					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P14					Dokumentum címe: **Adatmegőrzési és megsemmisítési 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/cikk	Megjegyzés
ISO/IEC 27001:2022	6.1.3, 8.1 pont	
ISO/IEC 27002:2022	5.10, 5.12, 5.30, 5. pont	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
GDPR	5(1)(e), 17, 32. cikk	
NIS2 irányelv	21(2)(a-e) cikk	
DORA-rendelet	5., 9. cikk	
COBIT 2019	DSS01, DSS05 – Biztonsági szolgáltatások kezelése, MEA	

1. Cél

1.1 Jelen szabályzat célja, hogy meghatározza a szervezeti követelményeket az adatok megőrzésére és biztonságos megsemmisítésére az információ életciklusának valamennyi szakaszában. Biztosítja a vonatkozó jogi, szabályozási és szerződéses kötelezettségek teljesítését, valamint megelőzi az adatok szükségtelen vagy kockázatos felhalmozódását.

1.2 Ez a szabályzat támogatja az ISO/IEC 27001:2022 bevezetését azáltal, hogy előírja az adatok megőrzési időtartamának ellenőrzését és a visszafordíthatatlan megsemmisítési gyakorlatok alkalmazását. Lehetővé teszi a nyilvántartások visszakövethető dokumentálását, előírja az osztályozási szinthez igazodó megőrzést, valamint biztosítja az auditra, a szabályozói ellenőrzésekre és a jogi feltárás támogatására való felkészültséget.

1.3 További cél a bizalmasság, sértetlenség és rendelkezésre állás fenntartása az adatok teljes megőrzési ideje alatt és megsemmisítésük során, miközben csökkennek a helytelen adatmegőrzésből vagy megsemmisítésből eredő üzleti kockázatok, működési hatékonyságvesztések és adatvédelmi jogsértésekből eredő kitettségek.

2. Hatály

2.1 Jelen szabályzat kiterjed a szervezet tulajdonában álló, általa kezelt vagy megőrzött valamennyi fizikai és digitális információs vagyonelemre, beleértve a harmadik felek, leányvállalatok vagy kiszervezési partnerek ellenőrzése alatt álló vagyonelemeket is.

2.2 A hatály többek között az alábbiakra terjed ki:

2.2.1 Dokumentumok, fájlok és nyilvántartások (digitális és papíralapú)

2.2.2 Adatbázisok és archívumok

2.2.3 E-mailek és azonnali üzenetküldési naplók

2.2.4 Biztonsági mentések, rendszernaplók és auditnyomok

2.2.5 Forráskód, alkalmazásadatok és felhőben üzemeltetett vagyonelemek

2.2.6 Adatot tartalmazó cserélhető adathordozók és leselejtezett hardverek

2.3 A szabályzat vonatkozik mind a működési nyilvántartásokra, mind a szabályozott adatkészletekre (pl. pénzügyi, jogi, HR-, ügyfélkapcsolati és audit szempontból releváns tartalmakra), a tárolási helytől vagy rendszertől függetlenül.

2.4 A szabályzat valamennyi szervezeti egységre, valamint minden munkavállalóra, vállalkozóra és beszállítóra alkalmazandó, akik adatok létrehozásában, tárolásában, kezelésében vagy megsemmisítésében részt vesznek.

3. Célkitűzések

3.1 Biztosítani kell, hogy az adatokat kizárólag addig őrizzék meg, ameddig az jogi, szerződéses vagy működési szempontból szükséges, és ezt követően biztonságosan megsemmisítsék.

3.2 Meg kell előzni azon nyilvántartások idő előtti, jogosulatlan vagy véletlen törlését, amelyek folyamatban lévő működési, megfelelési, peres vagy auditcélokhoz szükségesek.

3.3 Egységes megőrzési rendet kell kialakítani és alkalmazni az információosztályozás, a vagyonelem típusa, az alkalmazandó jogszabályok és a kockázati kitettség alapján.

3.4 Védeni kell az adatok bizalmasságát és adatvédelmét a megőrzési idő alatt és a megsemmisítés időpontjában, beleértve az érintetti jogok teljesítését is (pl. törlés a GDPR 17. cikke alapján).

3.5 Biztosítani kell, hogy minden adatmegsemmisítési módszer visszafordíthatatlan, megfelelően dokumentált és az elismert szabványokkal, például a NIST SP 800-88 előírásaival összhangban álló legyen.

3.6 Minimalizálni kell a túlzott megőrzésből vagy a nyomon nem követett örökölt adatokból eredő működési hatékonyságvesztéseket, többletköltségeket és jogi kitettségeket.

3.7 Támogatni kell az üzletmenet-folytonossági és katasztrófa utáni helyreállítási célkitűzéseket a biztonsági mentések megőrzésének integrált irányítása és az igazolható adatarchiválási gyakorlat révén.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja a jelen szabályzatot, és biztosítja a megfelelő finanszírozást, erőforrásokat, valamint a vállalati kockázatkezelési és megfelelési programokba történő integrációt.

4.1.2 Átfogó felelősséggel tartozik az adatmegőrzéssel és a biztonságos megsemmisítéssel kapcsolatos jogi és szabályozási megfelelésért.

4.2 Információbiztonsági vezető

4.2.1 A szabályzat gazdája, és felelős az adatmegőrzési és megsemmisítési irányítás meghatározásáért és felülvizsgálatáért az IBIR-rel összhangban.

4.2.2 Biztosítja, hogy az osztályozásvezérelt megőrzési és megsemmisítési követelmények megvalósuljanak az üzleti területeken és a technikai rendszerekben.

4.2.3 Nyomon követi a szabályzatnak való megfelelést, és szükség esetén helyesbítő intézkedéseket rendel el.

[... 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 évente, vagy az alábbi feltételek bármelyikének bekövetkezése esetén felül kell vizsgálni:

9.1.1 Az adatmegőrzést érintő alkalmazandó jogszabályok vagy szabályozások változása (pl. GDPR, adójogi előírások vagy a DORA-rendelet módosulása)

9.1.2 Az osztályozási keretrendszer vagy az üzleti folyamatok olyan módosítása, amely hatással van az adat-életciklus szakaszaira

9.1.3 Új IT-rendszerek, archiválási platformok vagy adathordozó-megsemmisítési technológiák bevezetése

9.1.4 Olyan belső auditmegállapítások vagy szabályozói ajánlások, amelyek hiányosságokra mutatnak rá az adatmegőrzési vagy megsemmisítési gyakorlatban

9.2 A felülvizsgálatot az információbiztonsági vezető és az adatvédelmi tisztviselő (DPO) vezeti, a jogi, megfelelési, IT- és üzleti területek bevonásával.

9.3 A központi adatmegőrzési rendet (MDRS) és a megsemmisítési nyilvántartást párhuzamosan kell felülvizsgálni annak biztosítására, hogy:

9.3.1 A megőrzési rend pontos maradjon, és tükrözze a működési, jogi és szabályozási igényeket

9.3.2 A megsemmisítési dokumentáció teljes és auditálható legyen

9.3.3 A jogi zárolási nyilvántartások ellenőrzöttek legyenek, és a megfelelő időpontban feloldásra kerüljenek

9.4 A szabályzat bármely módosításának:

9.4.1 Formálisan verziózott formában kell megjelennie, és az IBIR dokumentumtárában meg kell őrizni

9.4.2 Tartalmaznia kell a módosítási előzményeket és a változtatás indokolását

9.4.3 A felső vezetés által jóváhagyottnak kell lennie

9.4.4 Az érintett munkatársakkal közölni kell, szükség szerint frissített képzési vagy útmutató anyagokkal együtt

9.5 Jelentős szabályzatmódosítás esetén az érintett munkavállalóknak a közzétételtől számított 30 napon belül célzott képzést kell teljesíteniük a megfelelés fenntartása érdekében.

9.6 Kapcsolódó szabályzatok és összefüggések

10. Kapcsolódó szabályzatok és összefüggések

10.1.1 P4 - Hozzáférés-szabályozási szabályzat: Biztosítja, hogy az adatmegőrzési idő alatt kizárólag jogosult személyek férjenek hozzá az adatokhoz, és hogy a lejárt adatokat a megsemmisítésig korlátozottan kezeljék.

10.1.2 P12 - Eszközkezelési szabályzat: Azonosítja azokat a vagyonelemeket, amelyek olyan adatokat hordoznak, amelyek ütemezett megsemmisítést igényelnek, és nyomon követi életciklusukat a beszerzéstől a megsemmisítésig.

10.1.3 P13 - Adatosztályozási és címkézési szabályzat: Iránymutatást ad azokhoz az osztályozási döntésekhez, amelyek közvetlenül meghatározzák az adatok megőrzési idejét és a szükséges megsemmisítési módot.

10.1.4 P15 - Biztonsági mentési és helyreállítási szabályzat: Meghatározza a biztonsági mentési adathordozók és a replikált adatok megőrzési időszakait és megsemmisítési eljárásait.

10.1.5 P18 - Kriptográfiai kontrollok szabályzata: Támogatja a kriptográfiai törlést a megsemmisítés során, és előírja a titkosítást az adatok tárolása során a megsemmisítésig.

10.1.6 P30 - Incidenskezelési szabályzat: Alkalmazandó azokban az esetekben, amikor a nem megfelelő megsemmisítés potenciális adatvesztéshez, incidenshez vagy szabályozási jogsértéshez vezet.

10.2 Minden kapcsolódó szabályzat szerepet játszik az egységes adatirányítási modell alkalmazásában az osztályozás, az életciklus-kontroll, a hozzáférés-szabályozás és az auditra való felkészültség területén.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll a nemzetközileg elismert szabványokkal és szabályozási keretrendszerekkel, amelyek meghatározzák a biztonságos, megfelelő és hatékony adat-életciklus-gyakorlatokat.

11.2 ISO/IEC 27001:

11.2.1 6.1.3 pont - kockázatkezelési terv: Támogatja a túlzott megőrzéssel, adatsértésekkel vagy megsemmisítési hibákkal kapcsolatos kockázatok kezelését.

11.2.2 8.1 pont - működési tervezés és kontroll: Olyan életciklus-kontrollokat határoz meg, amelyek szabályozzák a tárolást, archiválást és megsemmisítést.

11.3 ISO/IEC 27002:2022 - 5.10, 5.12, 5.30, 5. kontrollok: Gyakorlati útmutatást adnak az elfogadható adathasználathoz, a megőrzés indokoltságához, a szabályozott törléshez és az igazolható nyilvántartáskezeléshez a szervezet kockázattűrésével összhangban.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Auditnaplók megőrzése: Biztosítja az auditnaplók és a megfelelőségi bizonyítékok megfelelő megőrzését.

11.4.2 MP-6 - Adathordozók adattisztítása: Előírja a fizikai és elektronikus adathordozók biztonságos, dokumentált megsemmisítési módszereit.

11.4.3 SI-12 - Információkezelés: Előírja az adatok megfelelő kezelését a megőrzési és megsemmisítési kontrollokkal összhangban.

11.4.4 PL-2 - Rendszerbiztonsági és adatvédelmi terv: Előírja az adat-életciklus-kezelés és a biztonságos megsemmisítési előírások rendszerszintű dokumentálását.

11.5 GDPR (2016/679):

11.5.1 5(1)(e) cikk - Adatminimalizálás és tárolási korlátozás: Előírja, hogy az adatokat nem szabad a szükségesnél hosszabb ideig megőrizni.

11.5.2 17. cikk - Törléshez való jog („elfeledtetéshez való jog”): Előírja a személyes adatok haladéktalan és végleges törlését megalapozott kérelem esetén.

11.5.3 32. cikk - Az adatkezelés biztonsága: Megerősíti az adatok védelmét a megőrzés során, és előírja a lejárt nyilvántartások biztonságos megsemmisítését.

11.6 NIS2 irányelv (2022/2555):

11.6.1 21(2)(a-e) cikk: Előírja, hogy a szervezetek szabályzatokat és technikai intézkedéseket alkalmazzanak a biztonságos adatkezelés érdekében, beleértve a tárolási korlátokat és a megsemmisítési módszereket.

11.7 DORA-rendelet (2022/2554):

11.7.1 5. cikk - Irányítás és kontroll: Előírja a strukturált IKT-kockázatkezelést, beleértve az információ életciklusának biztonságos kezelését.

11.7.2 9. cikk - IKT-kockázatkezelési keretrendszer: Előírja a digitális működés adatmegőrzésére, megsemmisítésére, valamint jogi és szabályozási megfelelésére vonatkozó szabályzatokat.

11.8 COBIT 2019:

11.8.1 DSS01 - Műveletek kezelése: Támogatja az adatmegőrzés nyomon követését és az adatrendszerek közötti következetességet.

11.8.2 DSS05 – Biztonsági szolgáltatások kezelése: Biztosítja a tárolt és archivált adatok védelmét a biztonságos megsemmisítésig.

11.8.3 MEA03 - Megfelelés monitorozása, értékelése és felmérése: Lehetővé teszi az adatmegőrzési szabályok végrehajtásának, a törlési eljárásoknak és a szabályozási megfelelésnek az auditálását.