					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P37					Dokumentum címe: **Jogi és szabályozói megfelelési 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**

1. Cél

1.1 Jelen szabályzat meghatározza a szervezet információbiztonságára, adatvédelmére és működési folyamataira vonatkozó valamennyi jogi, szabályozási és szerződéses kötelezettség azonosításának, kezelésének és teljesítésének kötelező keretrendszerét.

1.2 A szabályzat célja a meg nem felelés megelőzése, amely bírsághoz, jogi felelősséghez, üzletmenet-fennakadáshoz, reputációs károkhoz vagy szabályozói intézkedéshez vezethet.

1.3 Jelen szabályzat támogatja a megfelelőségi követelmények integrálását az irányításba, a kockázatkezelésbe, a működési folyamatokba, a projekt-életciklusokba és a rendszertervezésbe.

1.4 A szabályzat biztosítja, hogy a különböző joghatóságokból, iparágakból és szabályozási hatókörökből eredő releváns kötelezettségek a szervezeten belül egyértelműen dokumentáltak, értékeltek, nyomon követettek és betartottak legyenek.

2. Hatály

2.1 Jelen szabályzat a szervezet nevében eljáró valamennyi szervezeti egységre, funkcióra, üzleti területre és személyre alkalmazandó, ideértve az alábbiakat:

2.1.1 Állandó és ideiglenes munkavállalók

2.1.2 Vállalkozók, tanácsadók és gyakornokok

2.1.3 Olyan harmadik fél beszállítók, adatfeldolgozók vagy partnerek, akik a szervezet adatait, rendszereit vagy szabályozási felelősségi köreit kezelik

2.1.4 Bármely üzleti folyamat, projekt vagy kezdeményezés, amely jogi vagy szabályozási követelmények hatálya alá tartozik

2.2 A jelen szabályzat által szabályozott megfelelési területek különösen az alábbiakat foglalják magukban:

2.2.1 Információbiztonsági és kiberbiztonsági kötelezettségek (pl. ISO/IEC 27001, NIS2, DORA)

2.2.2 Adatvédelmi és magánélet-védelmi jogszabályok (pl. GDPR, ágazatspecifikus adatvédelmi jogszabályok)

2.2.3 Ágazati szabályozások (pl. pénzügyi, egészségügyi, gépjárműipari, védelmi)

2.2.4 Titoktartási megállapodásokból, szolgáltatási szintre vonatkozó megállapodásokból (SLA-k) vagy harmadik féllel kötött adatfeldolgozási megállapodásokból eredő szerződéses kötelezettségek

2.2.5 Az incidensjelentéssel, a bűnüldöző hatóságokkal való együttműködéssel és a nemzetközi adattovábbítással kapcsolatos jogi követelmények

3. Célkitűzések

3.1 Annak biztosítása, hogy valamennyi alkalmazandó jogszabály, szabályozás, szabvány és szerződéses kötelezettség a szervezet egészében azonosított, dokumentált, értelmezett és betartott legyen.

3.2 A jogi és szabályozási követelmények integrálása a szervezet információbiztonság-irányítási rendszerébe, kockázatkezelési folyamataiba, beszállítói megállapodásaiba, valamint termék- és szolgáltatástervezésébe.

3.3 Olyan mechanizmus biztosítása, amely lehetővé teszi a szabályozási változások proaktív nyomon követését, valamint a kontrollok és a dokumentáció ennek megfelelő frissítését.

3.4 Egyértelmű elszámoltathatóság meghatározása a megfelelési felügyelet, a szabálysértések eszkalációja, a kivételkezelés és a külső jelentéstétel tekintetében.

3.5 Annak biztosítása, hogy a szervezet jogi és szabályozói megfelelési helyzete auditok, vizsgálatok vagy tanúsítási felülvizsgálatok során ellenőrizhető és igazolható legyen.

4. Szerepkörök és felelősségek

4.1 Felső vezetés

4.1.1 Felelős a jogi és szabályozási megfelelés vállalati szintű stratégiai elszámoltathatóságáért.

4.1.2 Felülvizsgálja és jóváhagyja a magas kockázatú megfelelőségi döntéseket, beleértve a kockázatelfogadást és a jogvitákat.

4.2 Megfelelőségi vezető / jogtanácsos / jogi vezető

4.2.1 Fenntartja a megfelelőségi kötelezettségek nyilvántartását, amely tartalmazza valamennyi alkalmazandó jogszabályt, szabványt, tanúsítást és szerződéses záradékot.

4.2.2 Jogi hatásvizsgálatot végez új szolgáltatások, piacok vagy adatáramlások esetén.

4.2.3 Hiteles értelmezést ad a jogszabályokról és szabványokról.

[... 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 Éves szabályzatfelülvizsgálat

9.1.1 Jelen szabályzatot naptári évenként legalább egyszer felül kell vizsgálni az alábbi célokból:

9.1.1.1 Annak biztosítása, hogy továbbra is összhangban legyen a frissített jogszabályokkal, iparági szabványokkal és szabályozási keretrendszerekkel

9.1.1.2 A működési hatékonyság ellenőrzése az auditmegállapítások és az incidenselőzmények alapján

9.1.1.3 A szervezeti változások tükrözése (pl. új joghatóságok, rendszerek vagy üzleti területek)

9.2 Eseményalapú felülvizsgálatok

9.2.1 Soron kívüli felülvizsgálatot kell indítani, ha:

9.2.2 új jogi vagy szabályozási követelmény lép hatályba vagy módosul

9.2.3 egy megfelelési incidens vagy audit a szabályzat hiányosságait tárja fel

9.2.4 a szervezet olyan új piacra vagy szolgáltatási területre lép, amely eltérő megfelelési keretrendszer hatálya alá tartozik

9.2.5 a végrehajtási trendek vagy a szabályozó hatósági útmutatások a kockázati helyzet változását jelzik

9.3 Tulajdonosi felelősség és jóváhagyás

9.3.1 A jogi terület és a megfelelőségi vezető együttesen felelősek a felülvizsgálati folyamat koordinálásáért.

9.3.2 A szabályzat végleges módosításait a felső vezetésnek kell jóváhagynia, és azokat a szabályzatváltozási nyilvántartásban kell rögzíteni a kapcsolódó változáskezelési hivatkozásokkal és kommunikációs tervekkel együtt.

9.4 Verziókezelés és kommunikáció

9.4.1 Jelen szabályzat bármely frissített változatának:

9.4.1.1 tartalmaznia kell a változások összefoglalását

9.4.1.2 hivatalos csatornákon keresztül ismételten közzé kell tenni (pl. szabályzati portál, tanulásmenedzsment rendszer, belső hírlevelek)

9.4.1.3 az érintett munkatársaktól tudomásulvételt kell megkövetelnie, különösen a jogi, működési, biztonsági és beszállítókezelési szerepkörökben

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat a szervezet IBIR-én belül az alábbi szabályzatokkal együtt alkalmazandó, és azok rendelkezéseit erősíti:

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza azokat az alapvető irányítási elveket, amelyek biztosítják, hogy valamennyi információbiztonsági szabályzat — beleértve a megfelelési szabályzatokat is — összhangban legyen a stratégiai üzleti és szabályozási követelményekkel.

10.1.2 P2 – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza a döntési jogosultságokat, beleértve a szabályozói felügyeletért és elszámoltathatóságért felelős jogi és megfelelőségi szerepköröket.

10.1.3 P6 – Kockázatkezelési szabályzat: Támogatja a jogi és szabályozói megfelelési kockázatok vállalati szintű értékelését, a tulajdonosok kijelölését és a kezelését.

10.1.4 P8 – Információbiztonsági tudatossági és képzési szabályzat: Biztosítja, hogy valamennyi munkatárs ismerje a megfelelési kötelezettségeit, és a szerepkörének megfelelő képzésben részesüljön.

10.1.5 P12 – Eszközkezelési szabályzat: Megerősíti a szabályozott vagy szerződéses kötöttségű eszközök kezelésére és védelmére vonatkozó jogi kötelezettségeket, beleértve a személyes adatokat és a kritikus infrastruktúrát érintő eszközöket is.

10.1.6 P30 – Incidenskezelési szabályzat: Szabályozza a kötelező jogi értesítéseket (pl. GDPR 33. cikk) és az eszkalációs eljárásokat megfelelési incidens vagy szabályozói esemény esetén.

10.1.7 P33 – Audit- és megfelelésfelügyeleti szabályzat: Olyan strukturált bizonyossági tevékenységeket biztosít — beleértve a kontrolltesztelést és a bizonyító dokumentumok gyűjtését —, amelyek a belső és külső megfelelőség-ellenőrzéshez szükségesek.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 4.2. pont – Az érdekelt felek igényeinek és elvárásainak megértése: Előírja a jogi és szabályozási követelmények azonosítását és integrálását az IBIR-be.

11.1.2 5.1. pont – Vezetés és elkötelezettség: Előírja a vezetői elszámoltathatóságot a jogi megfelelés szervezeti szintű kialakításáért és fenntartásáért.

11.1.3 5.3. pont – Szervezeti szerepkörök, felelősségek és hatáskörök: Biztosítja a jogi felügyelet és a szabályozói megfelelés szerepköreinek egyértelmű meghatározását.

11.1.4 A melléklet 5.36. kontrollja – Jogi, jogszabályi, szabályozási és szerződéses követelményeknek való megfelelés: Meghatározza a jogszabályokból, szabályozásokból és szerződésekből eredő kötelezettségek azonosításának és teljesítésének követelményét.

11.2 ISO/IEC 27002

11.2.1 5.36. kontroll: Bevezetési útmutatást ad a megfelelőségi kötelezettségek nyilvántartásának fenntartásához, a szabályozási követelmények ellenőrzéséhez és a strukturált bizonyítékmegőrzés biztosításához.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Biztonságtervezési szabályzat és eljárások: Előírja, hogy a megfelelési követelmények beépüljenek az irányítási struktúrákba és a dokumentációba.

11.3.2 PM-1 – Információbiztonsági programterv: Előírja a szabályozási kontrollok alkalmazását a tágabb biztonsági program részeként.

11.3.3 CA-7 – Folyamatos monitorozás: Támogatja a kontrollok hatékonyságának felügyeletét a jogi és szabályzati követelmények teljesítése érdekében.

11.3.4 AU-9 – Auditinformációk védelme: Biztosítja, hogy a megfelelőségi auditnaplók és nyilvántartások védettek és ellenőrzés céljára rendelkezésre álljanak.

11.4 GDPR (2016/679)

11.4.1 5. cikk – Az adatkezelésre vonatkozó alapelvek: Előírja a jogszerű adatkezelést, az átláthatóságot és az elszámoltathatóságot.

11.4.2 6. cikk – Az adatkezelés jogszerűsége: Előírja a megfelelő jogalap alkalmazását valamennyi adatkezelési tevékenység esetén.

11.4.3 24. cikk – Az adatkezelő felelőssége: Közvetlen elszámoltathatóságot állapít meg a szabályozói megfelelés biztosításáért.

11.4.4 32. cikk – Az adatkezelés biztonsága: Megköveteli a megfelelő technikai és szervezési intézkedések bevezetését.

11.4.5 33. cikk – Incidensbejelentés: Előírja, hogy a személyes adatok megsértésével járó incidenseket 72 órán belül jelenteni kell az illetékes hatóságnak.

11.5 NIS2 irányelv (2022/2555)

11.5.1 20–21. cikk: Előírja, hogy az alapvető és fontos szervezetek dokumentált irányítást, jogi megfelelési stratégiákat és a jogi kockázatok folyamatos felülvizsgálatát valósítsák meg.

11.6 DORA-rendelet (2022/2554)

11.6.1 5. cikk (2) bekezdés – IKT-kockázatkezelési keretrendszer: Előírja a jogi megfelelés integrálását a tágabb kockázatkezelési és felügyeleti funkciókba.

11.6.2 19. cikk – IKT-harmadikfél-kockázat: Konkrét jogi követelményeket állapít meg a külső beszállítókat és platformokat érintő szerződéses és szabályozási kötelezettségek kezelésére.

11.7 COBIT 2019

11.7.1 APO12 – Kockázatkezelés: A jogi és szabályozói megfelelést a vállalati kockázatirányítás kritikus elemének tekinti.

11.7.2 MEA03 – Külső követelményeknek való megfelelés nyomon követése: Meghatározza a szabályozási kötelezettségek valamennyi formájára vonatkozó folyamatos nyomon követést, a kivételkezelést és az auditra való felkészültséget.