					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P16					Dokumentum címe: **Adatmaszkolási és pszeudonimizálási 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**

Összhang a vonatkozó szabványokkal és jogszabályokkal

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1. pont	Általános követelmények az adatmaszkolásra és pszeudonimizálásra vonatkozó kockázatkezeléshez és működési kontrollokhoz
ISO/IEC 27002:2022	8.11. kontroll	Kontrollútmutatás az adatmaszkolás és a pszeudonimizálás bevezetéséhez
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Adatvédelmi és bizalmassági kontrollok az adatminimalizálásra, adatátalakításra és hozzáférés-korlátozásra
GDPR	4. cikk (5), 5. cikk (1) c), f), 32. cikk	A pszeudonimizálás meghatározása és az adatvédelmi intézkedésekre vonatkozó követelmények
NIS2 irányelv	21. cikk (2) c)	A technikai és szervezési intézkedések, köztük a magánszféra-védelmet erősítő technológiák alkalmazásának kötelezettsége
DORA-rendelet	10. cikk (1), 10. cikk (2) e)	IKT-kockázatkezelési és bizalmassági kontrollok az adatmaszkolásra és a pszeudonimizálásra
COBIT 2019	DSS05.01, DSS06.06, MEA03	Irányítási kontrollok az adatvédelem támogatására adatmaszkolással és a megfelelés értékelésével

1. Cél

1.1 Jelen szabályzat meghatározza a szervezet adatmaszkolási és pszeudonimizálási megközelítését, mint a magánszféra védelmét erősítő technológiák alkalmazását a személyes vagy érzékeny adatok azonosíthatóságának és kitettségének csökkentése érdekében.

1.2 A szabályzat támogatja az információk biztonságos felhasználását tesztelési, elemzési és üzemeltetési célokra, miközben biztosítja a jogi és szabályozási követelmények teljesülését, mérsékli az adatvédelmi incidensek hatását, és érvényesíti az adatminimalizálás és a bizalmasság elveit.

1.3 A szabályzat összhangban áll az ISO/IEC 27001:2022 szabvánnyal, támogatja a GDPR 4. cikk (5) bekezdésében meghatározott pszeudonimizálást, és a NIST, a NIS2, a DORA és a COBIT 2019 követelményeivel összhangban kockázatalapú bevezetést ír elő.

2. Hatály

2.1 Jelen szabályzat hatálya kiterjed:

2.1.1 minden munkavállalóra, vállalkozóra, harmadik félre vagy beszállítóra, aki olyan rendszerekhez fér hozzá, amelyek személyes, bizalmas vagy érzékeny információkat kezelnek;

2.1.2 valamennyi adatkezelési környezetre, beleértve az éles, fejlesztői, teszt- és előéles környezeteket;

2.1.3 az adatmaszkolás valamennyi formájára, ideértve például a statikus, dinamikus, determinisztikus és tokenizációs megoldásokat, valamint a magánszféra-védelmi kockázatok csökkentésére alkalmazott pszeudonimizálási technikákra;

2.1.4 valamennyi adattípusra (strukturált vagy strukturálatlan), rendszerre (helyszíni vagy felhőalapú), valamint személyes vagy szabályozott adatokat érintő alkalmazásra.

2.2 A hatály az alábbi felhasználási területekre is kiterjed:

2.2.1 alkalmazásfejlesztési és minőségbiztosítási/tesztelési környezetek;

2.2.2 elemzési vagy jelentéskészítési platformok;

2.2.3 adatok megosztása harmadik felekkel vagy szolgáltatókkal;

2.2.4 biztonsági mentési, archiválási vagy helyreállítási rendszerek.

3. Célkitűzések

3.1 Biztosítani kell az adatmaszkolás és pszeudonimizálás következetes és hatékony alkalmazását az adatok kitettségéből vagy helytelen felhasználásából eredő kockázatok csökkentése érdekében.

3.2 Biztosítani kell, hogy nem éles környezetekben valós adatok ne kerüljenek felhasználásra, kivéve, ha azokat jóváhagyott PET-technika alkalmazásával átalakították.

3.3 A működési következetesség érdekében szükség esetén fenn kell tartani a referenciális integritást, a használhatóságot és a formátummegtartó átalakításokat.

3.4 Szigorú hozzáférés-szabályozást kell alkalmazni az eredeti adatokra, a maszkolt adatokra és az újraazonosítást lehetővé tevő kulcsokra.

3.5 A maszkolt vagy pszeudonimizált adatkészleteket érzékeny adatokként kell kezelni, amelyekre hozzáférés-naplózás, megőrzési kontrollok és incidenskezelési eljárások vonatkoznak.

3.6 E kontrollok hatékonyságát folyamatos teszteléssel, nyomon követéssel és auditeljárásokkal ellenőrizni kell.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja jelen szabályzatot, és biztosítja annak alkalmazását a tágabb IT-irányítási és adatvédelmi kezdeményezések részeként.

4.2 Információbiztonsági vezető / IBIR-vezető

4.2.1 Felügyeli a bevezetést és a folyamatos megfelelést.

4.2.2 Biztosítja az összhangot az ISO/IEC 27001 6.1.3. pontjával (kockázatkezelés) és 8.1. pontjával (működési kontrollok).

4.2.3 Felülvizsgálja a naplókat, és ellenőrzi a kontrollok hatékonyságát.

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

9. Felülvizsgálati és frissítési követelmények

9.1 Jelen szabályzatot legalább évente, vagy az alábbi esetek bármelyikének bekövetkezésekor ennél korábban is felül kell vizsgálni:

9.1.1 az adatmaszkolást vagy pszeudonimizálást érintő szabályozási változások;

9.1.2 érzékeny adatokat kezelő új IT-rendszerek bevezetése;

9.1.3 a szervezet adatosztályozási rendszerének lényeges módosulása;

9.1.4 kontrollhiányosságokat jelző auditmegállapítások;

9.1.5 új fenyegetések vagy adatmaszkolási technológiák megjelenése.

9.2 A felülvizsgálatot az IBIR-vezető vezeti a DPO, az adatgazdák, az információbiztonsági és a jogi terület bevonásával. A módosításokat verziókezeléssel kell nyomon követni, a felső vezetésnek kell jóváhagynia, és azokat valamennyi érintett féllel közölni kell.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P13 - Adatosztályozási és adatjelölési szabályzat. Az adatmaszkolásra és pszeudonimizálásra vonatkozó döntések közvetlenül a P13-ban meghatározott adatmező-osztályozástól és érzékenységi szintektől függenek.

10.2 P14 - Adatmegőrzési és selejtezési szabályzat. Az átalakított adatkészleteket a P14 életciklus-szabályainak megfelelően kell megőrizni és selejtezni, biztosítva, hogy a maszkolt és pszeudonimizált adatokat érzékeny adatként kezeljék.

10.3 P17 - Adatvédelmi és magánszféra-védelmi szabályzat. Meghatározza azokat az adatvédelmi elveket és szabályozási alapokat, amelyek alapján a pszeudonimizálás a GDPR és hasonló jogszabályok szerinti megfelelő adatkezelési tevékenységként alkalmazható.

10.4 P22 - Naplózási és felügyeleti szabályzat. Lehetővé teszi az adatmaszkolási és pszeudonimizálási események központi auditálását és riasztását, az előírt biztonsági megfigyelési protokollokkal összhangban.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.1.3. pont - Kockázatkezelési terv: Az adatmaszkolást és a pszeudonimizálást olyan kockázatkezelési mechanizmusként határozza meg, amely csökkenti az érzékeny adatok azonosíthatóságát a nem alapvető adatkezelési környezetekben.

11.1.2 8.1. pont - Működési tervezés és kontroll: Előírja a biztonságos adatátalakításhoz szükséges technikai és eljárási kontrollokat a feldolgozás, tárolás vagy továbbítás során.

11.2 ISO/IEC 27002:2022

11.2.1 8.11. kontroll: Iránymutatás az adatmaszkolásra és pszeudonimizálásra az újraazonosítási és adatszivárgási kockázatok minimalizálása érdekében.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Személyazonosításra alkalmas információk védelme: Olyan, a magánszféra védelmét erősítő technológiák bevezetése, mint az adatmaszkolás és a pszeudonimizálás.

11.3.2 PT-2, PT-3 - A személyazonosításra alkalmas információk kezelésének minimalizálása és biztonsága: Azonosíthatóságot csökkentő átalakítás és hozzáférés-szabályozás alkalmazása.

11.3.3 SC-12, SC-28, SC-30 - Adatbizalmasság és sértetlenség: A tárolás, továbbítás és felhasználás során alkalmazandó bizalmassági és elfedési kontrollok.

11.4 GDPR (2016/679)

11.4.1 4. cikk (5): A pszeudonimizálás hivatalos meghatározása.

11.4.2 32. cikk: Az adatkezelés biztonsága - szervezeti és technikai intézkedések a pszeudonimizálás érdekében.

11.4.3 5. cikk (1) c), f): Adatminimalizálás és bizalmasság pszeudonimizálás vagy adatmaszkolás alkalmazásával.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) c): Előírja az olyan PET-technológiák alkalmazását, mint az adatmaszkolás és a pszeudonimizálás, mint biztonsági intézkedések.

11.6 DORA-rendelet (2022/2554)

11.6.1 10. cikk (1): Az IKT-kockázatkezelési keretrendszernek adatmaszkolási és pszeudonimizálási kontrollokat kell tartalmaznia.

11.6.2 10. cikk (2) e): Előírja adatátalakítási technológiák használatát a személyes és pénzügyi adatok védelmére.

11.7 COBIT 2019

11.7.1 DSS05.01: Információs vagyon védelme - követelmények az adatmaszkolásra és a pszeudonimizálásra.

11.7.2 DSS06.06: Biztonságos tesztelés és elemzés - adatmaszkolás éles környezeten kívüli rendszerekben.

11.7.3 MEA03: A megfelelés nyomon követése az adatmaszkolás és pszeudonimizálás hatékonyságára vonatkozóan.