1.2 [All] A Process Owner / Business Owner KÖTELES biztosítani, hogy a lejárt határidejű kötelező adatvédelmi képzést teljesítsék vagy eszkalálják a REG11-ben vagy a REG12-ben a lejárt státusz rögzítését követő 10 munkanapon belül.

10.1.3 [Conditional] A System Owner / Application Owner KÖTELES korlátozni az új nagy hatású PII-hozzáférést a REG12-ben, ha az előírt beléptetési vagy szerepkör-alapú adatvédelmi képzés az eszkalációt követően is hiányos marad.

10.1.4 [Processor] A Vendor / Procurement Owner KÖTELES eszkalálni a hiányzó adatfeldolgozói, al-adatfeldolgozói vagy külső munkaerőre vonatkozó képzési bizonyossági bizonyítékokat a REG08-ban és a REG12-ben az azonosítást követő öt munkanapon belül.

10.1.5 [Conditional] Az Incident Response Coordinator KÖTELES a képzéssel kapcsolatos betartatási intézkedéseket összekapcsolni a REG10-zel egy munkanapon belül, ha a képzési hiba hozzájárult egy feltételezett vagy megerősített PII-incidenshez.

10.1.6 [All] Az Internal Audit / Compliance Reviewer KÖTELES ellenőrizni a képzési helyesbítő intézkedések lezárási bizonyítékait a következő ütemezett audit során vagy a lezárástól számított 60 napon belül, attól függően, melyik következik be korábban.

11. Felülvizsgálat és karbantartás

11.1.1 [All] A Privacy Lead / PIMS Manager KÖTELES legalább évente felülvizsgálni ezt a szabályzatot és a képzési tartalmat, valamint rögzíteni a felülvizsgálat eredményét a REG11-ben vagy a REG12-ben.

11.1.2 [All] A Privacy Lead / PIMS Manager KÖTELES felülvizsgálni ezt a szabályzatot 30 napon belül a PIMS alkalmazási területét, az adatvédelmi jogot, az adatkezelési tevékenységeket, a szerepkörmodellt, az incidensekből származó tanulságokat, az auditmegállapításokat vagy a képzési hatékonysági eredményeket érintő lényeges változást követően.

11.1.3 [Conditional] A Data Protection Officer / Privacy Advisor KÖTELES felülvizsgálni az adatvédelmi szempontból jelentős szabályzatmódosításokat a REG12-ben a jóváhagyás előtt.

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

11.1.5 [All] A Privacy Lead / PIMS Manager KÖTELES frissíteni a REG11 képzési tartalmát és hozzárendelési bizonyítékait 30 napon belül egy jóváhagyott lényeges szabályzatmódosítást követően.

12. Kapcsolódó szabályzatok

12.1 Ezt a szabályzatot a következőkkel együtt kell értelmezni:

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 szabályzata;

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 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik félre vonatkozó adatvédelmi kezelési szabályzat;

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 információ- és bizonyítékkezelési szabályzat;

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

13. Hivatkozott szabványok és keretrendszerek

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].