					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: PII15-FS					Dokumentum címe: **Pénzügyi szektorra vonatkozó PII-incidens- és adatsértés-kezelési 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 7.4; Clause 7.5	Both	Supporting	PIMS-kommunikációk és dokumentált incidensbizonyítékok
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operatív kontroll, valamint az adatvédelmi kockázatértékelés és kockázatkezelés kapcsolódása
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Nyomon követés, értékelés, meg nem felelés, helyesbítő intézkedés és fejlesztés
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Incidenskezelési tervezés és felkészülés a PII kezelésére
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	PII-t érintő információbiztonsági incidensekre adott válasz
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Jogi, törvényi, szabályozási és szerződéses követelmények, valamint a nyilvántartások védelme
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Adatfeldolgozói ügyfélszerződés és az ügyfélkötelezettségek támogatása
GDPR	Article 5(2); Article 24	Controller	Supporting	Elszámoltathatóság és adatkezelői felelősség
GDPR	Article 26	Joint Controller	Supporting	Közös adatkezelői incidensfelelősség koordinálása
GDPR	Article 28	Both	Supporting	Adatfeldolgozói segítségnyújtás és adatfeldolgozói

				szerződéses kötelezettségek
GDPR	Article 32	Both	Supporting	Az adatkezelés biztonsága és adatsértés-észlelési képesség
GDPR	Article 33	Both	Primary	Személyesadat-sértés bejelentése és adatsértési dokumentáció
GDPR	Article 34	Controller	Primary	Személyesadat-sértések közlése az érintett PII-alanyokkal
GDPR	Article 39	Conditional	Supporting	DPO tanácsadás, nyomon követés, együttműködés és kapcsolattartási pont támogatása
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	ICT-hez kapcsolódó incidenskezelési folyamat a hatály alá tartozó pénzügyi szervezetek számára
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	ICT-hez kapcsolódó incidensek és jelentős kiberfenyegetések osztályozási kritériumai
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Súlyos ICT-hez kapcsolódó incidensek jelentése és jelentős kiberfenyegetések bejelentése
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Jelentéstételi tartalom, határidők, sablonok és eljárások
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Jelentős incidensek bejelentése, ahol alkalmazandó
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Információbiztonsági és adatvédelmi megfelelési alapelvek
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	PII-incidensreagálási felelősségek és eseményjelentés

ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidenstervezés, értékelés, reagálás, levont tanulságok és bizonyítékgyűjtés
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Az incidenskezelési folyamat életciklusa
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidensszabályzat, terv, tudatosság, tesztelés és levont tanulságok
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Észlelési, értesítési, triázs-, elemzési, reagálási és jelentéstételi műveletek
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Nyilvános felhő adatfeldolgozói értesítési és adatsértési nyilvántartási elvárások

1. Hatály

1.1 Ez a szabályzat meghatározza a PII-incidensek és PII-adatsértések azonosítására, jelentésére, triázsára, osztályozására, értékelésére, elszigetelésére, bejelentésére, dokumentálására, lezárására és az azokból eredő fejlesztésekre vonatkozó követelményeket a pénzügyi szektorra kiterjedő PIMS alkalmazási területeken.

1.2 **Végrehajtási megjegyzés:** Ez a szabályzat a PII15 pénzügyi szektorra vonatkozó helyettesítő változata. Ugyanarra a PIMS alkalmazási területre, üzleti egységre, termékre, ügyfélkörnyezetre, szabályozott szolgáltatásra vagy bizonyítékhatárra nem vezethető be a PII15-tel párhuzamosan. A szervezeteknek ugyanarra a hatályra vagy a PII15-öt, vagy a PII15-FS-t kell kiválasztaniuk, hogy elkerüljék a párhuzamos incidenskezelési kötelezettségeket, párhuzamos nyilvántartásokat és párhuzamos auditbizonyíték-munkát.

1.3 Ez a szabályzat alkalmazandó:

1.3.1 a szervezetre, amikor pénzügyi szektorbeli környezetben PII-adatkezelőként jár el;

1.3.2 a szervezetre, amikor közös adatkezelőként jár el, és az incidenssel vagy adatsértéssel kapcsolatos felelősség koordinálása szükséges;

1.3.3 a szervezetre, amikor pénzügyi szektorbeli ügyfelek számára PII-adatfeldolgozóként jár el;

1.3.4 a szervezetre, amikor pénzügyi szektorbeli ügyfelek vagy upstream adatfeldolgozók számára al-adatfeldolgozóként jár el;

1.3.5 azokra a rendszerekre, alkalmazásokra, szolgáltatásokra, folyamatokra, beszállítókra, adatfeldolgozókra, al-adatfeldolgozókra és harmadik felekre, amelyek a pénzügyi szektorra kiterjedő PIMS alkalmazási területén belül PII-t kezelnek, tárolnak, továbbítanak, támogatnak, hozzáférnek vagy egyéb módon érintenek.

1.4 Ez a szabályzat a REG10 - PII-incidens- és adatsértési nyilvántartást használja elsődleges bizonyítékobjektumként a pénzügyi szektorbeli PII-incidens- és adatsértés-kezeléshez.

1.5 Ez a szabályzat a támogató bizonyítékobjektumokat az alábbiak szerint használja:

1.5.1 REG01 a PIMS alkalmazási területéhez, az alkalmazandó érdekelt felekhez, ágazati, ügyfél-, szerződéses és jelentéstételi környezethez.

1.5.2 REG02 az érintett adatkezelési tevékenységekhez, PII-kategóriákhoz, PII-alany-kategóriákhoz, célokhoz, rendszerekhez és szolgáltatásokhoz.

1.5.3 REG03 az alkalmazhatósági nyilatkozathoz és a kontrollalkalmazhatóság frissítéseihez, beleértve a PII15 PII15-FS általi helyettesítését ugyanarra a hatályra.

1.5.4 REG04 az adatvédelmi kockázathoz, DPIA-hoz, maradványkockázathoz és kockázatkezelési kapcsolódáshoz.

1.5.5 REG08 az adatfeldolgozói, al-adatfeldolgozói, ügyfél-, beszállítói és harmadik fél incidensinterfész bizonyítékaihoz.

1.5.6 REG09 a nemzetközi adattovábbítási kapcsolódáshoz, amikor egy incidens határokon átnyúló adatkezelést érint.

1.5.7 REG11 a képzéshez, tudatossághoz és incidensreagálási kompetenciához kapcsolódó bizonyítékokhoz.

1.5.8 REG12 az audit-, meg nem felelési, helyesbítő intézkedési, vezetőségi felülvizsgálati és fejlesztési bizonyítékokhoz.

1.6 Ez a szabályzat a speciális kontrollok tekintetében a kapcsolódó PIMS-szabályzatokra támaszkodik:

1.6.1 A PII03 szabályozza az adatkezelési tevékenységek nyilvántartását és a jogalap-nyilvántartásokat.

1.6.2 A PII04 szabályozza az adatvédelmi tájékoztatókat és az átláthatósági kontrollokat az adatsértés-specifikus kommunikáción kívül.

1.6.3 A PII06 szabályozza azokat a PII-alanyi joggyakorlási kérelmeket, amelyek incidens előtt, alatt vagy után merülnek fel.

1.6.4 A PII07 szabályozza az adatvédelmi kockázatértékelési és DPIA-módszertant.

1.6.5 A PII08 szabályozza a beépített és alapértelmezett adatvédelmi kontrollokat.

1.6.6 A PII10 szabályozza a megőrzési, törlési és selejtezési kontrollokat.

1.6.7 A PII12 szabályozza az adatfeldolgozói, al-adatfeldolgozói, beszállítói és harmadik féllel fennálló adatvédelmi kapcsolatok kontrolljait.

1.6.8 A PII13 szabályozza a nemzetközi PII-továbbítási mechanizmusokat és az adattovábbítási kockázati nyilvántartásokat.

1.6.9 A PII14 szabályozza a megelőző és észlelő PII-biztonsági és hozzáférés-szabályozási kontrollokat.

1.6.10 A PII16 szabályozza az adatvédelmi képzést, tudatosságot és kompetenciát.

1.6.11 A PII17 szabályozza a dokumentált információk és bizonyítékok kezelését.

1.6.12 A PII18 szabályozza a nyomon követést, belső auditot, vezetőségi felülvizsgálatot, meg nem felelést, helyesbítő intézkedést és folyamatos fejlesztést.

1.6.13 A PII23 szabályozza a felhőben működő PII-adatfeldolgozói kontrollokat, ahol a felhő-adatfeldolgozói kötelezettségek hatályban vannak.

1.7 E szabályzat alkalmazásában:

1.7.1 „PII-incidens” olyan feltételezett vagy megerősített esemény, amely érintette, érinthette vagy észszerűen érintheti a PII bizalmasságát, sértetlenségét, rendelkezésre állását, jogszerű kezelését vagy engedélyezett kezelését.

1.7.2 „PII-adatsértés” olyan megerősített PII-incidens, amely PII jogosulatlan, jogellenes, véletlen vagy nem szándékos megsemmisítésével, elvesztésével, megváltoztatásával, közlésével, hozzáférésével, elérhetetlenségével vagy kompromittálódásával jár.

1.7.3 „Pénzügyi szektorbeli PII-incidens” olyan PII-incidens, amely érinti, érintheti vagy észszerűen kapcsolódik szabályozott pénzügyi szolgáltatásokhoz, pénzügyi szektorbeli ügyfelekhez, pénzügyi partnerekhez, pénzügyi tranzakciókhoz, pénzügyi műveletekhez vagy pénzügyi szektorbeli PII-kezeléshez.

1.7.4 „Súlyos pénzügyi szektorbeli incidens” olyan pénzügyi szektorbeli PII-incidens vagy kapcsolódó ICT-incidens, amely megfelel a REG10-ben dokumentált lényegességi vagy jelentéstételi kritériumoknak.

1.7.5 „Jelentős kiberfenyegetés” olyan, a REG10-ben rögzített kiberfenyegetés, amely lényegesen érintheti a hatályba tartozó pénzügyi szektorbeli szolgáltatásokat, PII-kezelést, ügyfeleket, partnereket vagy műveleteket.

1.7.6 „Adatsértési értékelés” annak dokumentált értékelése, hogy egy PII-incidens PII-adatsértésnek minősül-e, milyen PII és mely PII-alanyok érintettek, milyen kockázatok merülhetnek fel, milyen bejelentések vagy kommunikációk szükségesek, és milyen helyreállító intézkedés szükséges.

1.7.7 „Tudomásszerzés” az a pont, amikor a szervezet észszerű bizonyossági szinttel rendelkezik arról, hogy biztonsági vagy adatvédelmi incidens történt, és PII kompromittálódott vagy kompromittálódhatott.

1.7.8 „Nagy hatású pénzügyi szektorbeli PII-incidens” olyan PII-incidens, amely nagy kockázatú adatkezelést, különleges kategóriájú vagy erősen érzékeny PII-t, nagyléptékű PII-t, sérülékeny személyeket, szabályozott ügyfeleket, lényeges szolgáltatáskimaradást, pénzügyi partnereket,

pénzügyi tranzakciókat, több joghatóságot érintő hatást, emelt jogosultságú hozzáférés kompromittálódását, nyilvános kitettséget, zsarolóvírust, szolgáltatáselérhetetlenséget vagy jelentős működési, ügyfél-, pénzügyi vagy reputációs hatást foglal magában.

1.7.9 „Lényeges incidensváltozás” olyan új vagy megváltozott információ, amely érinti az incidens hatályát, súlyosságát, PII-kategóriáit, PII-alanyi hatását, szolgáltatási hatását, pénzügyi szektorbeli besorolását, bejelentési döntését, ügyfélhatását, gyökérokát, elszigetelését, helyreállítását, helyesbítő intézkedését vagy külső jelentéstételi kötelezettségeit.

2. Cél

2.1 E szabályzat célja annak biztosítása, hogy a pénzügyi szektorbeli környezetekben felmerülő PII-incidenseket és adatsértéseket következetesen, haladéktalanul, jogszerűen, biztonságosan és auditra alkalmas bizonyítékokkal kezeljék.

2.2 Ez a szabályzat az elszámoltathatóságot támogatja azzal, hogy előírja a pénzügyi szektorbeli PII-incidensek és adatsértések REG10-ben történő rögzítését, valamint összekapcsolását az érintett adatkezelési nyilvántartásokkal, adatvédelmi kockázatokkal, adatfeldolgozói és al-adatfeldolgozói kapcsolatokkal, adattovábbítási nyilvántartásokkal, helyesbítő intézkedésekkel, képzési nyilvántartásokkal, pénzügyi szektorbeli jelentéstételi döntésekkel és vezetőségi felülvizsgálati bizonyítékokkal, ahol ezek kiváltódnak.

2.3 Ez a szabályzat biztosítja, hogy az adatkezelői, közös adatkezelői, adatfeldolgozói és al-adatfeldolgozói kötelezettségek elkülönített alkalmazhatósági szabályok szerint kerüljenek kezelésre, miközben egy integrált pénzügyi szektorbeli incidens- és adatsértési bizonyítékmodell marad fenn.

3. Célkitűzések

3.1 E szabályzat célkitűzései a következők:

3.1.1 biztosítani, hogy a feltételezett pénzügyi szektorbeli PII-incidenseket haladéktalanul jelentsék és rögzítsék;

3.1.2 biztosítani, hogy a pénzügyi szektorbeli PII-incidensek triázsa és osztályozása következetes adatvédelmi, biztonsági, működési és ágazati kritériumok alapján történjen;

3.1.3 biztosítani, hogy az adatsértési értékelések figyelembe vegyék az érintett PII-t, PII-alanyokat, rendszereket, szolgáltatásokat, adatkezelési tevékenységeket, adatfeldolgozókat, al-adatfeldolgozókat, adattovábbításokat, kockázatokat, ügyfeleket, partnereket és helyreállító intézkedéseket;

3.1.4 biztosítani, hogy az adatkezelői bejelentési és a PII-alanyoknak szóló kommunikációs döntéseket dokumentálják;

3.1.5 biztosítani, hogy az adatfeldolgozói és al-adatfeldolgozói adatsértési értesítések az ügyfelek vagy upstream felek felé indokolatlan késedelem nélkül és az alkalmazandó megállapodásoknak megfelelően történjenek;

3.1.6 biztosítani, hogy a pénzügyi szektorbeli jelentéstételi kiváltó okokat szükség esetén értékeljék, dokumentálják és nyomon kövessék;

3.1.7 biztosítani, hogy az incidenskezelés során a bizonyítékokat megőrizzék és védjék;

3.1.8 biztosítani, hogy az elszigetelés, eltávolítás, helyreállítás és ellenőrzés nyomon követése a REG10-en keresztül történjen;

3.1.9 biztosítani, hogy a jelentős kiberfenyegetéseket és a súlyos pénzügyi szektorbeli incidenseket megfelelő döntési és jelentéstételi munkafolyamatokba irányítsák;

3.1.10 biztosítani, hogy az incidensekből levont tanulságok helyesbítő intézkedésekhez, képzéshez, kontrollfejlesztéshez és vezetőségi felülvizsgálathoz vezessenek;

3.1.11 biztosítani, hogy az incidens- és adatsértési nyilvántartások rendelkezésre álljanak audithoz, vezetőségi felülvizsgálathoz, ügyfélbizonyossághoz és szabályozói felülvizsgálathoz, ahol alkalmazandó;

3.1.12 biztosítani, hogy a PII15-FS ugyanarra a pénzügyi szektorbeli hatályra a PII15 helyébe lépjen, és ne eredményezzen párhuzamos PII15 bizonyítékmunkát.

4. Szabályzati követelmények

4.1 Változat aktiválása, felkészültség és felvétel

4.1.1 [Conditional] The Privacy Lead / PIMS Manager MUST dokumentálni köteles a PII15-FS aktiválását a REG01-ben és a REG03-ban, mielőtt ezt a szabályzatot pénzügyi szektorbeli PIMS alkalmazási területre használják.

4.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST dokumentálni köteles a REG03-ban és a REG12-ben, hogy a PII15 nem kerül párhuzamosan bevezetésre ugyanarra a pénzügyi szektorbeli PIMS alkalmazási területre, mielőtt a PII15-FS jóváhagyásra kerül.

4.1.3 [All] The Incident Response Coordinator MUST minden bejelentett vagy észlelt feltételezett pénzügyi szektorbeli PII-incidenst köteles rögzíteni a REG10-ben a kézhezvételtől számított egy munkanapon belül, vagy korábban, ha alkalmazandó bejelentési, ügyfél- vagy jelentéstételi határidő aktiválódhat.

4.1.4 [Conditional] The Privacy Lead / PIMS Manager MUST legalább évente, valamint a PIMS alkalmazási terület, jogi környezet, ügyfélkötelezettségek, szerződéses kötelezettségek, ágazati jelentéstételi környezet vagy nagy kockázatú adatkezelés bármely lényeges változását követően köteles fenntartani a pénzügyi szektorbeli PII-incidens- és adatsértés-kezelési kritériumokat a REG10-ben.

4.1.5 [Both] The Information Security Lead MUST a feltételezett incidens PII-t kezelő rendszert, szolgáltatást vagy alkalmazást érintő bekövetkezését követő 24 órán belül köteles megerősíteni az incidensbizonyítékok megőrzésére vonatkozó követelményeket a REG10-ben.

4.1.6 [Conditional] The Vendor / Procurement Owner MUST a hatályba tartozó adatfeldolgozók, al-adatfeldolgozók, beszállítók és kiszervezett jelentéstételi szolgáltatók esetében a beléptetés előtt és legalább évente köteles fenntartani a pénzügyi szektorbeli harmadik fél incidenskapcsolattartási és bizonyítékirányítási követelményeit a REG08-ban.

4.2 Osztályozás és adatsértési értékelés

4.2.1 [All] The Incident Response Coordinator MUST minden REG10-bejegyzést a felvételtől számított 24 órán belül köteles besorolni nem PII-eseményként, feltételezett PII-incidensként, megerősített PII-incidensként, megerősített PII-adatsértésként, pénzügyi szektorbeli PII-incidensként, súlyos pénzügyi szektorbeli incidensként, jelentős kiberfenyegetésként vagy besorolás alatt álló bejegyzésként.

4.2.2 [Conditional] The Information Security Lead MUST köteles értékelni az érintett szolgáltatásokat, ügyfeleket, partnereket, tranzakciókat, szolgáltatáskiesést, földrajzi kiterjedést, adatvesztést, szolgáltatáskritikusságot és gazdasági hatást a REG10-ben, ha egy PII-incidens pénzügyi szektorbeli szolgáltatásokat vagy műveleteket érinthet.

4.2.3 [Both] The Privacy Lead / PIMS Manager MUST az adatsértési bejelentési döntés véglegesítése előtt köteles azonosítani az érintett adatkezelési tevékenységet, PII-kategóriákat, PII-alany-kategóriákat, rendszereket, adatfeldolgozókat, al-adatfeldolgozókat, adattovábbítási helyszíneket és adatvédelmi kockázatokat a REG02-ben, REG04-ben, REG08-ban, REG09-ben és REG10-ben.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor MUST minden megerősített vagy észszerűen feltételezett PII-adatsértés esetében köteles értékelni az érintett PII-alanyokat

érintő kockázatot, és a külső bejelentési döntés meghozatala előtt rögzíteni a bejelentési ajánlást, a kockázati indokolást és a tanácsot a REG10-ben.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST a feltételezett vagy megerősített PII-adatsértésért fennálló megosztott felelősség azonosítását követő 24 órán belül köteles rögzíteni a közös adatkezelői incidensfelelősség megosztását a REG08-ban és a REG10-ben.

4.2.6 [Processor] The Privacy Lead / PIMS Manager MUST a feltételezett vagy megerősített PII-adatsértés adatfeldolgozóként végzett adatkezelést érintő bekövetkezését követő 24 órán belül köteles értékelni az ügyfélutasításokat, a szerződéses értesítési kötelezettségeket és az együttműködési kötelezettségeket a REG08-ban és a REG10-ben.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MUST a feltételezett vagy megerősített PII-incidens al-adatfeldolgozóként végzett adatkezelést érintő bekövetkezését követő 24 órán belül köteles azonosítani az upstream értesítési láncot és a szükséges bizonyítékirányítást a REG08-ban és a REG10-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 Privacy Lead / PIMS Manager MUST köteles e szabályzat alóli bármely kivételt a végrehajtás előtt, vagy sürgősségi intézkedés esetén, ha az előzetes jóváhagyás nem volt megvalósítható, 24 órán belül rögzíteni a REG12-ben.

9.1.2 [Conditional] Top Management MUST köteles jóváhagyni minden olyan kivételt, amely lényegesen érinti az adatsértési bejelentés időzítését, a pénzügyi szektorbeli jelentéstétel időzítését, a nyilvános kommunikációt, az ügyfélkötelezettség-vállalást, a bizonyítékmegőrzést vagy a PII-alanyi kockázatot az incidens lezárása előtt, a jóváhagyási bizonyítékokat pedig a REG10-ben és a REG12-ben kell megőrizni.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST az incidens lezárása előtt köteles dokumentálni a tanácsot minden késedelmes bejelentéshez, bejelentés mellőzésére vonatkozó döntéshez, jelentéstételi kivételhez vagy kivételes kommunikációs megközelítéshez, a tanácsot pedig a REG10-ben kell megőrizni.

9.1.4 [Both] The Vendor / Procurement Owner MUST a kivétel azonosítását követő öt munkanapon belül köteles rögzíteni a pénzügyi szektorbeli incidensreagálást érintő beszállítói, adatfeldolgozói, al-adatfeldolgozói, ügyfél- vagy kiszervezett szolgáltatói kivételeket a REG08-ban és a REG12-ben.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST lezárásig legalább havonta köteles felülvizsgálni e szabályzat nyitott kivételeit, a felülvizsgálati állapotot pedig a REG12-ben kell megőrizni.

10. Betartatás

10.1.1 [All] The Process Owner / Business Owner MUST a feltételezett pénzügyi szektorbeli PII-incidens bejelentésének elmulasztását, a bizonyítékmegőrzés elmulasztását, a kijelölt intézkedések követésének elmulasztását vagy az adatsértési értékeléssel való együttműködés elmulasztását a felfedezést követő két munkanapon belül köteles eszkalálni a Privacy Lead / PIMS Manager felé, a bizonyítékokat pedig a REG12-ben kell megőrizni.

10.1.2 [Both] The Incident Response Coordinator MUST a késedelmes jelentést, elmulasztott besorolást, hiányzó bizonyítékot, elmulasztott eszkalációt vagy lejárt határidejű elszigetelési intézkedést az ügy azonosítását követő egy munkanapon belül köteles eszkalálni a Privacy Lead / PIMS Manager felé, a bizonyítékokat pedig a REG10-ben és a REG12-ben kell megőrizni.

10.1.3 [Both] The Privacy Lead / PIMS Manager MUST köteles REG12 szerinti meg nem felelést rögzíteni, ha e szabályzat megsértése érinti az incidensfelvételt, triázst, elszigetelést, bejelentést, jelentéstételt, bizonyítékok sértetlenségét, kommunikációt vagy helyesbítő intézkedést.

10.1.4 [Both] The Vendor / Procurement Owner MUST öt munkanapon belül köteles beszállítói, adatfeldolgozói, al-adatfeldolgozói vagy kiszervezett szolgáltatói helyreállítást kezdeményezni a REG08-on és REG12-n keresztül, ha egy harmadik fél nem teljesíti a megállapodott incidens-, adatsértési, bizonyíték- vagy jelentéstételi kötelezettségeket.

10.1.5 [Conditional] Top Management MUST a következő ütemezett vezetőségi felülvizsgálaton köteles áttekinteni a lényeges vagy ismétlődő PII15-FS meg nem feleléseket, a döntéseket és szükséges intézkedéseket pedig a REG12-ben kell megőrizni.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST 30 naptári napon belül köteles helyreállító képzést indítani a REG11-ben, ha egy szabályzati meg nem felelés szerepkörtudatosságot, késedelmes jelentést, eszkalációs hibát, bizonyítékkezelési hibát vagy kommunikációs hibát érint.

11. Felülvizsgálat és karbantartás

11.1.1 [Conditional] The Privacy Lead / PIMS Manager MUST legalább évente köteles felülvizsgálni ezt a szabályzatot, és a felülvizsgálat eredményét, a szükséges módosításokat és a jóváhagyási állapotot a REG12-ben rögzíteni.

11.1.2 [Conditional] The Incident Response Coordinator MUST minden nagy hatású pénzügyi szektorbeli PII-incidens, megerősített PII-adatsértés, súlyos pénzügyi szektorbeli incidens vagy jelentős kiberfenyegetés lezárását követő 30 naptári napon belül köteles kezdeményezni e szabályzat incidens utáni felülvizsgálatát, a felülvizsgálati bizonyítékokat pedig a REG10-ben és a REG12-ben kell megőrizni.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST 30 naptári napon belül köteles felülvizsgálni ezt a szabályzatot, miután tudomást szerez a jogi, ágazati, ügyfél-, szerződéses, adatfeldolgozói, al-adatfeldolgozói, jelentéssablon-, jelentési határidő- vagy adattovábbítással kapcsolatos incidensjelentési követelmények lényeges változásáról, a felülvizsgálati bizonyítékokat pedig a REG01-ben, REG08-ban, REG09-ben és REG12-ben kell megőrizni.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST legalább évente köteles felülvizsgálni e szabályzat végrehajtását a PIMS belső auditprogramon keresztül, az auditmegállapításokat és helyesbítő intézkedéseket pedig a REG12-ben kell megőrizni.

11.1.5 [Conditional] Top Management MUST az ütemezett vezetőségi felülvizsgálat során köteles áttekinteni az incidenstrendeket, jelentős adatsértéseket, jelentéstételi teljesítményt, lejárt határidejű helyesbítő intézkedéseket és a szabályzat eredményességét, a kimeneteket pedig a REG12-ben kell megőrizni.

11.1.6 [Conditional] The Privacy Lead / PIMS Manager MUST legalább évente és minden PIMS-hatókörváltozást követően köteles felülvizsgálni a PII15-FS és a PII15 közötti helyettesítési kapcsolatot annak ellenőrzésére, hogy a két szabályzatot nem vezették be ugyanarra a pénzügyi szektorbeli hatályra, a felülvizsgálati bizonyítékokat pedig a REG03-ban és a REG12-ben kell megőrizni.

12. Kapcsolódó szabályzatok

12.1 Ezt a szabályzatot az alábbiakkal együtt kell olvasni:

12.1.1 PII01 - Adatvédelmi információirányítási rendszer szabályzat

12.1.2 PII02 - Adatvédelmi szerepkörök, felelősségek és elszámoltathatósági szabályzat

12.1.3 PII03 - PII-kezelési nyilvántartási és jogalap-szabályzat

12.1.4 PII04 - Adatvédelmi tájékoztató és átláthatósági szabályzat

12.1.5 PII06 - PII-alanyi jogok kezelésére vonatkozó szabályzat

12.1.6 PII07 - Adatvédelmi kockázatértékelési és DPIA-szabályzat

12.1.7 PII08 - Beépített és alapértelmezett adatvédelmi szabályzat

12.1.8 PII10 - PII-megőrzési, törlési és selejtezési szabályzat

12.1.9 PII12 - Adatfeldolgozói, al-adatfeldolgozói és harmadik fél adatvédelmi kezelésére vonatkozó szabályzat

12.1.10 PII13 - Nemzetközi PII-továbbítási szabályzat

12.1.11 PII14 - PII-biztonsági és hozzáférés-szabályozási szabályzat

12.1.12 PII16 - Adatvédelmi képzési, tudatossági és kompetenciaszabályzat

12.1.13 PII17 - PIMS dokumentált információk és bizonyítékkezelési szabályzat

12.1.14 PII18 - PIMS nyomonkövetési, audit- és fejlesztési szabályzat

12.1.15 PII23 - Felhő PII-adatfeldolgozói szabályzat, ahol a pénzügyi szektorbeli felhő-adatfeldolgozói kötelezettségek hatályban vannak

12.2 PII15 - PII-incidens- és adatsértés-kezelési szabályzat az alap incidens- és adatsértési szabályzat. A PII15-FS a PII15 pénzügyi szektorra vonatkozó helyettesítő változata. A PII15 és a PII15-FS nem vezethető be párhuzamosan ugyanarra a PIMS alkalmazási területre, üzleti egységre, termékre, ügyfélkörnyezetre, szabályozott szolgáltatásra vagy bizonyítékhatárra.

13. Hivatkozott szabványok és keretrendszerek

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].