					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P17					Dokumentum címe: **Adatvédelmi és magánszféra-védelmi 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**

Jogi nyilatkozat (szerzői jog és felhasználási korlátozások)

(C) 2025 Clarysec LLC. All rights reserved.

Ez a dokumentum a Clarysec LLC szellemi tulajdona. A dokumentum semmilyen része nem másolható, nem használható fel újra, nem terjeszthető és nem módosítható kereskedelmi vagy bevezetési célból előzetes, kifejezett írásbeli engedély nélkül.

A jogosulatlan felhasználás szigorúan tilos, és jogi eljárást vonhat maga után.

Licenceléssel kapcsolatban keresse: info@clarysec.com

Vonatkozó szabványokkal és jogszabályokkal összhangban

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.1., 6.1.3., 8.1. és 10. pont	Releváns általános, technikai, valamint folyamatos fejlesztési és adatvédelmi kontrollok
ISO/IEC 27002:2022	5.34., 8.10., 8.11. és 8.12. kontroll	Kontrollok a személyes adatok kezelésére, megőrzésére, törlésére, anonimizálására és az érintetti jogok biztosítására
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Irányítási, kockázatkezelési, hozzáférés-kezelési, naplózási, incidensjelentési és adatvédelmi programkövetelmények
EU GDPR	5., 6., 12–23., 25., 28., 30., 32–34. cikk; 78. preambulumbekezdés	Az adatvédelem alapvető követelményei, az elszámoltathatóság, az érintetti jogok, az érintetti kérelmek kezelése, az incidenskezelés, valamint a beépített és alapértelmezett adatvédelem elvei
EU NIS2	21. cikk (2) bekezdés e) és f) pont	Kockázatalapú biztonsági kontrollok az alapvető és fontos szervezetek számára
EU DORA	6. cikk (2) bekezdés d) pont, 11. cikk (1) bekezdés c) pont, 15. cikk (1) bekezdés, 17. cikk	Irányítási, harmadik félhez kapcsolódó kockázati és biztonságos adatkezelési követelmények
COBIT 2019	APO12, DSS01, DSS05, MEA	Kockázatkezelés, biztonságos üzemeltetés, megfelelőség-felügyelet

1. Cél

1.1 Jelen szabályzat meghatározza a személyes adatok védelmére és a beépített adatvédelem valamennyi környezetben történő érvényesítésére vonatkozó kötelező szervezeti alapelveket és technikai követelményeket.

1.2 A szabályzat rögzíti a szervezet nemzetközi szabványokból és szabályozási keretrendszerekből eredő kötelezettségeit annak biztosítása érdekében, hogy a személyes adatok gyűjtése, kezelése, megőrzése, megosztása és megsemmisítése jogszerűen, biztonságosan és átlátható módon történjen.

1.3 Jelen szabályzat továbbá megerősíti az alkalmazandó adatvédelmi jogszabályoknak és keretrendszereknek való megfelelést, ideértve a GDPR-t, az EU NIS2 irányelvet, az EU DORA-rendeletet, az ISO/IEC 27001:2022 szabványt és a COBIT 2019 keretrendszert.

2. Hatály

2.1 Jelen szabályzat minden olyan szervezeti egységre, munkatársra és rendszerre kiterjed, amely személyes adatok kezelésében részt vesz, beleértve az alábbiakat:

2.1.1 munkavállalók, vállalkozók, tanácsadók és harmadik fél szolgáltatók;

2.1.2 belső és külső forrásokból származó, valamennyi üzleti funkció során gyűjtött adatok;

2.1.3 fizikai és digitális adathordozók, beleértve a felhőszolgáltatásokat, a SaaS-platformokat, a mobileszközöket és a papíralapú nyilvántartásokat;

2.1.4 valamennyi környezet, ideértve az éles, fejlesztési, teszt- és biztonsági mentési rendszereket, ahol személyes adatok előfordulhatnak.

2.2 A szabályzat valamennyi olyan adatkezelési tevékenységre kiterjed, amelyet az alkalmazandó adatvédelmi jogszabályok és szabványok szabályoznak, különösen az alábbiakra:

2.2.1 személyes adatok gyűjtése, tárolása, felhasználása, továbbítása és megsemmisítése;

2.2.2 érintetti jogok érvényesítése, a jogalap dokumentálása, hozzájárulások kezelése;

2.2.3 határokon átnyúló adattovábbítások, incidensjelentés és személyes adatok harmadik felekkel történő megosztása;

2.2.4 a beépített és alapértelmezett adatvédelem érvényesítése rendszerekben és folyamatokban.

3. Célkitűzések

3.1 A személyes adatok jogszerű, átlátható és elszámoltatható kezelése az ISO/IEC 27001:2022 szabvánnyal és a kapcsolódó jogi kötelezettségekkel összhangban.

3.2 A beépített és alapértelmezett adatvédelem elveinek beépítése valamennyi információs rendszerbe, szolgáltatásba és üzleti folyamatba.

3.3 Olyan technikai és szervezési intézkedések (TOM) érvényesítése, amelyek a személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását teljes életciklusuk során védik.

3.4 Az adatvédelemhez kapcsolódó irányítási szerepkörök és elszámoltathatósági struktúrák meghatározása, beleértve az adatvédelmi tisztviselő (DPO), az információbiztonság, a jogi és megfelelőségi terület, valamint az adatgazdák feladatait.

3.5 A GDPR 5., 6., 25., 30. és 32. cikkének, továbbá a NIS2 és a DORA szerinti kockázatcsökkentési és reziliencia-követelményeknek való teljes megfelelés biztosítása.

3.6 Az érintetti jogok biztosítása, beleértve a hozzáféréshez, helyesbítéshez, törléshez, az adatkezelés korlátozásához, az adathordozhatósághoz és a tiltakozáshoz való jogot, valamint az automatizált döntéshozatallal szembeni védelmet.

3.7 A személyes adatokhoz való jogosulatlan hozzáférésből, azok helytelen felhasználásából vagy elvesztéséből eredő szabályozási, reputációs, jogi és működési kockázatok csökkentése.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Stratégiai felügyeletet biztosít, és megfelelő erőforrásokat rendel az adatvédelmi program támogatásához.

4.1.2 Jóváhagyja jelen szabályzatot, és biztosítja annak érvényesítését a teljes szervezetben.

4.2 Adatvédelmi tisztviselő (DPO)

4.2.1 Független módon jár el az adatvédelmi jogszabályoknak való megfelelés felügyelete érdekében.

4.2.2 Fenntartja a GDPR 30. cikke szerinti adatkezelési tevékenységek nyilvántartását (RoPA).

4.2.3 Irányítja a felügyeleti hatóságokkal való kapcsolattartást, adatvédelmi hatásvizsgálatokat (DPIA) végez, és kezeli az incidensjelentési folyamatokat.

4.2.4 Felülvizsgálja az adatvédelmi kivételeket, és fenntartja az adatvédelmi kivételnyilvántartást.

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

9.1 Jelen szabályzatot legalább évente egyszer, illetve az alábbi esetek bármelyikében korábban felül kell vizsgálni:

9.1.1 jelentős jogi vagy szabályozási változások esetén, például a GDPR módosítása vagy a DORA határidejének változása;

9.1.2 új, személyes adatokat érintő rendszerek vagy adatkezelési tevékenységek bevezetésekor;

9.1.3 olyan belső auditmegállapítások esetén, amelyek szabályzati hiányosságokra utalnak;

9.1.4 jelentős személyesadat-sértések vagy felügyeleti hatósági visszajelzés esetén.

9.2 Felülvizsgálati felelősségek

9.2.1 A DPO kezdeményezi a szabályzat felülvizsgálatát a jogi és megfelelőségi, a kockázatkezelési, az információbiztonsági terület és a felső vezetés bevonásával.

9.2.2 Minden frissítést rögzíteni kell az IBIR dokumentumkezelési nyilvántartásában, és el kell juttatni az érintett érdekelt felek részére.

9.3 Változáskezelés

9.3.1 Jelen szabályzat bármely módosítását a felső vezetésnek formálisan jóvá kell hagynia.

9.3.2 Az elavult verziókat biztonságosan archiválni kell, a frissített verziónak pedig dokumentált változáselőzményeket kell tartalmaznia.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 – Információbiztonsági szabályzat. Meghatározza azokat az átfogó biztonságirányítási elveket, amelyek megalapozzák jelen adatvédelmi szabályzatot. A P1 támogatja a személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását valamennyi rendszerben és szolgáltatásban.

10.2 P6 – Kockázatkezelési szabályzat. Meghatározza a szervezet kockázatkezelési módszertanát, amely elengedhetetlen az adatvédelmi kockázatok értékeléséhez, a DPIA-folyamatokhoz és a GDPR, valamint az ISO/IEC 27001 6.1.3. pontja által megkövetelt maradványkockázat-értékelésekhez.

10.3 P13 – Adatosztályozási és jelölési szabályzat. Iránymutatást ad a személyes és érzékeny adatok kategorizálásához, amely alapul szolgál a megfelelő adatvédelmi kontrollok alkalmazásához, ideértve a megőrzési követelmények érvényesítését, a hozzáférés korlátozását és a biztonságos megsemmisítést.

10.4 P14 – Adatmegőrzési és megsemmisítési szabályzat. Közvetlenül támogatja a GDPR 5. cikk (1) bekezdés e) pontja és 17. cikke szerinti adatvédelmi követelményeket, biztosítva, hogy a személyes adatok megőrzése kizárólag a szükséges ideig történjen, és megsemmisítésük a jogi kötelezettségekkel összhangban, biztonságosan valósuljon meg.

10.5 P16 – Adatmaszkolási és álnevesítési szabályzat. Olyan kontrollokat határoz meg, amelyek technikai intézkedésekkel – például tokenizációval, dinamikus maszkolással és álnevesítéssel – csökkentik a személyes adatok azonosíthatóságát, ezáltal érvényesítve a GDPR 32. cikkét és az ISO/IEC 27002 5.34. kontrollját.

10.6 P30 – Incidenskezelési szabályzat. Meghatározza azokat a kötelező incidenskezelési protokollokat, amelyek illeszkednek a GDPR 33. és 34. cikke szerinti adatvédelmi incidenskezelési és bejelentési határidőkhöz.

10.7 P33 – Audit- és megfelelőségfelügyeleti szabályzat. Előírja az adatvédelmi program hatékonyságának, a szabályzat betartásának és a helyesbítő intézkedések nyomon követésének ütemezett értékelését a szervezeti egységek és a személyes adatokat kezelő harmadik felek körében.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 5.1. pont – Vezetés és elkötelezettség: Meghatározza a felső vezetés felelősségét a személyes adatok védelméért és az adatvédelmi elvek érvényesítéséért.

11.1.2 6.1.3. pont – Információbiztonsági kockázatkezelés: Támogatja az adatvédelmi kockázatok azonosítását, értékelését és kezelését DPIA-kon és kivételeken keresztül.

11.1.3 8.1. pont – Operatív tervezés és felügyelet: Előírja a technikai és eljárási védelmi intézkedéseket a személyes adatok biztonságos kezelése érdekében.

11.1.4 10.1. pont – Folyamatos fejlesztés: Kötelezővé teszi az adatvédelmi program időszakos értékelését és továbbfejlesztését.

11.2 ISO/IEC 27002:2022 5.34., 8.10., 8.11. és 8.12. kontroll: Iránymutatást ad a személyes adatok kezelésére, a megőrzésre, törlésre, anonimizálásra és az érintetti jogok átlátható biztosítására.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Meghatározza az irányítási, szerepköri, elszámoltathatósági és adatvédelmi képzési kötelezettségeket.

11.3.2 PL-2, PL-8: Előírja az adatvédelmi kontrollok integrálását a rendszer-életciklusba és a vállalati architektúrába.

11.3.3 AC-2, AC-6: Érvényesíti a legkisebb jogosultság elvét és a fiókkezelést a személyes adatok védelme érdekében.

11.3.4 AU-2, AU-6, AU-9: Előírja a naplózást, a visszakövethetőséget és az auditnyomok sértetlenségét a személyes adatokhoz való hozzáférés tekintetében.

11.3.5 IR-4, IR-5, IR-6: Meghatározza az adatvédelmi incidensek strukturált észlelési, elemzési és jelentési folyamatait.

11.3.6 PM-1, PM-21, PM-23: Átfogó adatvédelmi program kialakítását írja elő, stratégiai kockázati és adatirányítási célokhoz igazítva.

11.4 GDPR (2016/679)

11.4.1 5., 6., 12–23., 25., 28., 30., 32–34. cikk: Szabályozza a jogszerű adatkezelést, a célhoz kötöttséget, az érintetti jogokat, az elszámoltathatóságot, a beépített és alapértelmezett adatvédelmet, a harmadik felek kötelezettségeit és az incidenskezelést.

11.4.2 78. preambulumbekezdés: Megerősíti a beépített adatvédelem elveit.

11.5 EU NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés e) és f) pont: Előírja a kockázatalapú biztonsági kontrollok bevezetését és a személyes adatok védelmét az alapvető és fontos szervezetek körében.

11.6 EU DORA (2022/2554)

11.6.1 6. cikk (2) bekezdés d) pont: Előírja az adatkezeléshez kapcsolódó IKT-kockázatok belső irányítását.

11.6.2 11. cikk (1) bekezdés c) pont: Kötelezővé teszi az adatokhoz kapcsolódó szolgáltatások harmadik félhez kapcsolódó kockázatának felügyeletét.

11.6.3 15. cikk (1) bekezdés és 17. cikk: Előírja a szolgáltatók általi biztonságos adatkezelést és az IKT-val kapcsolatos incidenseket követő időben történő felügyeleti tájékoztatást.

11.7 COBIT 2019

11.7.1 APO12 – Kockázatkezelés: Az adatvédelmi kockázatokat beépíti a szélesebb körű vállalati kockázatfelügyeletbe.

11.7.2 DSS01 – Menedzselt üzemeltetés és DSS05 – Biztonsági szolgáltatások kezelése: Biztosítja a biztonságos működést, beleértve a hozzáférés-szabályozást, a megőrzést és a rendszerek sértetlenségét.

11.7.3 MEA03 – Megfelelés nyomon követése: Előírja a szabályozási és szabályzati alapú adatvédelmi kötelezettségek teljesülésének folyamatos felülvizsgálatát.