					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P17S					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**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.1., 6.1.3., 8. pont	
ISO/IEC 27002:2022	5.34., 8.10–8. pont	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
GDPR	5., 6., 12–23., 30., 32–34. cikk	
NIS2 irányelv	21. cikk (2) bekezdés e), 21. cikk (2) bekezdés f) pont	
DORA-rendelet	6., 15., 17. cikk	
COBIT 2019	APO12, DSS05, MEA	

1. Cél

1.1. Jelen szabályzat meghatározza, hogy a szervezet miként védi a személyes adatokat a jogi kötelezettségekkel, a szabályozási keretrendszerekkel és a nemzetközi biztonsági szabványokkal összhangban.

1.2. Biztosítja, hogy az ügyfelekre, munkatársakra vagy partnerekre vonatkozó személyes adatok gyűjtése, felhasználása, tárolása és törlése jogszerűen, tisztességesen és biztonságos módon történjen.

1.3. Jelen szabályzat támogatja továbbá az ISO/IEC 27001:2022 követelményeinek való megfelelést, valamint az auditkészültséget azáltal, hogy a magánszféra védelmére egységes, kockázatalapú megközelítést ír elő.

1.4. A szervezet e szabályzat révén igazolja elszámoltathatóságát, és erősíti az ügyfelek bizalmát az átláthatóság, az adattakarékosság és a szilárd adatvédelmi irányítás előtérbe helyezésével.

2. Hatály

2.1. Jelen szabályzat az alábbiakra terjed ki:

2.1.1. minden munkavállalóra, vállalkozóra vagy szolgáltatóra, aki személyes adatokhoz hozzáfér, azokat kezeli vagy adminisztrálja;

2.1.2. minden olyan rendszerre, alkalmazásra vagy helyszínre, ahol személyes adatokat tárolnak vagy továbbítanak;

2.1.3. valamennyi személyes adatra, függetlenül attól, hogy azokat elektronikusan, papíralapon, felhőkörnyezetben vagy mobileszközökön tárolják.

2.2. Jelen szabályzat kiterjed az ügyfelekre, munkatársakra, beszállítókra és bármely más azonosítható természetes személyre vonatkozó adatokra.

2.3. A szabályzat attól függetlenül hatályban marad, hogy az adatkezelés belsőleg vagy harmadik fél szolgáltató által történik.

3. Célkitűzések

3.1. Biztosítani kell, hogy a személyes adatok kezelése az adatvédelmi jogszabályokkal és biztonsági szabványokkal, ideértve a GDPR-t, a NIS2 irányelvet és az ISO/IEC 27001 szabványt, összhangban történjen.

3.2. A személyes adatokat egyértelmű technikai és szervezési kontrollokkal kell védeni a jogosulatlan hozzáféréssel, visszaélésszerű felhasználással, módosítással vagy elvesztéssel szemben.

3.3. Tiszteletben kell tartani az érintettek adatvédelmi jogait, ideértve a személyes adataikhoz való hozzáféréshez, azok helyesbítéséhez és törléséhez való jogot.

3.4. Egyértelmű szerepköröket és felelősségi köröket kell meghatározni a szervezeten belüli adatvédelem vonatkozásában.

3.5. Valamennyi rendszerben és folyamatban érvényesíteni kell az adattakarékosságot, a biztonságos megőrzést és az időben történő törlést.

3.6. Csökkenteni kell a nemmegfelelés, a jogi szankciók, a reputációs károk és az ügyfélbizalom csökkenésének kockázatát.

4. Szerepkörök és felelősségi körök

4.1. Ügyvezető

4.1.1. jóváhagyja jelen szabályzatot, és biztosítja annak betartását;

4.1.2. biztosítja az adatvédelmi kockázatok kezeléséhez és az incidensekre adott intézkedésekhez szükséges erőforrásokat;

4.1.3. átfogó elszámoltathatósággal tartozik az adatvédelmi jogszabályoknak és szabványoknak való megfelelésért.

4.2. Adatvédelmi koordinátor (belső vagy kiszervezett)

4.2.1. fenntartja az adatkezelési tevékenységek nyilvántartását;

4.2.2. kezeli az érintetti kérelmeket és a felügyeleti hatóságok megkereséseit;

4.2.3. támogatja a kockázatértékeléseket, a képzéseket és a szabályzat végrehajtását;

4.2.4. dokumentálja az adatvédelmi incidenseket, és szükség esetén értesíti a hatóságokat.

[... 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. Ütemezett felülvizsgálatok

9.1.1. Jelen szabályzatot legalább 12 havonta egyszer az adatvédelmi koordinátornak felül kell vizsgálnia, és azt az ügyvezetőnek jóvá kell hagynia.

9.1.2. A felülvizsgálatnak értékelnie kell a szabályzat aktualitását, szabályozási összhangját és működési hatékonyságát.

9.2. Soron kívüli felülvizsgálat kiváltó okai

9.2.1. A szabályzat frissítését az alábbi esetekben is kezdeményezni kell:

9.2.1.1. új vagy módosított adatvédelmi jogszabályok esetén (pl. GDPR, DORA-rendelet);

9.2.1.2. személyes adatokat érintő biztonsági incidensek vagy adatvédelmi incidensek esetén;

9.2.1.3. személyes adatokat kezelő új rendszerek, eszközök vagy szolgáltatások bevezetése esetén;

9.2.1.4. lényeges auditmegállapítások vagy szabályozói ajánlások esetén.

9.3. Változáskezelés és kommunikáció

9.3.1. A szabályzat valamennyi módosítását formálisan dokumentálni kell a változásnaplóban.

9.3.2. A módosított verziókat valamennyi munkatárs és érintett vállalkozó részére ki kell küldeni.

9.3.3. Az archivált verziókat a megfelelés auditnyomvonalának biztosítása érdekében meg kell őrizni.

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat más KKV-szabályzatokkal együtt teljes körű és végrehajtható adatvédelmi keretrendszert alkot:

10.1.1. P13S – Adatosztályozási és jelölési szabályzat: biztosítja, hogy a személyes adatok megfelelő osztályozást kapjanak, így az adatvédelmi intézkedések kockázatalapon alkalmazhatók.

10.1.2. P14S – Adatmegőrzési és selejtezési szabályzat: egyértelmű szabályokat határoz meg arra vonatkozóan, hogy a személyes adatokat mennyi ideig kell megőrizni, valamint milyen biztonságos módszerekkel kell azokat a megőrzési idő lejártát követően megsemmisíteni.

10.1.3. P16S – Adatmaszkolási és pszeudonimizálási szabályzat: meghatározza, hogyan kell a személyazonosító adatokat átalakítani, mielőtt az adatokat nem éles környezetben használnák vagy külső féllel megosztanák.

10.1.4. P30S – Incidenskezelési szabályzat: lefedi az adatsértések kezeléséhez szükséges lépéseket, beleértve a felügyeleti hatóságok és az érintettek értesítését az előírt határidőkön belül.

10.1.5. P2S – Irányítási szerepkörök és felelősségek szabályzata: tisztázza az adatvédelmi alkalmazásra és felügyeletre vonatkozó elszámoltathatósági struktúrát és döntési szerepköröket.

10.2. E kapcsolódó szabályzatokat együtt kell felülvizsgálni és alkalmazni annak érdekében, hogy a rendszerek, a munkatársak és a beszállítók vonatkozásában teljes körű adatvédelmi lefedettség valósuljon meg.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 5.1. pont – Előírja, hogy a felső vezetés vezetői szerepvállalást és elkötelezettséget tanúsítson a személyes adatok védelme iránt.

11.1.2. 6.1.3. pont – Előírja a személyes adatok kezeléséhez kapcsolódó kockázatok kezelését.

11.1.3. 8.1. pont – Előírja olyan működési kontrollok bevezetését, amelyek az adatokat teljes életciklusuk során védik.

11.2. ISO/IEC 27002

11.2.1. 5.34. kontroll – Végrehajtási útmutatást ad a magánszféra védelméhez és a személyes adatok (PII) biztonságos kezeléséhez.

11.2.2. 8.10. kontroll – A személyes adatok biztonságos megsemmisítésével foglalkozik a fennmaradó közzétételi kockázat megelőzése érdekében.

11.2.3. 8.11. kontroll – Támogatja a maszkolás és a pszeudonimizálás alkalmazását az adattakarékosság érdekében.

11.2.4. 8.12. kontroll – Az adatokhoz való hozzáférésre és az adatfelhasználásra vonatkozó kontrollokkal megelőzi a jogosulatlan adatszivárgást.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – Szerepköröket és felelősségi köröket rendel a magánszférát érintő kockázatok kezeléséhez.

11.3.2. PL-5 – Előírja az adatfelhasználást és az adatvédelmet lefedő adatvédelmi terv dokumentálását.

11.3.3. AC-6 – Előírja a legkisebb jogosultság elvének és a hozzáférés-szabályozásnak az alkalmazását a személyes adatok esetében.

11.3.4. IR-4 – Előírja a személyes adatokat érintő incidensekre vonatkozó incidenskezelési folyamatokat.

11.4. GDPR

11.4.1. 5. cikk – Meghatározza a jogszerű, tisztességes és átlátható adatkezelés alapelveit.

11.4.2. 6. cikk – Előírja, hogy minden személyesadat-kezelési tevékenységhez érvényes jogalap tartozzon.

11.4.3. 12–23. cikk – Meghatározza az érintetti jogokat, beleértve a hozzáférést, a helyesbítést, a törlést és a tiltakozást.

11.4.4. 30. cikk – Előírja az adatkezelési tevékenységek nyilvántartását.

11.4.5. 32. cikk – Előírja a megfelelő technikai és szervezési biztonsági intézkedések alkalmazását.

11.4.6. 33–34. cikk – Meghatározza a hatóságok és az érintettek felé fennálló incidensbejelentési kötelezettségeket.

11.5. NIS2 irányelv

11.5.1. 21. cikk (2) bekezdés e) pont – Előírja az adatvédelmet a kiberbiztonsági szabályzatokkal összhangban biztosító intézkedéseket.

11.5.2. 21. cikk (2) bekezdés f) pont – Előírja a személyes és bizalmas adatok IKT-rendszerekben történő biztonságos kezelését biztosító mechanizmusokat.

11.6. DORA-rendelet

11.6.1. 6. cikk – Előírja az adatkockázat és az adatvédelem kezelését biztosító belső irányítási keretrendszereket.

11.6.2. 15. cikk – Kötelezi a pénzügyi szervezeteket annak biztosítására, hogy a harmadik fél szolgáltatók védjék a személyes adatokat és támogassák a jogszabályi megfelelést.

11.6.3. 17. cikk – Előírja, hogy a személyes adatokat kezelő IKT-rendszerek biztonságosak, reziliensek és felügyeltek legyenek.

11.7. COBIT 2019

11.7.1. APO12 – Kockázatkezelés: előírja a magánszférát és az adatvédelmet érintő kockázatok azonosítását és kezelését.

11.7.2. DSS05 – Biztonsági szolgáltatások kezelése: előírja a személyes adatokhoz való jogosulatlan hozzáférés megelőzését szolgáló védelmi intézkedéseket.

11.7.3. MEA03 – A megfelelés nyomon követése: előírja, hogy a szervezetek folyamatosan biztosítsák az adatvédelmi és magánszféra-védelmi jogszabályoknak való megfelelést.