					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P17S					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	Kapitoly 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Opatření 5.34, 8.10–8.12	
NIST SP 800-53 Rev. 5	AR-2, PL-5, AC-6, IR-4	
GDPR	Články 5, 6, 12–23, 30, 32–34	
směrnice NIS2	Článek 21(2)(e), 21(2)(f)	
nařízení DORA	Články 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

1. Účel

1.1. Tato politika stanoví, jak organizace chrání osobní údaje v souladu s právními povinnostmi, regulatorními rámci a mezinárodními bezpečnostními normami.

1.2. Zajišťuje, aby osobní údaje zákazníků, pracovníků a partnerů byly shromažďovány, používány, uchovávány a mazány zákonným, korektním a bezpečným způsobem.

1.3. Tato politika dále zajišťuje soulad s normou ISO/IEC 27001:2022 a podporuje připravenost na audit uplatňováním jednotného přístupu k ochraně soukromí založeného na rizicích.

1.4. Prostřednictvím této politiky organizace prokazuje odpovědnost a posiluje důvěru zákazníků tím, že upřednostňuje transparentnost, minimalizaci údajů a důsledné řízení ochrany soukromí.

2. Rozsah

2.1. Tato politika se vztahuje na:

2.1.1. všechny zaměstnance, smluvní pracovníky a poskytovatele služeb, kteří přistupují k osobním údajům, zpracovávají je nebo je spravují,

2.1.2. veškeré systémy, aplikace a umístění, v nichž jsou osobní údaje uchovávány nebo přenášeny,

2.1.3. veškeré osobní údaje bez ohledu na to, zda jsou uchovávány elektronicky, v listinné podobě, v cloudových systémech nebo v mobilních zařízeních.

2.2. Tato politika se vztahuje na údaje týkající se zákazníků, pracovníků, dodavatelů a všech dalších identifikovatelných fyzických osob.

2.3. Tato politika se uplatňuje bez ohledu na to, zda jsou údaje zpracovávány interně nebo poskytovateli služeb třetích stran.

3. Cíle

3.1. Zajistit, aby s osobními údaji bylo nakládáno v souladu s předpisy na ochranu soukromí a bezpečnostními normami, včetně GDPR, směrnice NIS2 a ISO/IEC 27001.

3.2. Chránit osobní údaje před neoprávněným přístupem, zneužitím, změnou nebo ztrátou prostřednictvím jasně stanovených technických a organizačních opatření.

3.3. Respektovat práva fyzických osob v oblasti soukromí, včetně práva na přístup k údajům, jejich opravu a výmaz.

3.4. Stanovit jasné role a odpovědnosti v oblasti ochrany dat v rámci organizace.

3.5. Prosazovat minimalizaci údajů, bezpečné uchovávání a včasný výmaz napříč všemi systémy a procesy.

3.6. Snižovat riziko nesouladu, právních sankcí, poškození dobré pověsti nebo ztráty důvěry zákazníků.

4. Role a odpovědnosti

4.1. Generální ředitel (GM)

4.1.1. schvaluje tuto politiku a zajišťuje její uplatňování,

4.1.2. poskytuje nezbytné zdroje pro řízení rizik v oblasti soukromí a reakci na incidenty,

4.1.3. nese celkovou odpovědnost za soulad s předpisy a normami v oblasti ochrany soukromí.

4.2. Koordinátor ochrany soukromí (interní nebo externě zajišťovaný)

4.2.1. vede záznamy o činnostech zpracování osobních údajů,

4.2.2. vyřizuje žádosti fyzických osob týkající se soukromí a dotazy regulačních orgánů,

4.2.3. podporuje hodnocení rizik, školení a implementaci této politiky,

4.2.4. dokumentuje případy porušení zabezpečení a v případě potřeby je oznamuje příslušným orgánům.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1. Plánované přezkumy

9.1.1. tato politika musí být přezkoumána nejméně jednou za 12 měsíců Koordinátorem ochrany soukromí a schválena generálním ředitelem (GM),

9.1.2. přezkum musí posoudit relevanci politiky, soulad s regulačními požadavky a provozní účinnost.

9.2. Spouštěče mimořádného přezkumu

9.2.1. aktualizace politiky musí být rovněž zahájena v reakci na:

9.2.1.1. nové nebo revidované právní předpisy v oblasti ochrany dat (např. GDPR, nařízení DORA),

9.2.1.2. bezpečnostní incidenty nebo případy porušení ochrany soukromí týkající se osobních údajů,

9.2.1.3. zavedení nových systémů, nástrojů nebo služeb zpracovávajících osobní údaje,

9.2.1.4. významná zjištění auditu nebo doporučení regulačního orgánu.

9.3. Řízení změn a komunikace

9.3.1. všechny změny této politiky musí být formálně zdokumentovány v přehledu změn,

9.3.2. revidované verze musí být distribuovány všem pracovníkům a příslušným smluvním pracovníkům,

9.3.3. archivované verze musí být uchovávány pro účely auditní stopy souladu.

10. Související politiky a vazby

10.1. Tato politika se uplatňuje společně s dalšími SME politikami a vytváří úplný a vymahatelný rámec ochrany soukromí:

10.1.1. P13S – Politika klasifikace a označování dat: Zajišťuje, aby osobní údaje byly vhodně klasifikovány, takže lze ochranu soukromí uplatnit podle rizika.

10.1.2. P14S – Politika uchovávání údajů a likvidace: Stanoví jasná pravidla, jak dlouho musí být osobní údaje uchovávány a jaké bezpečné metody musí být použity pro jejich likvidaci po uplynutí stanovené doby.

10.1.3. P16S – Politika maskování dat a pseudonymizace: Stanoví, jak musí být osobní identifikátory transformovány před použitím dat v neprodukčním prostředí nebo před jejich externím sdílením.

10.1.4. P30S – Politika reakce na incidenty: Upravuje kroky nezbytné pro reakci na porušení zabezpečení dat, včetně oznámení regulačním orgánům a dotčeným fyzickým osobám ve stanovených lhůtách.

10.1.5. P2S – Politika rolí a odpovědností v oblasti správy a řízení: Vyjasňuje strukturu odpovědnosti a rozhodovací role uplatňované při prosazování ochrany soukromí a dohledu nad ní.

10.2. Tyto související politiky musí být přezkoumávány a uplatňovány společně, aby bylo zajištěno komplexní pokrytí ochrany soukromí napříč systémy, pracovníky a dodavateli.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 5.1 – Vyžaduje, aby vrcholové vedení prokazovalo vedení a závazek při ochraně osobních údajů.

11.1.2. Kapitola 6.1.3 – Nařizuje ošetření rizik souvisejících se zpracováním osobních údajů.

11.1.3. Kapitola 8.1 – Vyžaduje zavedení provozních opatření k ochraně údajů v celém jejich životním cyklu.

11.2. ISO/IEC 27002

11.2.1. Opatření 5.34 – Poskytuje pokyny pro implementaci ochrany soukromí a bezpečné nakládání s PII.

11.2.2. Opatření 8.10 – Řeší bezpečnou likvidaci osobních údajů, aby se zabránilo zbytkovému zpřístupnění.

11.2.3. Opatření 8.11 – Podporuje použití maskování a pseudonymizace za účelem minimalizace údajů.

11.2.4. Opatření 8.12 – Zabraňuje neoprávněnému úniku dat prostřednictvím opatření pro přístup k datům a jejich používání.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AR-2 – Přiděluje role a odpovědnosti za řízení rizik v oblasti soukromí.

11.3.2. PL-5 – Vyžaduje dokumentaci plánu ochrany soukromí pokrývající používání a ochranu údajů.

11.3.3. AC-6 – Nařizuje zásadu minimálních oprávnění a řízení přístupu k osobním údajům.

11.3.4. IR-4 – Vyžaduje procesy zvládání incidentů pro případy porušení týkající se osobních údajů.

11.4. GDPR

11.4.1. Článek 5 – Definuje základní zásady zákonného, korektního a transparentního zpracování osobních údajů.

11.4.2. Článek 6 – Vyžaduje platný právní základ pro každou činnost zpracování osobních údajů.

11.4.3. Články 12–23 – Vymezují práva subjektů údajů, včetně přístupu, opravy, výmazu a námitky.

11.4.4. Článek 30 – Nařizuje vedení záznamů o činnostech zpracování.

11.4.5. Článek 32 – Vyžaduje odpovídající technická a organizační bezpečnostní opatření.

11.4.6. Články 33–34 – Stanoví oznamovací povinnosti při porušení zabezpečení vůči orgánům a subjektům údajů.

11.5. směrnice NIS2

11.5.1. Článek 21(2)(e) – Vyžaduje opatření k zajištění ochrany dat v souladu s politikami kybernetické bezpečnosti.

11.5.2. Článek 21(2)(f) – Nařizuje mechanismy pro řízení bezpečnosti osobních a důvěrných údajů v systémech ICT.

11.6. nařízení DORA

11.6.1. Článek 6 – Vyžaduje interní rámce správy a řízení, které řídí rizika a ochranu dat.

11.6.2. Článek 15 – Ukládá finančním subjektům zajistit, aby poskytovatelé třetích stran chránili osobní údaje a podporovali soulad s regulačními požadavky.

11.6.3. Článek 17 – Vyžaduje, aby organizace zajistily, že systémy ICT zpracovávající osobní údaje jsou bezpečné, odolné a monitorované.

11.7. COBIT 2019

11.7.1. APO12 – Řízení rizik: Vyžaduje identifikaci a ošetření rizik v oblasti soukromí a ochrany dat.

11.7.2. DSS05 – Řízení bezpečnostních služeb: Nařizuje ochranná opatření k zabránění neoprávněnému přístupu k osobním údajům.

11.7.3. MEA03 – Monitorování souladu: Vyžaduje, aby organizace zajišťovaly průběžný soulad s právními předpisy v oblasti ochrany soukromí a dat.