					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P37S					Dokumentum címe: **Jogi és szabályozási 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**

A szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.1., 6.1., 6.2. és 8. pont	
ISO/IEC 27002:2022	5. kontroll	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
GDPR	5., 6., 32. és 33. cikk	
NIS2 irányelv	21. cikk (2) bekezdés a) és f) pont, 23. cikk	
DORA rendelet	5. cikk (2) bekezdés, 9. cikk (1) bekezdés, 17. cikk	
COBIT 2019	APO12, APO13, DSS01	

1. Cél

1.1 Jelen szabályzat meghatározza a szervezet megközelítését a jogi, szabályozási és szerződéses kötelezettségek azonosítására, a megfelelés biztosítására, valamint a követelmények teljesítésének igazolására.

1.2 A szabályzat egyértelmű felelősségi köröket és gyakorlati lépéseket határoz meg annak érdekében, hogy a vállalkozás teljesíteni tudja megfelelési kötelezettségeit, ideértve az adatvédelmi jogszabályokat, a kiberbiztonsági keretrendszereket, az ügyfélszerződéseket és a tanúsítási követelményeket.

1.3 A szabályzat biztosítja, hogy a vállalkozás külön megfelelőségi csapat nélkül is jogszerű működést tartson fenn, megfelelően reagáljon az incidensekre, valamint fenntartsa az auditra való felkészültséget.

1.4 Ez a szabályzat alapvető az ISO/IEC 27001:2022 szerinti tanúsítás támogatásához, valamint az ügyfelek, a szabályozó hatóságok és a partnerek külső elvárásainak teljesítéséhez.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi munkavállalóra, vállalkozóra, szabadúszóra és harmadik fél beszállítóra;

2.1.2 valamennyi szolgáltatásra, működési tevékenységre, rendszerre és adatkezelési tevékenységre, ahol a szervezetnek jogi vagy szerződéses követelményeknek kell megfelelnie;

2.1.3 valamennyi helyszínre és eszközre, amelyet üzleti információk kezelésére használnak, függetlenül attól, hogy irodai, távoli vagy felhőalapú környezetről van szó.

2.2 A szabályzat az alábbi területekre terjed ki:

2.2.1 adatvédelmi jogszabályok, például a GDPR;

2.2.2 kiberbiztonsági szabályozások, például a NIS2 irányelv;

2.2.3 ágazatspecifikus kötelezettségek, amennyiben alkalmazandók;

2.2.4 ügyfélszerződések, titoktartási megállapodások és auditálási záradékok;

2.2.5 önkéntes tanúsítások (pl. ISO 27001), valamint azok a belső szabályzatok, amelyeket a megfelelés érdekében be kell tartani.

3. Célkitűzések

3.1 Elszámoltathatóság biztosítása: egyértelmű felelősség kijelölése a jogi, szabályozási és szerződéses kötelezettségek nyomon követésére, aktualizálására és betartatására.

3.2 A vállalkozás védelme: a jogsértések, bírságok, adatvédelmi incidensek és reputációs károk kockázatának minimalizálása.

3.3 Auditra való felkészültség biztosítása: ellenőrizhető nyilvántartások fenntartása annak igazolására, hogy a szervezet miként teljesíti megfelelési kötelezettségeit.

3.4 A szabályzatok integrációjának támogatása: annak biztosítása, hogy a jogi és szabályozási kötelezettségek valamennyi szabályzatban és folyamatban következetesen érvényesüljenek.

3.5 A kivételek átlátható kezelése: annak biztosítása, hogy minden megfelelési kivétel dokumentált, indokolt és jóváhagyott legyen a felelősségi kockázatok csökkentése érdekében.

4. Szerepkörök és felelősségek

4.1 Ügyvezető

4.1.1 Átfogó felelősséggel tartozik a szervezet jogi és szabályozási megfeleléséért.

4.1.2 Vezeti a megfelelési nyilvántartást, és gondoskodik annak naprakészen tartásáról.

4.1.3 Felülvizsgálja az ügyfélszerződéseket, és biztosítja, hogy az egyedi kötelezettségek nyomon követése és teljesítése megtörténjen.

4.1.4 A megfelelési kötelezettségek alóli kivételeket kizárólag jogilag indokolható esetben és kompenzáló kontrollok mellett hagyhatja jóvá.

4.2 Külső tanácsadók (pl. jogi, informatikai vagy megfelelőségi tanácsadók)

4.2.1 Támogatják az ügyvezetőt az alkalmazandó jogszabályok, tanúsítások és kötelezettségek azonosításában (pl. GDPR, NIS2, ISO 27001).

4.2.2 Iránymutatást adnak az új szabályozások vagy a meglévő jogszabályok módosításainak értelmezéséhez.

4.2.3 Jogi kitettséggel járó esetekben közreműködhetnek a szabályzatok frissítésében, auditokban vagy adatvédelmi incidensek kezelésében.

[... 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 éves felülvizsgálat

9.1.1 Jelen szabályzatot az ügyvezetőnek 12 havonta felül kell vizsgálnia.

9.1.2 A felülvizsgálatnak meg kell erősítenie:

9.1.2.1 a szabályzat megfelelőségét az aktuális jogi és szerződéses környezethez;

9.1.2.2 az ügyfélszerződések és szolgáltatási kötelezettségek megfelelő megjelenítését;

9.1.2.3 az összhangot a megfelelési nyilvántartással és az egyéb szabályzatokkal.

9.2 Eseményvezérelt frissítések

9.2.1 Azonnali felülvizsgálat szükséges, ha:

9.2.1.1 új jogszabály vagy szabályozás válik alkalmazandóvá (pl. új adatvédelmi előírás);

9.2.1.2 egy ügyfél összetett megfelelési feltételeket épít be a szerződésébe;

9.2.1.3 szabálysértés vagy meg nem felelési incidens történik;

9.2.1.4 a vállalat szabályozott piacra vagy ágazatba lép.

9.3 Frissítések jóváhagyása és verziókezelés

9.3.1 Minden frissítést dokumentálni, verziózni és az ügyvezetővel jóváhagyatni kell.

9.3.2 A korábbi verziókat audit- és jogi célból meg kell őrizni.

9.4 A változások kommunikálása

9.4.1 A munkatársakat és a vállalkozókat a szabályzat módosításairól a jóváhagyást követő 5 munkanapon belül tájékoztatni kell.

9.4.2 Minden érintett beszállítónak is tudomásul kell vennie a módosított feltételeket a szolgáltatásnyújtás folytatása előtt.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat végrehajtását és alkalmazását az alábbi KKV-szabályzatok támogatják:

10.1.1 P3S – Elfogadható használati szabályzat: megelőzi azokat a magatartásokat, amelyek jogi vagy szerződéses feltételek megsértéséhez vezethetnek (pl. jogosulatlan fájlmegosztás).

10.1.2 P8S – Információbiztonsági tudatossági és képzési szabályzat: tájékoztatja a munkatársakat a megfelelési kötelezettségekről és a szabályszegések megelőzésének módjáról.

10.1.3 P14S – Adatmegőrzési és megsemmisítési szabályzat: biztosítja a jogszerű adatkezelési gyakorlatokat a teljes információ-életciklus során.

10.1.4 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: teljesíti a GDPR és az ügyféladat-kezelési követelményeket.

10.1.5 P30S – Incidenskezelési szabályzat: meghatározza az adatvédelmi incidensekre vagy megfelelőségi hibákra adandó reagálást, beleértve az incidensbejelentési határidőket is.

10.1.6 P36S – Közösségi média és külső kommunikációs szabályzat: biztosítja, hogy a nyilvános kommunikáció ne sértse a jogi vagy szabályozási kötelezettségeket.

10.2 Minden kapcsolódó szabályzat a jogi megfelelési keretrendszer egy részét érvényesíti, ezért azokat összehangoltan kell alkalmazni.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 6.1. pont – A kockázatok és lehetőségek kezelésére irányuló intézkedések: magában foglalja a megfelelési kockázatokat.

11.1.2 8.1. pont – Működéstervezés és -szabályozás: előírja olyan folyamatok végrehajtását, amelyek megfelelnek a jogi és szerződéses követelményeknek.

11.2 ISO/IEC 27002

11.2.1 5.36. kontroll – Iránymutatást ad a szervezet számára a kötelezettségek nyilvántartásának fenntartásához és a jogi, illetve szabályozási követelményekre adott megfelelő válaszok biztosításához.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Szabályzat és eljárások: előírja a formális megfelelési szabályzatok meglétét.

11.3.2 PM-1 – Információbiztonsági programterv: előírja a jogi megfelelés integrálását a biztonsági tervezésbe.

11.3.3 CA-1 – Értékelés, felhatalmazás és monitorozás.

11.3.4 AU-1 – Auditszabályzat: előírja a megfelelési bizonyítékok megőrzését.

11.4 GDPR

11.4.1 5. cikk – Az adatkezelés alapelvei, beleértve az elszámoltathatóságot.

11.4.2 6. cikk – Az adatkezelés jogalapja.

11.4.3 32. cikk – Az adatkezelés biztonsága.

11.4.4 33. cikk – Incidensbejelentés 72 órán belül.

11.5 NIS2 irányelv

11.5.1 21. cikk (2) bekezdés a) és f) pont – Belső szabályzatok a kockázatok és a szabályozási kontroll biztosítására.

11.5.2 23. cikk – Végrehajtás és szankciók megfelelőségi hibák esetén.

11.6 DORA rendelet

11.6.1 5. cikk (2) bekezdés – Az IKT-kockázatkezelés felügyelete.

11.6.2 9. cikk (1) bekezdés – A megfelelés belső irányítása.

11.6.3 17. cikk – Szerződéses megállapodások IKT-szolgáltatókkal.

11.7 COBIT 2019

11.7.1 APO12 – Kezelt kockázatok: biztosítja a megfelelési kockázatok nyomon követését és kezelését.

11.7.2 APO13 – Kezelt biztonság: lefedi a szabályozási és szerződéses megfelelés kockázatalapú érvényesítését.

11.7.3 DSS01 – Kezelt működés: előírja a jogi kötelezettségek teljesítéséhez szükséges működési felkészültséget.