					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P16S					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**

A vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1.3. pont, 8. pont	Információbiztonsági kockázatok és a szükséges kontrollok, beleértve a maszkolást és a pszeudonimizálást
ISO/IEC 27002:2022	8.11. kontroll, 8. pont	Iránymutatás a maszkolásra és az adatszivárgás megelőzésére
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Adatelrejtés, az adatvédelmet erősítő technológiák
EU NIS2	21. cikk (2) bekezdés c) pont	Arányos technikai intézkedések, a pszeudonimizálás mint kontroll
EU DORA	10. cikk (1) bekezdés	IKT-kockázati kontrollok, beleértve az adatátalakítást biztosító védelmi intézkedéseket
COBIT 2019	DSS05.01, DSS06	Adatvédelem, adatelrejtési és pszeudonimizálási technikák
EU GDPR	4. cikk (5) bekezdés, 5. cikk (1) bekezdés c) pont, 32. cikk	Adatminimalizálás, a pszeudonimizálás mint technikai kontroll

1. Cél

1.1. Jelen szabályzat kötelezően alkalmazandó követelményeket határoz meg az adatmaszkolás és a pszeudonimizálás alkalmazására a bizalmas, személyes és érzékeny adatok védelme érdekében a kis- és középvállalkozásoknál (KKV-k).

1.2. E technikák alkalmazása kötelező minden olyan esetben, amikor valós adatok használata nem szükséges, például fejlesztési, elemzési vagy külső szolgáltatók bevonásával járó helyzetekben, ezáltal csökkentve a kitettség, a visszaélés vagy az adatsértés kockázatát.

1.3. Jelen szabályzat közvetlenül támogatja az ISO/IEC 27001:2022 szerinti tanúsítási megfelelést, valamint az olyan európai szabályozási követelmények teljesítését, mint a GDPR, a NIS2 irányelv és a DORA-rendelet.

1.4. Az adatok eredeti üzleti környezetükön kívüli felhasználását megelőző átalakításával a szervezet korlátozza a kitettséget, és erősíti annak igazolhatóságát, hogy az adatvédelem és az információbiztonság terén kellő gondossággal járt el.

2. Hatály

2.1. Jelen szabályzat hatálya kiterjed minden olyan strukturált vagy strukturálatlan adatra, amely személyes, bizalmas vagy érzékeny besorolású, függetlenül attól, hogy azt hol tárolják vagy kezelik:

2.1.1. Éles, teszt- vagy fejlesztői környezetben

2.1.2. Helyi eszközökön, szervereken vagy felhőplatformokon

2.1.3. Belső munkatársak, szerződéses partnerek vagy külső szolgáltatók által

2.2. A szabályzat kiterjed továbbá minden adatátalakítási eszközre is (maszkolás, tokenizáció, pszeudonimizálás), függetlenül attól, hogy azok nyílt forráskódú, kereskedelmi vagy saját fejlesztésű megoldások.

2.3. Jelen szabályzat szerinti felhasználási esetek különösen:

2.3.1. Teszt- vagy fejlesztési adatkészletek előállítása

2.3.2. Adatok exportálása elemző rendszerekbe

2.3.3. Beszállítók vagy tanácsadók hozzáférése működési rendszerekhez

2.3.4. Az érintettekre vonatkozó adatok minimalizálása a kezelési kockázat csökkentése érdekében

3. Célkitűzések

3.1. Biztosítani kell, hogy valós személyes vagy érzékeny adatok soha ne legyenek hozzáférhetők alacsonyabb biztonsági szintű környezetekben, ahol azok használata nem feltétlenül szükséges.

3.2. Kötelezővé kell tenni a maszkolási vagy pszeudonimizálási technikák alkalmazását minden olyan esetben, amikor a feladat végrehajtásához nincs feltétlenül szükség valós azonosítókra.

3.3. Meg kell előzni az adatokhoz való jogosulatlan hozzáférést vagy az azokkal való visszaélést azáltal, hogy adatátadás vagy adatkezelés előtt kötelező az adatátalakítási kontrollok alkalmazása.

3.4. Biztosítani kell, hogy minden maszkolási és pszeudonimizálási folyamat nyomon követhető, auditálható, valamint jóváhagyott eszközökkel kikényszerített legyen.

3.5. Meg kell felelni minden alkalmazandó jogi és szabályozási követelménynek, amely adatminimalizálást, bizalmasságot és adatátalakítást biztosító védelmi intézkedéseket ír elő.

4. Szerepkörök és felelősségi körök

4.1. Ügyvezető

4.1.1. A szabályzat tulajdonosa, és jóváhagyja azt.

4.1.2. Biztosítja, hogy minden szervezeti egység és szolgáltató megfeleljen az adatátalakítási követelményeknek.

4.1.3. Felülvizsgálja a kivételeket, a kockázatértékeléseket és az adatátalakítással kapcsolatos naplókat.

4.1.4. Szabálysértés esetén koordinálja a jogi, működési vagy beszállítókat érintő intézkedéseket.

4.2. Informatikai szolgáltató / belső IT

4.2.1. Kiválasztja és üzemelteti a maszkolási vagy pszeudonimizálási eszközöket.

4.2.2. Biztosítja, hogy az adattípusnak megfelelő adatátalakítási módszerek kerüljenek alkalmazásra.

4.2.3. Fenntartja az átalakított adatkészletek naplóit és a kulcskezelési eljárások dokumentációját.

4.2.4. Biztosítja, hogy a maszkolás a tesztelési, beszállítói vagy elemzési felhasználást megelőzően megtörténjen.

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

9. Felülvizsgálati és aktualizálási követelmények

9.1. Éves felülvizsgálat

9.1.1. Jelen szabályzatot az ügyvezetőnek legalább évente egyszer felül kell vizsgálnia annak biztosítása érdekében, hogy az tükrözze:

9.1.1.1. Az alkalmazandó jogszabályok változásait (pl. GDPR, DORA).

9.1.1.2. Az új üzleti rendszereket vagy a külső felekkel megvalósuló új adatcseréket.

9.1.1.3. Az auditokból vagy a maszkolatlan adatok használatával kapcsolatos incidensekből származó visszajelzéseket.

9.2. Soron kívüli felülvizsgálatok

9.2.1. Felülvizsgálatot kell végezni akkor is, ha:

9.2.1.1. Olyan új alkalmazásokat vagy platformokat vezetnek be, amelyek érzékeny adatokat kezelnek.

9.2.1.2. Egy jelentős incidens hiányosságokat tár fel a jelenlegi adatátalakítási kontrollokban.

9.2.1.3. A besorolási szintek változása érinti az adatkezelési eljárásokat.

9.3. Verziókezelés és változáskezelés

9.3.1. Minden szabályzatmódosítást:

9.3.1.1. Az ügyvezetőnek jóvá kell hagynia, és azt a változásnaplóban dokumentálni kell.

9.3.1.2. Egyértelműen közölni kell az érintett munkavállalókkal és szolgáltatókkal.

9.3.1.3. Biztonságosan kell archiválni, az elavult változatokhoz való hozzáférést korlátozva.

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzatot az alábbi KKV-szabályzatokkal együtt kell alkalmazni az érzékeny adatok következetes és kikényszeríthető védelmének biztosítása érdekében:

10.1.1. P13S – Adatbesorolási és címkézési szabályzat: Meghatározza azokat a besorolási szinteket (pl. „Bizalmas – Személyes”), amelyek alapján eldől, mikor kell maszkolást vagy pszeudonimizálást alkalmazni. Jelen szabályzat az adatátalakítási szabályokat az adatok érzékenységi szintje alapján érvényesíti.

10.1.2. P14S – Adatmegőrzési és törlési szabályzat: Biztosítja, hogy az átalakított adatkészletek, beleértve a maszkolt vagy pszeudonimizált adatokat tartalmazó biztonsági mentéseket is, a vonatkozó szabályok szerint kerüljenek megőrzésre és törlésre, ideértve a megfeleltetési kulcsok törlését is, amikor azokra már nincs szükség.

10.1.3. P17S – Adatvédelmi és információs önrendelkezési szabályzat: Összhangba hozza az adatátalakítási gyakorlatokat a szélesebb körű adatvédelmi kötelezettségekkel, beleértve a GDPR szerinti adatminimalizálási követelményeket és a pszeudonimizálás mint védelmi intézkedés alkalmazását a személyes adatok kezelése során.

10.1.4. P30S – Incidenskezelési szabályzat: Meghatározza a bejelentési és eszkalációs eljárásokat jogosulatlan adatközlés esetén, beleértve a maszkolt vagy pszeudonimizált adatok nem megfelelő használatát vagy visszafejtését.

10.1.5. P2S – Irányítási szerepkörök és felelősségek szabályzat: Kijelöli a szabályzat végrehajtásáért, a kockázatelfogadásért és a kivételek jóváhagyásáért fennálló átfogó felelősséget, elsődlegesen az ügyvezető számára.

10.2. E szabályzatok egységes adatvédelmi keretrendszert alkotnak, biztosítva, hogy a maszkolási és pszeudonimizálási intézkedések támogassák az ISO 27001 szerinti tanúsítást és a több szabályozási területre kiterjedő megfelelést.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 6.1.3. pont: Előírja az információbiztonsági kockázatok kezelését, amely magában foglalja a kitettség csökkentését adatátalakítási technikák alkalmazásával.

11.1.2. 8.1. pont: Előírja a biztonsági célok teljesítéséhez szükséges kontrollok bevezetését, beleértve a pszeudonimizálást és a maszkolást.

11.2. ISO/IEC 27002

11.2.1. 8.11. kontroll: Iránymutatást ad az érzékeny adatok maszkolására teszt- és fejlesztői rendszerekben.

11.2.2. 8.12. kontroll: Módszereket határoz meg az adatszivárgás megelőzésére ellenőrzött adatátalakítási és hozzáférési gyakorlatok alkalmazásával.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Biztosítja az információk bizalmasságát adatelrejtés útján.

11.3.2. SC-28: Védi a tárolt és használatban lévő információkat.

11.3.3. PT-2/PT-3: Elősegíti az adatvédelmet erősítő technológiák, így a pszeudonimizálás alkalmazását személyazonosításra alkalmas adatok kezelése során.

11.4. EU GDPR

11.4.1. 4. cikk (5) bekezdés: Jogilag meghatározza a pszeudonimizálást, és kontrollokat ír elő a megfeleltetési kulcsok és azonosítók kezelésére.

11.4.2. 5. cikk (1) bekezdés c) pont: Támogatja az adatminimalizálás elvét maszkolás alkalmazásán keresztül.

11.4.3. 32. cikk: Elismert technikai kontrollként kezeli a pszeudonimizálást, amely csökkenti az adatvédelmi kockázatokat.

11.5. EU NIS2 irányelv

11.5.1. 21. cikk (2) bekezdés c) pont: Előírja az arányos technikai intézkedések alkalmazását az adatbiztonsági kockázat csökkentése érdekében, beleértve a pszeudonimizálást mint kockázatkezelési kontrollt.

11.6. EU DORA-rendelet

11.6.1. 10. cikk (1) bekezdés: Előírja az IKT-hoz kapcsolódó kockázati kontrollokat, amelyek magukban foglalják az adatátalakítást biztosító védelmi intézkedéseket az üzletmenet-folytonosság és a bizalmasság érdekében kiszervezés és rendszerfejlesztés során.

11.7. COBIT 2019

11.7.1. DSS05.01: Előírja az információs vagyonelemek védelmét, beleértve – ahol lehetséges – az adatátalakítást.

11.7.2. DSS06.06: Megfelelő adatelrejtési és pszeudonimizálási technikák alkalmazását írja elő az adatkitettség korlátozására alacsonyabb bizalmi szintű környezetekben.