| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vložte název registrované právnické osoby | | | | | | |
| Číslo dokumentu:<br>PII16 | | | | | Název dokumentu:<br>**Politika školení, povědomí a kompetencí v oblasti ochrany soukromí** | | | | | | |
| Verze:<br>1.0 | | Datum účinnosti:<br>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** |
| | | | |
| | | | |

**Právní upozornění (autorská práva a omezení užití)**

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševním vlastnictvím společnosti Clarysec LLC. Žádná jeho část nesmí být kopírována, znovu použita, distribuována ani upravována pro komerční nebo implementační účely bez výslovného písemného souhlasu.

Neoprávněné použití je přísně zakázáno a může vést k právním krokům.

V případě licencování kontaktujte: info@clarysec.com

## V souladu s normami a právními předpisy

| Norma / právní předpis | Kapitola / opatření / článek | Použitelnost | Typ pokrytí | Komentář |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 7.2; Clause 7.3 | Both | Primary | Kompetence a povědomí |
| ISO/IEC 27701:2025 | Clause 7.4; Clause 7.5 | Both | Supporting | Komunikace a dokumentované důkazy |
| ISO/IEC 27701:2025 | Clause 8.1; Clause 9.1; Clause 10.2 | Both | Supporting | Provozní řízení, měření a zlepšování |
| ISO/IEC 27701:2025 | Annex A.3.17 | Both | Primary | Povědomí, vzdělávání a školení v oblasti zpracování PII |
| GDPR | Article 5(2); Article 24; Article 28; Article 32; Article 39 | Both | Supporting | Odpovědnost, řízení zpracovatelů, zabezpečení a úkoly DPO |
| ISO/IEC 27001:2022 | Clause 7.2; Clause 7.3; Annex A control 6.3 | Both | Supporting | Kompetence, povědomí a školení |
| ISO/IEC 27002:2022 | Control 6.3 | Both | Supporting | Pokyny k povědomí, vzdělávání a školení |
| ISO/IEC 29100:2020 | Clause 5.11; Clause 5.12 | Both | Supporting | Bezpečnost informací a soulad v oblasti ochrany soukromí |

## 1. Rozsah

1.1 Tato politika stanoví požadavky organizace na školení, povědomí a kompetence v oblasti ochrany soukromí v rámci systému řízení informací o soukromí.

1.2 Tato politika se vztahuje na personál, dodavatele, dočasné pracovníky, relevantní třetí strany, zpracovatele, dílčí zpracovatele a další zainteresované strany, jejichž práce může ovlivnit zpracování PII, výkonnost PIMS, práva subjektů PII, riziko pro soukromí, bezpečnost informací souvisejících s PII, pokyny pro zpracovatele, incidenty týkající se soukromí, dokumentované informace nebo důkazy o souladu.

1.3 Tato politika se vztahuje na kontexty správce, společného správce, zpracovatele a dílčího zpracovatele.

**1.4 Tato politika pokrývá:**

1.4.1 identifikaci cílových skupin školení v oblasti ochrany soukromí;

1.4.2 nástupní školení;

1.4.3 každoroční opakovací školení;

1.4.4 školení podle rolí a školení vyvolané událostí;

1.4.5 důkazy o absolvování školení;

1.4.6 eskalaci nesplnění školení;

1.4.7 přezkum účinnosti školení;

1.4.8 důkazy o zajištění školení zpracovatelů, dílčích zpracovatelů a třetích stran.

1.5 Tato politika nevytváří samostatnou matici školení, řídicí panel školení, registr lidských zdrojů, registr kompetencí, disciplinární registr ani registr školení zákazníků. Přiřazení školení, absolvování, připomínky, důkazy o kompetencích a důkazy o povědomí se zaznamenávají v REG11, přičemž výjimky, eskalace, neshody, nápravná opatření a důkazy o přezkumu se zaznamenávají v REG12. Důkazy o zajištění školení zpracovatelů, dílčích zpracovatelů a třetích stran se tam, kde je to relevantní, zaznamenávají v REG08.

**1.6 Tato politika neduplikuje:**

1.6.1 přiřazení odpovědnosti za role v PII02;

1.6.2 požadavky na evidenci činností zpracování a právní základ v PII03;

1.6.3 metodiku rizik pro soukromí a DPIA v PII07;

1.6.4 kontrolní brány ochrany osobních údajů již od návrhu v PII08;

1.6.5 řízení životního cyklu zpracovatelů v PII12;

1.6.6 provoz zabezpečení PII a řízení přístupu v PII14;

1.6.7 pracovní postup pro incidenty týkající se PII a porušení zabezpečení osobních údajů v PII15;

1.6.8 správu dokumentovaných informací v PII17;

1.6.9 řízení monitorování, interního auditu a zlepšování v PII18.

## 2. Účel

2.1 Účelem této politiky je zajistit, aby osoby, jejichž práce ovlivňuje zpracování PII, rozuměly svým odpovědnostem v oblasti ochrany soukromí, absolvovaly odpovídající školení ve stanovené periodicitě, udržovaly kompetence relevantní pro svou roli a vytvářely auditovatelné důkazy o školení, povědomí a eskalaci.

2.2 Tato politika podporuje konzistentní implementaci PIMS tím, že používá REG11 jako primární objekt důkazů o školení a povědomí a REG08, REG10 a REG12 jako podpůrné objekty důkazů.

## 3. Cíle

**3.1 Cílem této politiky je:**

3.1.1 definovat cílové skupiny školení v oblasti ochrany soukromí;

3.1.2 definovat požadavky na nástupní školení;

3.1.3 definovat požadavky na každoroční opakovací školení;

3.1.4 definovat požadavky na školení v oblasti ochrany soukromí podle rolí;

3.1.5 zaznamenávat důkazy o absolvování v REG11;

3.1.6 eskalovat nesplnění školení prostřednictvím REG12;

3.1.7 uchovávat důkazy o zajištění školení zpracovatelů, dílčích zpracovatelů a třetích stran v REG08 tam, kde je to relevantní;

3.1.8 přezkoumávat účinnost školení bez vytváření nadměrných metrik nebo duplicitních registrů;

3.1.9 zajistit, aby obsah školení zůstal sladěn s aktuálními politikami PIMS a významnými povinnostmi v oblasti ochrany soukromí.

## 4. Prohlášení politiky

### 4.1 Cílová skupina školení a přiřazení

4.1.1 [All] Privacy Lead / PIMS Manager MUSÍ definovat kategorie cílových skupin školení PIMS v REG11 před zahájením každého ročního cyklu školení.

4.1.2 [All] Process Owner / Business Owner MUSÍ identifikovat v REG11 personál, jehož povinnosti zahrnují zpracování PII, a to před onboardingem, přiřazením role nebo významnou změnou pracovních povinností.

4.1.3 [Conditional] System Owner / Application Owner MUSÍ identifikovat v REG11 uživatele vyžadující školení v oblasti ochrany soukromí pro systémy PII, privilegovaný přístup nebo administrátorské činnosti před tím, než je přístup povolen nebo významně změněn.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager MUSÍ zaznamenat rozdělení odpovědností za školení společných správců v REG11 nebo REG08 před zahájením nebo významnou změnou společné činnosti zpracování.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor MUSÍ identifikovat rozšířené potřeby školení v oblasti ochrany soukromí v REG11 před přiřazením školení rolím, které se zabývají vysoce rizikovým zpracováním, zvláštními kategoriemi PII, právy subjektů PII, DPIAs, mezinárodními předáváními nebo posouzením porušení zabezpečení osobních údajů.

4.1.6 [All] Privacy Lead / PIMS Manager MUSÍ zaznamenat přiřazenou cílovou skupinu školení, typ školení, požadované datum absolvování a vlastníka důkazů v REG11 před zahájením každého ročního cyklu školení.

### 4.2 Onboarding a roční periodicita školení

4.2.1 [All] Privacy Lead / PIMS Manager MUSÍ přiřadit základní školení povědomí o ochraně soukromí v REG11 do 10 pracovních dnů od onboardingu pro personál s přístupem k PII nebo s odpovědnostmi v PIMS.

4.2.2 [All] Process Owner / Business Owner MUSÍ zajistit, aby přiřazený personál absolvoval nástupní školení v oblasti ochrany soukromí v REG11 před schválením přístupu k PII bez dohledu nebo do 30 dnů od onboardingu, podle toho, co nastane dříve.

4.2.3 [All] Privacy Lead / PIMS Manager MUSÍ přiřadit každoroční opakovací školení v oblasti ochrany soukromí v REG11 alespoň jednou za 12 měsíců.

4.2.4 [All] Process Owner / Business Owner MUSÍ potvrdit stav absolvování každoročního opakovacího školení pro přiřazený personál v REG11 do zveřejněného ročního termínu splnění.

4.2.5 [Conditional] Privacy Lead / PIMS Manager MUSÍ přiřadit cílené opakovací školení v REG11 do 30 dnů po významné změně politiky ochrany soukromí, významné změně procesu PIMS, zjištění auditu, opakovaném selhání školení nebo relevantním poznatku z incidentu týkajícího se PII.

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

## 9. Výjimky

9.1.1 [All] Process Owner / Business Owner MUSÍ zaznamenat žádost o výjimku ze školení v oblasti ochrany soukromí v REG12 před prodloužením požadovaného termínu absolvování.

9.1.2 [All] Privacy Lead / PIMS Manager MUSÍ schválit nebo zamítnout žádosti o výjimku ze školení v oblasti ochrany soukromí v REG12 před tím, než výjimka nabude účinnosti.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSÍ poskytnout poradenství k výjimkám ze školení v REG12 před schválením, pokud výjimka ovlivňuje vysoce rizikové zpracování, zvláštní kategorie PII, vyřizování práv, řešení incidentů, mezinárodní předávání nebo důkazy pro certifikaci.

9.1.4 [Conditional] Top Management MUSÍ schválit výjimky ze školení v oblasti ochrany soukromí v REG12 před aktivací, pokud výjimka ovlivňuje opakované nesplnění, privilegovaný přístup k PII, zpracování PII s významným dopadem nebo důkazy předkládané regulačním orgánům.

9.1.5 [All] Privacy Lead / PIMS Manager MUSÍ definovat vlastníka výjimky, datum skončení platnosti, kompenzační opatření a datum přezkumu v REG12 před schválením jakékoli výjimky ze školení v oblasti ochrany soukromí.

9.1.6 [All] Process Owner / Business Owner MUSÍ uzavřít nebo obnovit schválené výjimky ze školení v oblasti ochrany soukromí v REG12 před datem skončení platnosti výjimky.

## 10. Uplatňování politiky

10.1.1 [All] Privacy Lead / PIMS Manager MUSÍ zaznamenat neshodu týkající se školení v REG12 do pěti pracovních dnů, pokud důkazy o povinném školení v oblasti ochrany soukromí chybí, jsou neúplné, po termínu nebo nejsou dohledatelné k REG11.

10.1.2 [All] Process Owner / Business Owner MUSÍ zajistit, aby povinné školení v oblasti ochrany soukromí po termínu bylo dokončeno nebo eskalováno v REG11 nebo REG12 do 10 pracovních dnů po zaznamenání stavu po termínu.

10.1.3 [Conditional] System Owner / Application Owner MUSÍ omezit nový přístup k PII s významným dopadem v REG12, pokud požadované nástupní školení nebo školení v oblasti ochrany soukromí podle rolí zůstává po eskalaci nedokončené.

10.1.4 [Processor] Vendor / Procurement Owner MUSÍ eskalovat chybějící důkazy o zajištění školení zpracovatele, dílčího zpracovatele nebo externích pracovníků v REG08 a REG12 do pěti pracovních dnů po identifikaci.

10.1.5 [Conditional] Incident Response Coordinator MUSÍ propojit opatření uplatňování související se školením s REG10 do jednoho pracovního dne, pokud selhání školení přispělo k podezření na incident týkající se PII nebo k potvrzenému incidentu týkajícímu se PII.

10.1.6 [All] Internal Audit / Compliance Reviewer MUSÍ ověřit důkazy o uzavření nápravných opatření týkajících se školení v REG12 při nejbližším plánovaném auditu nebo do 60 dnů od uzavření, podle toho, co nastane dříve.

## 11. Přezkum a údržba

11.1.1 [All] Privacy Lead / PIMS Manager MUSÍ přezkoumat tuto politiku a obsah školení alespoň jednou ročně a zaznamenat výsledek přezkumu v REG11 nebo REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUSÍ přezkoumat tuto politiku do 30 dnů po významné změně rozsahu PIMS, právních předpisů v oblasti ochrany soukromí, činností zpracování, modelu rolí, poznatků z incidentů, zjištění auditu nebo výsledků účinnosti školení.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSÍ přezkoumat změny politiky významné z hlediska ochrany soukromí v REG12 před schválením.

11.1.4 [All] Top Management MUSÍ schválit významné změny této politiky v REG12 před zveřejněním.

11.1.5 [All] Privacy Lead / PIMS Manager MUSÍ aktualizovat obsah školení a důkazy o přiřazení v REG11 do 30 dnů po schválené významné změně politiky.

## 12. Související politiky

12.1 Tato politika má být čtena společně s:

12.2 PII01 - Politika systému řízení informací o soukromí;

12.3 PII02 - Politika rolí, odpovědností a odpovědnosti za ochranu soukromí;

12.4 PII03 - Politika evidence zpracování PII a právního základu;

12.5 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti;

12.6 PII05 - Politika správy souhlasů a preferencí;

12.7 PII06 - Politika správy práv subjektů PII;

12.8 PII07 - Politika posouzení rizik pro soukromí a DPIA;

12.9 PII08 - Politika ochrany osobních údajů již od návrhu a ve výchozím nastavení;

12.10 PII09 - Politika shromažďování, používání, zpřístupňování a sdílení PII;

12.11 PII10 - Politika uchovávání, výmazu a likvidace PII;

12.12 PII12 - Politika řízení ochrany soukromí zpracovatelů, dílčích zpracovatelů a třetích stran;

12.13 PII13 - Politika mezinárodního předávání PII;

12.14 PII14 - Politika zabezpečení PII a řízení přístupu;

12.15 PII15 - Politika řízení incidentů týkajících se PII a porušení zabezpečení osobních údajů;

12.16 PII17 - Politika dokumentovaných informací a správy důkazů PIMS;

12.17 PII18 - Politika monitorování, auditu a zlepšování PIMS.

## 13. Referenční normy a rámce

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].