					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P17					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, 8.1, 10	Relevantné všeobecné, technické a kontrolné opatrenia v oblasti neustáleho zlepšovania a ochrany údajov
ISO/IEC 27002:2022	Kontroly 5.34, 8.10, 8.11, 8.12	Kontroly pre nakladanie s PII, uchovávanie, vymazanie, anonymizáciu a práva dotknutých osôb
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Požiadavky na správu a riadenie, riziká, riadenie prístupu, logovanie, reakciu na porušenie ochrany údajov a program ochrany súkromia
GDPR EÚ	Články 5, 6, 12–23, 25, 28, 30, 32–34; odôvodnenie 78	Všetky kľúčové požiadavky na ochranu súkromia, zodpovednosť, práva dotknutých osôb, žiadosti dotknutých osôb, porušenia ochrany údajov a zásady ochrany údajov už pri návrhu a štandardne
Smernica EÚ NIS2	Článok 21 ods. 2 písm. e), f)	Bezpečnostné kontroly založené na riziku pre základné a dôležité subjekty
Nariadenie EÚ DORA	Články 6 ods. 2 písm. d), 11 ods. 1 písm. c), 15 ods. 1, 17	Správa a riadenie, riziká tretích strán a lehoty bezpečného spracúvania
COBIT 2019	APO12, DSS01, DSS05, MEA	Riadenie rizík, bezpečná prevádzka, dohľad nad súladom

1. Účel

1.1 Táto politika ustanovuje záväzné organizačné princípy a technické požiadavky na ochranu osobných údajov a uplatňovanie zásad ochrany súkromia už pri návrhu vo všetkých prostrediach.

1.2 Formalizuje zodpovednosti organizácie podľa medzinárodných noriem a regulačných rámcov a zabezpečuje, aby sa osobné údaje získavali, spracúvali, uchovávali, zdieľali a likvidovali zákonným, bezpečným a transparentným spôsobom.

1.3 Táto politika zároveň posilňuje súlad s uplatniteľnými právnymi predpismi a rámcami ochrany súkromia vrátane nariadenia GDPR, smernice NIS2, nariadenia DORA, ISO/IEC 27001:2022 a COBIT 2019.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky organizačné jednotky, pracovníkov a systémy zapojené do spracúvania osobných údajov vrátane:

2.1.1 zamestnancov, zmluvných pracovníkov, konzultantov a poskytovateľov služieb tretích strán.

2.1.2 údajov získavaných z interných a externých zdrojov vo všetkých podnikových funkciách.

2.1.3 fyzických a digitálnych médií vrátane cloudových služieb, platforiem SaaS, mobilných zariadení a papierových záznamov.

2.1.4 všetkých prostredí vrátane produkčných, vývojových, testovacích a záložných systémov, v ktorých sa môžu nachádzať osobné údaje.

2.2 Zahŕňa všetky činnosti spracúvania regulované uplatniteľnými právnymi predpismi a normami ochrany súkromia vrátane, ale nie výlučne:

2.2.1 získavania, uchovávania, používania, prenosu a likvidácie osobných údajov.

2.2.2 uplatňovania práv dotknutých osôb, dokumentovania právneho základu a riadenia súhlasu.

2.2.3 cezhraničných prenosov, oznamovania porušenia ochrany údajov a zdieľania údajov s tretími stranami.

2.2.4 bezpečného návrhu a uplatňovania ochrany súkromia v predvolenom nastavení v systémoch a procesoch.

3. Ciele

3.1 Zabezpečiť zákonné, transparentné a preukázateľne zodpovedné spracúvanie osobných údajov v súlade s ISO/IEC 27001:2022 a súvisiacimi právnymi požiadavkami.

3.2 Zaviesť zásady ochrany súkromia už pri návrhu a ochrany súkromia v predvolenom nastavení do všetkých informačných systémov, služieb a podnikových procesov.

3.3 Uplatňovať technické a organizačné opatrenia (TOM), ktoré chránia dôvernosť, integritu a dostupnosť osobných údajov počas celého ich životného cyklu.

3.4 Vymedziť riadiace roly a štruktúry zodpovednosti za ochranu údajov vrátane povinností zodpovednej osoby pre ochranu osobných údajov (DPO), funkcie informačnej bezpečnosti, právneho oddelenia a compliance a vlastníkov údajov.

3.5 Umožniť plný súlad s článkami 5, 6, 25, 30 a 32 GDPR, ako aj s požiadavkami na znižovanie rizika a odolnosť podľa NIS2 a DORA.

3.6 Zabezpečiť práva dotknutých osôb vrátane prístupu, opravy, výmazu, obmedzenia spracúvania, prenosnosti, námietky a ochrany pred automatizovaným rozhodovaním.

3.7 Zmierňovať regulačné, reputačné, právne a prevádzkové riziká vyplývajúce z neoprávneného prístupu k osobným údajom, ich zneužitia alebo straty.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Zabezpečuje strategický dohľad a prideľuje dostatočné zdroje na podporu programu ochrany súkromia.

4.1.2 Schvaľuje túto politiku a zabezpečuje jej uplatňovanie v celej organizácii.

4.2 Zodpovedná osoba pre ochranu osobných údajov (DPO)

4.2.1 Koná nezávisle pri dohľade nad súladom s predpismi o ochrane údajov.

4.2.2 Vedie záznamy o spracovateľských činnostiach (RoPA) podľa článku 30 GDPR.

4.2.3 Riadi komunikáciu s regulačnými orgánmi, vykonáva posúdenia vplyvu na ochranu údajov (DPIA) a riadi procesy oznamovania porušenia ochrany údajov.

4.2.4 Preskúmava výnimky v oblasti ochrany súkromia a vedie register výnimiek ochrany súkromia.

[... 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 Táto politika sa musí preskúmať najmenej raz ročne alebo skôr za nasledujúcich podmienok:

9.1.1 významné právne alebo regulačné zmeny (napr. zmeny GDPR, lehoty podľa DORA)

9.1.2 nové systémy alebo činnosti spracúvania zahŕňajúce osobné údaje

9.1.3 auditné zistenia vnútorného auditu poukazujúce na nedostatky v politike

9.1.4 závažné incidenty porušenia ochrany údajov alebo spätná väzba od dozorného orgánu

9.2 Zodpovednosti za preskúmanie

9.2.1 DPO iniciuje preskúmanie politiky v koordinácii s právnym oddelením, riadením rizík, informačnou bezpečnosťou a vrcholovým manažmentom.

9.2.2 Všetky aktualizácie musia byť zaznamenané v registri riadenia dokumentácie ISMS a distribuované dotknutým zainteresovaným stranám.

9.3 Riadenie zmien

9.3.1 Každá revízia tejto politiky musí byť formálne schválená vrcholovým manažmentom.

9.3.2 Neplatné verzie sa musia bezpečne archivovať a aktualizovaná verzia musí obsahovať zdokumentovanú históriu zmien.

10. Súvisiace politiky a väzby

10.1 P1 – Politika informačnej bezpečnosti. Ustanovuje nadradené princípy správy a riadenia bezpečnosti, ktoré tvoria základ tejto politiky ochrany súkromia. P1 podporuje dôvernosť, integritu a dostupnosť osobných údajov vo všetkých systémoch a službách.

10.2 P6 – Politika riadenia rizík. Definuje metodiku ošetrenia rizík organizácie, ktorá je nevyhnutná na posudzovanie rizík ochrany súkromia, procesy DPIA a hodnotenie reziduálneho rizika vyžadované podľa GDPR a kapitoly 6.1.3 ISO/IEC 27001.

10.3 P13 – Politika klasifikácie a označovania údajov. Usmerňuje kategorizáciu osobných a citlivých údajov a vytvára základ na uplatňovanie primeraných kontrol ochrany súkromia vrátane uplatňovania lehôt uchovávania, obmedzenia prístupu a bezpečnej likvidácie.

10.4 P14 – Politika uchovávania a likvidácie údajov. Priamo podporuje požiadavky ochrany súkromia podľa článkov 5 ods. 1 písm. e) a 17 GDPR a zabezpečuje, aby sa osobné údaje uchovávali len nevyhnutne dlhý čas a likvidovali bezpečne v súlade so zákonnými povinnosťami.

10.5 P16 – Politika maskovania údajov a pseudonymizácie. Ustanovuje kontroly na znižovanie identifikovateľnosti osobných údajov prostredníctvom technických opatrení, ako sú tokenizácia, dynamické maskovanie a pseudonymizácia, čím podporuje uplatňovanie článku 32 GDPR a kontroly 5.34 ISO/IEC 27002.

10.6 P30 – Politika reakcie na incidenty. Vymedzuje záväzné protokoly reakcie na porušenie ochrany údajov, ktoré sa integrujú s postupmi riešenia porušení ochrany súkromia a oznamovacími lehotami podľa článkov 33 a 34 GDPR.

10.7 P33 – Politika monitorovania auditu a súladu. Uplatňuje plánované posúdenia účinnosti programu ochrany súkromia, dodržiavania politiky a sledovania nápravných opatrení naprieč organizačnými jednotkami a sprostredkovateľmi tretích strán.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 5.1 – Vedenie a záväzok: Ustanovuje zodpovednosť vrcholového vedenia za ochranu osobných údajov a uplatňovanie zásad ochrany súkromia.

11.1.2 Kapitola 6.1.3 – Ošetrenie rizík informačnej bezpečnosti: Podporuje identifikáciu, posúdenie a ošetrenie rizík ochrany súkromia prostredníctvom DPIA a výnimiek.

11.1.3 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: Vyžaduje technické a procesné ochranné opatrenia na bezpečné spracúvanie osobných údajov.

11.1.4 Kapitola 10.1 – Neustále zlepšovanie: Ukladá povinnosť pravidelného hodnotenia a prispôsobovania programu ochrany súkromia.

11.2 ISO/IEC 27002:2022 kontroly 5.34, 8.10, 8.11, 8.12: Poskytujú usmernenie pre nakladanie s PII, uplatňovanie uchovávania, vymazania, anonymizácie a transparentnosti pri právach dotknutých osôb.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Vymedzujú správu a riadenie, roly, zodpovednosť a povinnosti v oblasti školení ochrany súkromia.

11.3.2 PL-2, PL-8: Vyžadujú integráciu kontrol ochrany súkromia do životného cyklu systémov a podnikovej architektúry.

11.3.3 AC-2, AC-6: Uplatňujú zásadu minimálnych oprávnení a správu účtov na ochranu osobných údajov.

11.3.4 AU-2, AU-6, AU-9: Ukladajú povinnosť logovania, sledovateľnosti a integrity auditu pri prístupe k osobným údajom.

11.3.5 IR-4, IR-5, IR-6: Vymedzujú štruktúrované procesy detekcie, analýzy a hlásenia porušení ochrany súkromia.

11.3.6 PM-1, PM-21, PM-23: Zavádzajú komplexný program ochrany súkromia zosúladený so strategickými cieľmi riadenia rizík a správy údajov.

11.4 GDPR EÚ (2016/679)

11.4.1 Články 5, 6, 12–23, 25, 28, 30, 32–34: Upravujú zákonné spracúvanie, obmedzenie účelu, práva dotknutých osôb, zodpovednosť, ochranu údajov už pri návrhu a v predvolenom nastavení, povinnosti tretích strán a riadenie porušenia ochrany údajov.

11.4.2 Odôvodnenie 78: Posilňuje zásady ochrany súkromia už pri návrhu.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21 ods. 2 písm. e) a f): Vyžaduje implementáciu bezpečnostných kontrol založených na riziku a ochranu osobných údajov v rozsahu pôsobnosti základných a dôležitých subjektov.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 6 ods. 2 písm. d): Uplatňuje internú správu a riadenie rizík IKT súvisiacich s nakladaním s údajmi.

11.6.2 Článok 11 ods. 1 písm. c): Ukladá dohľad nad rizikami tretích strán pri službách súvisiacich s údajmi.

11.6.3 Články 15 ods. 1 a 17: Vyžadujú bezpečné spracúvanie údajov poskytovateľmi služieb a včasné oznámenia orgánom dohľadu po incidentoch súvisiacich s IKT.

11.7 COBIT 2019

11.7.1 APO12 – Riadenie rizík: Začleňuje riziká ochrany súkromia do širšieho dohľadu nad podnikovými rizikami.

11.7.2 DSS01 – Riadené operácie a DSS05 – Bezpečnostné služby: Zabezpečujú bezpečnú prevádzku vrátane riadenia prístupu, uchovávania a integrity systémov.

11.7.3 MEA03 – Monitorovanie súladu: Vyžaduje priebežné preskúmanie stavu súladu voči regulačným požiadavkám a povinnostiam ochrany súkromia vyplývajúcim z politík.