					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P37S					Názov dokumentu: **Politika právneho a regulačného súladu**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Kontrola 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
Nariadenie EÚ GDPR	Články 5, 6, 32, 33	
Smernica EÚ NIS2	Články 21(2)(a), 21(2)(f), 23	
Nariadenie EÚ DORA	Články 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Účel

1.1 Táto politika vymedzuje prístup organizácie k identifikácii, plneniu a preukazovaniu súladu s právnymi, regulačnými a zmluvnými povinnosťami.

1.2 Stanovuje jasné zodpovednosti a praktické postupy, ktoré organizácii umožňujú plniť povinnosti v oblasti súladu vrátane požiadaviek právnych predpisov na ochranu údajov, rámcov kybernetickej bezpečnosti, zmlúv so zákazníkmi a certifikačných požiadaviek.

1.3 Zabezpečuje, že aj bez vyhradeného tímu pre compliance môže organizácia udržiavať právne vyhovujúcu prevádzku, primerane reagovať na incidenty a zachovať plnú pripravenosť na audit.

1.4 Táto politika je nevyhnutná na získanie certifikácie podľa ISO/IEC 27001:2022 a na splnenie externých očakávaní zákazníkov, regulátorov a partnerov.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetkých zamestnancov, zmluvných pracovníkov, freelancerov a dodávateľov tretích strán,

2.1.2 všetky služby, prevádzkové činnosti, systémy a činnosti spracúvania údajov, pri ktorých je organizácia povinná plniť právne alebo zmluvné požiadavky,

2.1.3 všetky lokality a zariadenia používané na spracúvanie informácií organizácie, či už v kancelárii, pri práci na diaľku alebo v cloudovom prostredí.

2.2 Politika pokrýva:

2.2.1 právne predpisy o ochrane údajov, ako je Nariadenie EÚ GDPR,

2.2.2 predpisy v oblasti kybernetickej bezpečnosti, ako je Smernica EÚ NIS2,

2.2.3 odvetvovo špecifické povinnosti, ak sa uplatňujú,

2.2.4 zmluvy so zákazníkmi, dohody o mlčanlivosti a auditné doložky,

2.2.5 dobrovoľné certifikácie (napr. ISO 27001) a interné politiky, ktoré sa musia uplatňovať na účely súladu.

3. Ciele

3.1 Zaviesť zodpovednosť: priradiť jasnú zodpovednosť za monitorovanie, aktualizáciu a uplatňovanie právnych, regulačných a zmluvných povinností.

3.2 Chrániť organizáciu: minimalizovať riziko porušenia právnych predpisov, sankcií, porušenia ochrany údajov a reputačnej ujmy.

3.3 Zabezpečiť pripravenosť na audit: viesť overiteľné záznamy preukazujúce, ako organizácia plní svoje povinnosti v oblasti súladu.

3.4 Podporiť integráciu politík: zabezpečiť, aby sa právne a regulačné povinnosti uplatňovali konzistentne vo všetkých politikách a procesoch.

3.5 Transparentne riadiť výnimky: zabezpečiť, aby všetky výnimky z požiadaviek súladu boli zdokumentované, odôvodnené a schválené s cieľom predísť zodpovednosti.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Nesie celkovú zodpovednosť za právny a regulačný súlad organizácie.

4.1.2 Vedie register súladu a zabezpečuje jeho aktuálnosť.

4.1.3 Preskúmava zmluvy so zákazníkmi a zabezpečuje sledovanie a plnenie konkrétnych povinností.

4.1.4 Schvaľuje výnimky z povinností súladu len v prípadoch, keď sú právne obhájiteľné a sú zavedené kompenzačné opatrenia.

4.2 Externí poradcovia (napr. právni, IT alebo compliance konzultanti)

4.2.1 Podporujú GM pri identifikácii uplatniteľných právnych predpisov, certifikácií a povinností (napr. GDPR, NIS2, ISO 27001).

4.2.2 Poskytujú usmernenia pri výklade nových predpisov alebo zmien existujúcich právnych predpisov.

4.2.3 Môžu pomáhať pri aktualizácii politík, auditoch alebo reakcii na porušenie ochrany údajov, ak existuje právna alebo regulačná expozícia.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Plánované ročné preskúmanie

9.1.1 Túto politiku musí každých 12 mesiacov preskúmať GM.

9.1.2 Preskúmanie musí potvrdiť:

9.1.2.1 relevantnosť vo vzťahu k aktuálnemu právnemu a zmluvnému kontextu,

9.1.2.2 správne zohľadnenie dohôd so zákazníkmi a servisných povinností,

9.1.2.3 súlad s registrom súladu a ostatnými politikami.

9.2 Aktualizácie na základe udalostí

9.2.1 Okamžité preskúmanie sa vyžaduje, ak:

9.2.1.1 sa začne uplatňovať nový právny predpis alebo regulácia (napr. nové pravidlo ochrany údajov),

9.2.1.2 zákazník doplní do zmluvy komplexné požiadavky na súlad,

9.2.1.3 dôjde k porušeniu alebo incidentu nesúladu,

9.2.1.4 organizácia vstúpi na regulovaný trh alebo do regulovaného odvetvia.

9.3 Schvaľovanie aktualizácií a riadenie verzií

9.3.1 Všetky aktualizácie musia byť zdokumentované, podliehať riadeniu verzií a byť schválené GM.

9.3.2 Historické verzie sa musia uchovávať na účely auditu a právnej obhájiteľnosti.

9.4 Oznámenie zmien

9.4.1 Zamestnanci a zmluvní pracovníci musia byť o zmenách politiky informovaní do 5 pracovných dní od schválenia.

9.4.2 Všetci dotknutí dodávatelia musia pred pokračovaním v poskytovaní služieb potvrdiť oboznámenie sa s aktualizovanými podmienkami.

10. Súvisiace politiky a väzby

10.1 Táto politika je podporovaná a uplatňovaná prostredníctvom týchto politík SME:

10.1.1 P3S – Politika prijateľného používania: predchádza správaniu, ktoré môže viesť k porušeniu právnych alebo zmluvných podmienok (napr. neoprávnenému zdieľaniu súborov),

10.1.2 P8S – Politika povedomia a školenia o informačnej bezpečnosti: vzdeláva zamestnancov o povinnostiach v oblasti súladu a o tom, ako predchádzať porušeniam,

10.1.3 P14S – Politika uchovávania a likvidácie údajov: zabezpečuje zákonné postupy pri zaobchádzaní s údajmi počas celého ich životného cyklu,

10.1.4 P17S – Politika ochrany údajov a súkromia: plní požiadavky GDPR a požiadavky zákazníkov na nakladanie s údajmi,

10.1.5 P30S – Politika reakcie na incidenty: stanovuje spôsob reakcie na porušenie ochrany údajov alebo zlyhania súladu vrátane notifikačných lehôt,

10.1.6 P36S – Politika sociálnych médií a externej komunikácie: zabezpečuje, aby verejná komunikácia neporušovala právne ani regulačné povinnosti.

10.2 Každá prepojená politika uplatňuje časť rámca právneho súladu a musí sa používať vo vzájomnej nadväznosti.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 6.1 – Opatrenia na riešenie rizík a príležitostí: zahŕňa riziká súladu.

11.1.2 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: vyžaduje vykonávanie procesov, ktoré spĺňajú právne a zmluvné požiadavky.

11.2 ISO/IEC 27002

11.2.1 Kontrola 5.36 – usmerňuje organizáciu pri vedení záznamov o povinnostiach a zabezpečovaní primeraných reakcií na právne a regulačné požiadavky.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika a postupy: vyžaduje formálne politiky súladu.

11.3.2 PM-1 – Plán programu informačnej bezpečnosti: vyžaduje integráciu právneho súladu do plánovania bezpečnosti.

11.3.3 CA-1 – Posudzovanie, autorizácia a monitorovanie.

11.3.4 AU-1 – Politika auditu: vyžaduje uchovávanie dôkazov o súlade.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 5 – zásady spracúvania údajov vrátane zodpovednosti.

11.4.2 Článok 6 – právny základ spracúvania.

11.4.3 Článok 32 – bezpečnosť spracúvania.

11.4.4 Článok 33 – oznámenie porušenia do 72 hodín.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21(2)(a) a (f) – interné politiky pre riadenie rizík a regulačnú kontrolu.

11.5.2 Článok 23 – presadzovanie a sankcie pri zlyhaniach súladu.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 5(2) – dohľad nad riadením rizík IKT.

11.6.2 Článok 9(1) – interná správa a riadenie súladu.

11.6.3 Článok 17 – zmluvné vzťahy s poskytovateľmi služieb IKT.

11.7 COBIT 2019

11.7.1 APO12 – Riadené riziko: zabezpečuje sledovanie a riešenie rizík súladu.

11.7.2 APO13 – Riadená bezpečnosť: pokrýva uplatňovanie regulačného a zmluvného súladu na základe rizík.

11.7.3 DSS01 – Riadené prevádzkové činnosti: vyžaduje prevádzkovú pripravenosť na plnenie právnych povinností.