					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P17					Název dokumentu: **Politika ochrany dat a soukromí**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma/právní předpis	Článek/ustanovení	Komentář
ISO/IEC 27001:2022	Články 5.1, 6.1.3, 8.1, 10	Relevantní obecná, technická a průběžně zlepšovaná opatření na ochranu dat
ISO/IEC 27002:2022	Opatření 5.34, 8.10, 8.11, 8.12	Opatření pro nakládání s osobními údaji, uchovávání, mazání, anonymizaci a práva subjektů údajů
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	Požadavky na správu a řízení, rizika, řízení přístupu, protokolování, reakci na porušení zabezpečení a program ochrany soukromí
GDPR	Články 5, 6, 12–23, 25, 28, 30, 32–34; bod odůvodnění 78	Všechny klíčové požadavky na ochranu soukromí, odpovědnost, práva subjektů údajů, žádosti subjektů údajů, porušení zabezpečení a zásady ochrany osobních údajů již od návrhu a ve výchozím nastavení
směrnice NIS2	Článek 21 odst. 2 písm. e), f)	Bezpečnostní opatření založená na rizicích pro základní a důležité subjekty
nařízení DORA	Články 6 odst. 2 písm. d), 11 odst. 1 písm. c), 15 odst. 1, 17	Správa a řízení, rizika třetích stran a požadavky na bezpečné zpracování
COBIT 2019	APO12, DSS01, DSS05, MEA	Řízení rizik, bezpečný provoz, dohled nad souladem

1. Účel

1.1 Tato politika stanoví závazné organizační zásady a technické požadavky na ochranu osobních údajů a uplatňování zásad ochrany osobních údajů již od návrhu ve všech prostředích.

1.2 Formalizuje odpovědnosti organizace podle mezinárodních norem a regulačních rámců a zajišťuje, aby osobní údaje byly shromažďovány, zpracovávány, uchovávány, sdíleny a likvidovány zákonným, bezpečným a transparentním způsobem.

1.3 Tato politika dále posiluje soulad s příslušnými právními předpisy a rámci v oblasti ochrany soukromí, včetně GDPR, směrnice NIS2, nařízení DORA, ISO/IEC 27001:2022 a COBIT 2019.

2. Rozsah

2.1 Tato politika se vztahuje na všechny organizační útvary, veškerý personál a systémy zapojené do zpracování osobních údajů, včetně:

2.1.1 zaměstnanců, dodavatelů, konzultantů a poskytovatelů služeb třetích stran.

2.1.2 údajů shromažďovaných z interních i externích zdrojů napříč všemi podnikovými funkcemi.

2.1.3 fyzických i digitálních médií, včetně cloudových služeb, SaaS platforem, mobilních zařízení a listinných záznamů.

2.1.4 všech prostředí, včetně produkčního prostředí, vývojových, testovacích a záložních systémů, ve kterých se mohou nacházet osobní údaje.

2.2 Zahrnuje všechny činnosti zpracování regulované příslušnými právními předpisy a normami v oblasti ochrany soukromí, mimo jiné:

2.2.1 shromažďování, ukládání, používání, přenos a likvidaci osobních údajů.

2.2.2 uplatňování práv subjektů údajů, dokumentaci právního základu a správu souhlasu.

2.2.3 přeshraniční přenosy dat, oznamování porušení zabezpečení a sdílení údajů s třetími stranami.

2.2.4 bezpečný návrh a uplatňování ochrany soukromí ve výchozím nastavení v systémech a procesech.

3. Cíle

3.1 Zajistit zákonné, transparentní a odpovědné zpracování osobních údajů v souladu s ISO/IEC 27001:2022 a souvisejícími právními požadavky.

3.2 Začlenit zásady ochrany soukromí již od návrhu a ochranu soukromí ve výchozím nastavení do všech informačních systémů, služeb a podnikových procesů.

3.3 Uplatňovat technická a organizační opatření (TOM), která chrání důvěrnost, integritu a dostupnost osobních údajů v celém jejich životním cyklu.

3.4 Vymezit role správy a řízení a struktury odpovědnosti za ochranu dat, včetně odpovědností pověřence pro ochranu osobních údajů (DPO), útvaru informační bezpečnosti, právního oddělení a vlastníků dat.

3.5 Umožnit plný soulad s články 5, 6, 25, 30 a 32 GDPR, jakož i s požadavky na snižování rizik a odolnost podle směrnice NIS2 a nařízení DORA.

3.6 Zajistit práva subjektů údajů, včetně přístupu, opravy, výmazu, omezení zpracování, přenositelnosti, námitky a ochrany před automatizovaným rozhodováním.

3.7 Snižovat regulační, reputační, právní a provozní rizika vyplývající z neoprávněného přístupu k osobním údajům, jejich zneužití nebo ztráty.

4. Role a odpovědnosti

4.1 Vrcholové vedení

4.1.1 Zajišťuje strategický dohled a přiděluje dostatečné zdroje na podporu programu ochrany soukromí.

4.1.2 Schvaluje tuto politiku a zajišťuje její uplatňování v celé organizaci.

4.2 Pověřenec pro ochranu osobních údajů (DPO)

4.2.1 Vykonává svou působnost nezávisle při zajišťování souladu s předpisy o ochraně osobních údajů.

4.2.2 Vede záznamy o činnostech zpracování (RoPA) podle článku 30 GDPR.

4.2.3 Řídí komunikaci s regulačními orgány, provádění posouzení vlivu na ochranu osobních údajů (DPIA) a procesy oznamování porušení zabezpečení.

4.2.4 Přezkoumává výjimky v oblasti ochrany soukromí a vede Registr výjimek ochrany soukromí.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumána nejméně jednou ročně nebo dříve za následujících podmínek:

9.1.1 významné právní nebo regulatorní změny (např. změny GDPR, termíny podle nařízení DORA)

9.1.2 nové systémy nebo činnosti zpracování zahrnující osobní údaje

9.1.3 zjištění interního auditu indikující nedostatky v politice

9.1.4 závažné incidenty porušení zabezpečení nebo zpětná vazba dozorového úřadu

9.2 Odpovědnosti za přezkum

9.2.1 DPO zahajuje přezkum politiky a koordinuje jej s právním oddělením, řízením rizik, útvarem informační bezpečnosti a vrcholovým vedením.

9.2.2 Všechny aktualizace musí být zaznamenány v registru řízení dokumentace ISMS a distribuovány dotčeným zainteresovaným stranám.

9.3 Řízení změn

9.3.1 Jakákoli revize této politiky musí být formálně schválena vrcholovým vedením.

9.3.2 Neplatné verze musí být bezpečně archivovány a aktualizovaná verze musí obsahovat zdokumentovanou historii změn.

10. Související politiky a vazby

10.1 P1 – Politika informační bezpečnosti. Stanoví zastřešující zásady správy a řízení bezpečnosti, na nichž je tato politika ochrany soukromí založena. P1 podporuje důvěrnost, integritu a dostupnost osobních údajů napříč všemi systémy a službami.

10.2 P6 – Politika řízení rizik. Definuje metodiku ošetření rizik organizace, která je nezbytná pro posuzování rizik ochrany soukromí, procesy DPIA a vyhodnocení zbytkového rizika vyžadované podle GDPR a článku 6.1.3 normy ISO/IEC 27001.

10.3 P13 – Politika klasifikace a označování dat. Poskytuje pravidla pro kategorizaci osobních a citlivých údajů a tvoří základ pro uplatnění odpovídajících kontrol ochrany soukromí, včetně vynucování uchovávání, omezení přístupu a bezpečné likvidace.

10.4 P14 – Politika uchovávání údajů a likvidace. Přímo podporuje požadavky na ochranu soukromí podle článku 5 odst. 1 písm. e) a článku 17 GDPR a zajišťuje, že osobní údaje jsou uchovávány pouze po nezbytně nutnou dobu a bezpečně likvidovány v souladu s právními povinnostmi.

10.5 P16 – Politika maskování dat a pseudonymizace. Stanoví opatření ke snížení identifikovatelnosti osobních údajů prostřednictvím technických mechanismů, jako jsou tokenizace, dynamické maskování a pseudonymizace, a tím zajišťuje plnění článku 32 GDPR a opatření 5.34 normy ISO/IEC 27002.

10.6 P30 – Politika reakce na incidenty (P30). Popisuje závazné protokoly reakce na porušení zabezpečení, které jsou provázány s postupy zvládání porušení ochrany soukromí a oznamovacími lhůtami vyžadovanými podle článků 33 a 34 GDPR.

10.7 P33 – Politika monitorování auditu a souladu. Zavádí plánovaná posouzení účinnosti programu ochrany soukromí, uplatňování politiky a sledování nápravných opatření napříč organizačními útvary a zpracovateli třetích stran.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Článek 5.1 – Vedení a závazek: stanoví odpovědnost vrcholového vedení za ochranu osobních údajů a uplatňování zásad ochrany soukromí.

11.1.2 Článek 6.1.3 – Ošetření rizik bezpečnosti informací: podporuje identifikaci, hodnocení a ošetření rizik ochrany soukromí prostřednictvím DPIA a výjimek.

11.1.3 Článek 8.1 – Provozní plánování a řízení: vyžaduje technická a procesní ochranná opatření k zajištění bezpečného zpracování osobních údajů.

11.1.4 Článek 10.1 – Průběžné zlepšování: vyžaduje pravidelné vyhodnocování a přizpůsobování programu ochrany soukromí.

11.2 ISO/IEC 27002:2022 Opatření 5.34, 8.10, 8.11, 8.12: poskytují pokyny pro nakládání s PII, uplatňování uchovávání, mazání, anonymizace a transparentnosti vůči právům subjektů údajů.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: definují správu a řízení, role, odpovědnost a povinnosti v oblasti školení ochrany soukromí.

11.3.2 PL-2, PL-8: vyžadují integraci kontrol ochrany soukromí do životního cyklu systému a podnikové architektury.

11.3.3 AC-2, AC-6: uplatňují zásadu minimálních oprávnění a správu účtů pro ochranu osobních údajů.

11.3.4 AU-2, AU-6, AU-9: vyžadují protokolování, dohledatelnost a integritu auditu pro přístup k osobním údajům.

11.3.5 IR-4, IR-5, IR-6: definují strukturované procesy detekce, analýzy a hlášení porušení ochrany soukromí.

11.3.6 PM-1, PM-21, PM-23: stanoví komplexní program ochrany soukromí sladěný se strategickými cíli v oblasti rizik a správy dat.

11.4 GDPR (2016/679)

11.4.1 Články 5, 6, 12–23, 25, 28, 30, 32–34: upravují zákonné zpracování, omezení účelu, práva subjektů údajů, odpovědnost, ochranu osobních údajů již od návrhu a ve výchozím nastavení, povinnosti třetích stran a řízení porušení zabezpečení.

11.4.2 Bod odůvodnění 78: posiluje zásady ochrany soukromí již od návrhu.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21 odst. 2 písm. e) a f): vyžaduje zavedení bezpečnostních opatření založených na rizicích a ochranu osobních údajů u základních a důležitých subjektů.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 6 odst. 2 písm. d): vyžaduje interní správu a řízení rizik v oblasti ICT souvisejících s nakládáním s daty.

11.6.2 Článek 11 odst. 1 písm. c): vyžaduje dohled nad riziky třetích stran u služeb souvisejících s daty.

11.6.3 Články 15 odst. 1 a 17: vyžadují bezpečné zpracování dat poskytovateli služeb a včasná oznámení dozorovým orgánům po incidentech souvisejících s ICT.

11.7 COBIT 2019

11.7.1 APO12 – Řízení rizik: začleňuje rizika ochrany soukromí do širšího podnikového dohledu nad riziky.

11.7.2 DSS01 – Řízený provoz a DSS05 – Bezpečnostní služby: zajišťují bezpečný provoz včetně řízení přístupu, uchovávání a integrity systémů.

11.7.3 MEA03 – Monitorování souladu: vyžaduje průběžný přezkum stavu souladu vůči regulatorním požadavkům a povinnostem ochrany soukromí vyplývajícím z politik.