					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P17S					Názov dokumentu: **Politika ochrany údajov a súkromia**							
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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitoly 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Kontroly 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
Nariadenie EÚ GDPR	Články 5, 6, 12–23, 30, 32–34	
Smernica EÚ NIS2	Článok 21(2)(e), 21(2)(f)	
Nariadenie EÚ DORA	Články 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Účel

1.1. Táto politika stanovuje, ako organizácia chráni osobné údaje v súlade s právnymi povinnosťami, regulačnými rámcami a medzinárodnými bezpečnostnými normami.

1.2. Zabezpečuje, aby sa osobné údaje zákazníkov, zamestnancov a partnerov získavali, používali, uchovávali a vymazávali zákonným, spravodlivým a bezpečným spôsobom.

1.3. Táto politika zároveň podporuje súlad s normou ISO/IEC 27001:2022 a pripravenosť na audit uplatňovaním konzistentného prístupu k ochrane súkromia založeného na riziku.

1.4. Prostredníctvom tejto politiky organizácia preukazuje zodpovedný prístup a posilňuje dôveru zákazníkov tým, že uprednostňuje transparentnosť, minimalizáciu údajov a účinné riadenie ochrany súkromia.

2. Rozsah

2.1. Táto politika sa vzťahuje na:

2.1.1. všetkých zamestnancov, zmluvných pracovníkov a poskytovateľov služieb, ktorí pristupujú k osobným údajom, spracúvajú ich alebo ich spravujú,

2.1.2. akýkoľvek systém, aplikáciu alebo umiestnenie, v ktorom sú osobné údaje uložené alebo prenášané,

2.1.3. všetky osobné údaje bez ohľadu na to, či sú uložené elektronicky, v listinnej podobe, v cloudových systémoch alebo na mobilných zariadeniach.

2.2. Táto politika sa vzťahuje na údaje týkajúce sa zákazníkov, zamestnancov, dodávateľov a akýchkoľvek iných identifikovateľných osôb.

2.3. Táto politika sa uplatňuje bez ohľadu na to, či sú údaje spracúvané interne alebo poskytovateľmi služieb tretích strán.

3. Ciele

3.1. Zabezpečiť, aby sa s osobnými údajmi nakladalo v súlade s právnymi predpismi na ochranu súkromia a bezpečnostnými normami vrátane GDPR, NIS2 a ISO 27001.

3.2. Chrániť osobné údaje pred neoprávneným prístupom, zneužitím, zmenou alebo stratou prostredníctvom jasne definovaných technických a organizačných opatrení.

3.3. Rešpektovať práva dotknutých osôb vrátane práva na prístup k údajom, ich opravu a vymazanie.

3.4. Zaviesť v organizácii jasne vymedzené roly a zodpovednosti v oblasti ochrany údajov.

3.5. Uplatňovať minimalizáciu údajov, bezpečné uchovávanie a včasné vymazanie vo všetkých systémoch a procesoch.

3.6. Znižovať riziko nesúladu, právnych sankcií, reputačnej ujmy alebo straty dôvery zákazníkov.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. schvaľuje túto politiku a zabezpečuje jej uplatňovanie,

4.1.2. poskytuje potrebné zdroje na riadenie rizík ochrany súkromia a reakciu na incidenty,

4.1.3. nesie celkovú zodpovednosť za súlad s právnymi predpismi a normami v oblasti ochrany súkromia.

4.2. Koordinátor ochrany súkromia (interný alebo externý)

4.2.1. vedie záznamy o spracovateľských činnostiach,

4.2.2. vybavuje žiadosti dotknutých osôb týkajúce sa ochrany súkromia a otázky regulačných orgánov,

4.2.3. podporuje posudzovanie rizík, školenia a implementáciu politiky,

4.2.4. dokumentuje porušenia ochrany údajov a podľa potreby oznamuje udalosti príslušným orgánom.

[... 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 preskúmania

9.1.1. táto politika musí byť preskúmaná najmenej raz za 12 mesiacov Koordinátorom ochrany súkromia a schválená Generálnym manažérom,

9.1.2. preskúmanie musí posúdiť relevantnosť politiky, súlad s predpismi a prevádzkovú účinnosť.

9.2. Spúšťače priebežného preskúmania

9.2.1. aktualizácie politiky sa musia iniciovať aj v reakcii na:

9.2.1.1. nové alebo revidované právne predpisy o ochrane údajov (napr. GDPR, DORA),

9.2.1.2. bezpečnostné incidenty alebo porušenia ochrany súkromia týkajúce sa osobných údajov,

9.2.1.3. zavedenie nových systémov, nástrojov alebo služieb spracúvajúcich osobné údaje,

9.2.1.4. významné auditné zistenia alebo odporúčania regulačných orgánov.

9.3. Riadenie zmien a komunikácia

9.3.1. všetky zmeny tejto politiky musia byť formálne zdokumentované v zozname zmien,

9.3.2. revidované verzie musia byť distribuované všetkým zamestnancom a príslušným zmluvným pracovníkom,

9.3.3. archivované verzie musia byť uchovávané na účely auditnej stopy súladu.

10. Súvisiace politiky a väzby

10.1. Táto politika sa uplatňuje spolu s ďalšími politikami SME s cieľom vytvoriť úplný a vykonateľný rámec ochrany súkromia:

10.1.1. P13S – Politika klasifikácie a označovania údajov: zabezpečuje, aby boli osobné údaje primerane klasifikované a aby bolo možné uplatniť ochranu súkromia podľa rizika.

10.1.2. P14S – Politika uchovávania a likvidácie údajov: stanovuje jasné pravidlá pre lehoty uchovávania osobných údajov a bezpečné metódy ich likvidácie po uplynutí týchto lehôt.

10.1.3. P16S – Politika maskovania údajov a pseudonymizácie: stanovuje, ako sa musia transformovať osobné identifikátory pred použitím údajov v neprodukčnom prostredí alebo pred ich externým zdieľaním.

10.1.4. P30S – Politika reakcie na incidenty: upravuje kroky potrebné pri reakcii na porušenie ochrany údajov vrátane oznámenia regulačným orgánom a dotknutým osobám v požadovaných lehotách.

10.1.5. P2S – Politika rolí a zodpovedností v oblasti správy a riadenia: objasňuje štruktúru zodpovedností a rozhodovacie roly, ktoré sa uplatňujú pri presadzovaní a dohľade nad ochranou súkromia.

10.2. Tieto súvisiace politiky sa musia preskúmavať a uplatňovať spoločne, aby sa zabezpečilo komplexné pokrytie ochrany súkromia v systémoch, medzi zamestnancami a u dodávateľov.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 5.1 – Vyžaduje, aby vrcholové vedenie preukázalo líderstvo a záväzok pri ochrane osobných údajov.

11.1.2. Kapitola 6.1.3 – Vyžaduje ošetrenie rizík súvisiacich so spracúvaním osobných údajov.

11.1.3. Kapitola 8.1 – Vyžaduje zavedenie prevádzkových opatrení na ochranu údajov počas celého ich životného cyklu.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.34 – Poskytuje implementačné usmernenia na ochranu súkromia a bezpečné nakladanie s PII.

11.2.2. Kontrola 8.10 – Rieši bezpečnú likvidáciu osobných údajov s cieľom zabrániť reziduálnemu sprístupneniu.

11.2.3. Kontrola 8.11 – Podporuje používanie maskovania a pseudonymizácie na účely minimalizácie údajov.

11.2.4. Kontrola 8.12 – Zabraňuje neoprávneným únikom údajov prostredníctvom kontrol prístupu k údajom a ich používania.

11.3. NIST SP 800-53 Rev.

11.3.1. AR-2 – Prideľuje roly a zodpovednosti za riadenie rizík ochrany súkromia.

11.3.2. PL-5 – Vyžaduje dokumentáciu plánu ochrany súkromia pokrývajúceho používanie a ochranu údajov.

11.3.3. AC-6 – Vyžaduje zásadu minimálnych oprávnení a riadenie prístupu k osobným údajom.

11.3.4. IR-4 – Vyžaduje procesy riešenia incidentov pri porušeniach týkajúcich sa osobných údajov.

11.4. Nariadenie EÚ GDPR

11.4.1. Článok 5 – Definuje základné zásady zákonného, spravodlivého a transparentného spracúvania údajov.

11.4.2. Článok 6 – Vyžaduje platný právny základ pre každú činnosť spracúvania osobných údajov.

11.4.3. Články 12–23 – Vymedzujú práva dotknutých osôb vrátane prístupu, opravy, vymazania a námietky.

11.4.4. Článok 30 – Vyžaduje záznamy o spracovateľských činnostiach.

11.4.5. Článok 32 – Vyžaduje primerané technické a organizačné bezpečnostné opatrenia.

11.4.6. Články 33–34 – Stanovujú oznamovacie povinnosti pri porušení ochrany údajov voči orgánom a dotknutým osobám.

11.5. Smernica EÚ NIS2

11.5.1. Článok 21(2)(e) – Vyžaduje opatrenia na zabezpečenie ochrany údajov v súlade s politikami kybernetickej bezpečnosti.

11.5.2. Článok 21(2)(f) – Vyžaduje mechanizmy na riadenie bezpečnosti osobných a dôverných údajov v systémoch IKT.

11.6. Nariadenie EÚ DORA

11.6.1. Článok 6 – Vyžaduje interné rámce správy a riadenia na riadenie rizík údajov a ich ochrany.

11.6.2. Článok 15 – Ukladá finančným subjektom povinnosť zabezpečiť, aby poskytovatelia tretích strán chránili osobné údaje a podporovali dodržiavanie regulačných požiadaviek.

11.6.3. Článok 17 – Vyžaduje, aby organizácie zabezpečili, že systémy IKT spracúvajúce osobné údaje sú bezpečné, odolné a monitorované.

11.7. COBIT 2019

11.7.1. APO12 – Riadenie rizík: vyžaduje identifikáciu a ošetrenie rizík ochrany súkromia a ochrany údajov.

11.7.2. DSS05 – Riadenie bezpečnostných služieb: vyžaduje ochranné opatrenia na zabránenie neoprávnenému prístupu k osobným údajom.

11.7.3. MEA03 – Monitorovanie súladu: vyžaduje, aby organizácie zabezpečovali priebežný súlad s právnymi predpismi v oblasti ochrany súkromia a ochrany údajov.