

				Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: PII19				Názov dokumentu: <b>Politika ochrany súkromia zamestnancov</b>							
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

<p><b>Právne upozornenie (autorské práva a obmedzenia používania)</b>  (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Tento dokument je duševným vlastníctvom spoločnosti Clarysec LLC. Žiadna časť tohto dokumentu nesmie byť bez predchádzajúceho výslovného písomného súhlasu kopírovaná, znovu použitá, distribuovaná ani upravovaná na komerčné alebo implementačné účely.</p> <p>Neoprávnené použitie je prísne zakázané a môže viesť k právnym krokom.</p> <p>V prípade licencovania kontaktujte: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p>
---

## Súlad s normami a predpismi

Norma/predpis	Ustanovenie/kontrola/článok	Uplatniteľnosť	Typ pokrytia	Poznámka
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dôkazy ochrany súkromia zamestnancov a prevádzkové riadenie
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorovanie, nezhoda a nápravné opatrenie
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Účely HR, väzba na právny základ, spúšťač DPIA, spoločná zodpovednosť a záznamy
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	Zmluvy so sprostredkovateľmi HR, pokyny, súčinnosť a záznamy
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Povinnosti zamestnancov, práva a smerovanie automatizovaného rozhodovania
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Zber, spracúvanie, minimalizácia a väzba na uchovávanie
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Záznamy o poskytnutí a nakladanie s právne záväzným poskytnutím údajov
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrana HR záznamov a dôkazy logovania
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Zásady ochrany súkromia zamestnancov a preukázateľná zodpovednosť

GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Zákonnosť, osobitné kategórie údajov a údaje z preverok spoľahlivosti
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparentnosť a oznámenia pre zamestnancov
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Práva zamestnancov a smerovanie automatizovaného rozhodovania
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Správa a riadenie, spoloční prevádzkovatelia, sprostredkovatelia, záznamy, bezpečnosť, DPIA a poradenstvo
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Účel, zber, minimalizácia, použitie, uchovávanie a poskytnutie
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparentnosť, účasť, preukázateľná zodpovednosť, bezpečnosť a súlad
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	Účel PII, zber, minimalizácia, uchovávanie a účasť dotknutej osoby
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Kontroly životného cyklu pracovnej sily chrániace PII
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Hodnotenie, monitorovanie a riadenie zmien sprostredkovateľov HR
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Riziko ochrany súkromia v HR a väzba na spúšťač DPIA

ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	Ochrana PII a životný cyklus informačnej bezpečnosti pracovnej sily
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Logovanie a monitorovacie činnosti

## 1. Rozsah

- 1.1 Táto politika stanovuje požiadavky na ochranu súkromia zamestnancov pri zbere, používaní, poskytovaní, väzbe na uchovávanie, oznamovaní, vybavovaní práv, monitorovaní, podpore zo strany sprostredkovateľov a správe dôkazov týkajúcich sa osobných údajov zamestnancov v rámci Privacy Information Management System.
- 1.2 Na účely tejto politiky „osobné údaje zamestnancov“ zahŕňajú PII týkajúce sa zamestnancov, uchádzačov o zamestnanie, bývalých zamestnancov, zmluvných pracovníkov, dočasného personálu, stážistov, vyslaných pracovníkov a ďalších účastníkov pracovnej sily, ak organizácia spracúva ich PII na účely pracovnej sily, nábora, zamestnania, spolupráce, odmeňovania, benefitov, bezpečnosti, súladu, správy pracoviska alebo súvisiace obchodné účely.
- 1.3 Táto politika sa vzťahuje na kontexty prevádzkovateľa a spoločného prevádzkovateľa, v ktorých organizácia určuje účely a prostriedky spracúvania osobných údajov zamestnancov.
- 1.4 Táto politika sa vzťahuje aj na kontexty sprostredkovateľa a ďalšieho sprostredkovateľa, v ktorých organizácia spracúva osobné údaje zamestnancov v mene zákazníka, nadradeného sprostredkovateľa alebo iného prevádzkovateľa podľa zdokumentovaných pokynov.

### 1.5 Táto politika pokrýva:

- 1.5.1 zber údajov zamestnancov;
  - 1.5.2 účely spracúvania HR;
  - 1.5.3 oznámenia o ochrane údajov pre zamestnancov;
  - 1.5.4 vybavovanie práv zamestnancov;
  - 1.5.5 väzbu na uchovávanie;
  - 1.5.6 monitorovanie zamestnancov;
  - 1.5.7 interné poskytnutie;
  - 1.5.8 kontroly sprostredkovateľov HR služieb, miezd, HRIS, benefitov, previerok spoľahlivosti a outsourcovaných HR služieb, ak sa uplatňujú;
  - 1.5.9 incidenty týkajúce sa osobných údajov zamestnancov, nezhody, nápravné opatrenia a dôkazy zlepšovania.
- 1.6 Táto politika nevytvára samostatný register ochrany súkromia v HR, register ochrany súkromia zamestnancov, register spracúvania HR, register monitorovania zamestnancov, register previerok spoľahlivosti, register HR dodávateľov, register práv zamestnancov ani register incidentov zamestnancov. Dôkazy o spracúvaní zamestnancov sa zaznamenávajú v REG02, REG04, REG06, REG07, REG08, REG10 a REG12.
- 1.7 Táto politika neposkytuje poradenstvo v oblasti pracovného práva, pracovnoprávných vzťahov, právny výklad k zamestnaneckej rade, obsah disciplinárnych postupov, obsah prevádzkových postupov miezd ani vzory pracovnoprávných dokumentov špecifické pre konkrétnu jurisdikciu.

### 1.8 Táto politika neduplikuje:

- 1.8.1 správu a riadenie PIMS v PII01;
- 1.8.2 zodpovednosť za roly v PII02;
- 1.8.3 evidenciu spracúvania a vlastníctvo právneho základu v PII03;
- 1.8.4 správu obsahu oznámení o ochrane údajov v PII04;
- 1.8.5 prevádzku súhlasov a preferencií v PII05;
- 1.8.6 pracovný tok práv dotknutých osôb v PII06;
- 1.8.7 metodiku rizík ochrany súkromia a DPIA v PII07;
- 1.8.8 brány ochrany súkromia už od návrhu v PII08;
- 1.8.9 základné pravidlá zberu, používania, poskytovania a zdieľania v PII09;

- 1.8.10 vykonávanie uchovávania, výmazu a likvidácie v PII10;
- 1.8.11 správu presnosti a kvality v PII11;
- 1.8.12 správu životného cyklu sprostredkovateľov, ďalších sprostredkovateľov a tretích strán v PII12;
- 1.8.13 kontroly mechanizmov medzinárodného prenosu v PII13;
- 1.8.14 implementáciu bezpečnosti a riadenia prístupu v PII14;
- 1.8.15 riešenie incidentov a porušení ochrany údajov v PII15;
- 1.8.16 riadenie školení a povedomia v PII16;
- 1.8.17 riadenie zdokumentovaných informácií v PII17;
- 1.8.18 správu monitorovania, auditu a zlepšovania PIMS v PII18;
- 1.8.19 kontroly AI a automatizovaného rozhodovania v PII21, ak je táto voliteľná politika zahrnutá.

## **2. Účel**

- 2.1 Účelom tejto politiky je zabezpečiť, aby sa osobné údaje zamestnancov spracúvali iba na zdokumentované, schválené, transparentné, primerané a preukázateľne zodpovedné účely pracovnej sily a aby sa dôkazy ochrany súkromia zamestnancov udržiavali v kanonických registroch PIMS bez vytvárania samostatnej dôkazovej vrstvy ochrany súkromia v HR.
- 2.2 Táto politika podporuje konzistentné zaobchádzanie so spracúvaním zamestnancov prepojením činností spracúvania zamestnancov s REG02, oznámení o ochrane údajov pre zamestnancov s REG07, žiadostí zamestnancov o uplatnenie práv s REG06, rizika ochrany súkromia v HR a spúšťačov DPIA s REG04, sprostredkovateľov HR služieb a dodávateľov miezd alebo HRIS s REG08, incidentov týkajúcich sa osobných údajov zamestnancov s REG10 a výnimiek, nezhôd, nápravných opatrení a dôkazov monitorovania s REG12.

## **3. Ciele**

### **3.1 Cieľmi tejto politiky je:**

- 3.1.1 udržiavať dôkazy evidencie spracúvania zamestnancov v REG02;
- 3.1.2 dokumentovať zdroje zberu údajov zamestnancov, kategórie PII, účely, systémy, príjemcov a väzbu na uchovávanie;
- 3.1.3 udržiavať dôkazy oznámení o ochrane údajov pre zamestnancov v REG07;
- 3.1.4 smerovať riziká ochrany súkromia zamestnancov a spúšťače DPIA cez REG04;
- 3.1.5 smerovať žiadosti zamestnancov o uplatnenie práv cez REG06;
- 3.1.6 udržiavať dôkazy o sprostredkovateľoch HR služieb, miezd, HRIS, benefitov, previerok spoľahlivosti a outsourcovaných HR služieb v REG08;
- 3.1.7 zabezpečiť, aby monitorovanie zamestnancov bolo zdokumentované, primerané, preskúmané a v príslušných prípadoch eskalované cez REG04 a REG12;
- 3.1.8 smerovať podozrenia na incidenty týkajúce sa osobných údajov zamestnancov cez REG10;
- 3.1.9 zaznamenávať výnimky ochrany súkromia zamestnancov, nezhody, nápravné opatrenia a zlepšovacie opatrenia v REG12;
- 3.1.10 vyhýbať sa poradenstvu v oblasti pracovného práva a právnomu výkladu k zamestnaneckej rade v prevádzkových ustanoveniach;
- 3.1.11 vyhýbať sa duplicitným registrom, rolám, formulárom, dashboardom alebo dôkazovým objektom špecifickým pre HR.

## **4. Vyhlásenia politiky**

### **4.1 Evidencia spracúvania zamestnancov a účely spracúvania HR**

- 4.1.1 [Controller] The Process Owner / Business Owner MUST zaznamenať každú činnosť spracúvania zamestnancov v REG02 pred tým, ako sa osobné údaje zamestnancov zhromaždia, vytvoria, importujú, použijú alebo poskytnú.
- 4.1.2 [Controller] The Process Owner / Business Owner MUST zdokumentovať kategórie osobných údajov zamestnancov, populáciu zamestnancov, zdroj zberu, účel spracúvania, systém, kategóriu interných príjemcov, kategóriu externých príjemcov a väzbu na uchovávanie v REG02 pred schválením činnosti spracúvania.
- 4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST preskúmať každú novú alebo podstatne zmenenú činnosť spracúvania zamestnancov v REG02 pred schválením činnosti spracúvania na prevádzku.
- 4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST zaznamenať poradenstvo v oblasti ochrany súkromia v REG04 pred schválením spracúvania zamestnancov zahŕňajúceho osobitné kategórie PII, údaje o trestných činoch, previerky spoľahlivosti, údaje o pracovnom zdraví, biometrické údaje, lokalizačné údaje, monitorovanie zamestnancov alebo spracúvanie, ktoré môže významne ovplyvniť zamestnanca.
- 4.1.5 [Processor] The Privacy Lead / PIMS Manager MUST zaznamenať pokyn zákazníka, účel služby, kategórie osobných údajov zamestnancov zákazníka a väzbu na rolu sprostredkovateľa v REG08 pred spracúvaním osobných údajov zamestnancov zákazníka ako outsourcovanej služby HR, miezd, benefitov, HRIS, preverovania alebo podpory pracovnej sily.
- 4.1.6 [Joint Controller] The Privacy Lead / PIMS Manager MUST zaznamenať rozdelenie zodpovedností spoločných prevádzkovateľov za spracúvanie osobných údajov zamestnancov v REG08 pred začatím spoločnej činnosti spracúvania zamestnancov.

## **4.2 Zber údajov zamestnancov a oznámenia o ochrane údajov pre zamestnancov**

- 4.2.1 [Controller] The Process Owner / Business Owner MUST obmedziť zber osobných údajov zamestnancov na kategórie zdokumentované v REG02 pred začatím zberu pri nábore, onboardingu, správe zamestnania, správe benefitov, prevádzke miezd, previerkach, monitorovaní alebo offboardingu.
- 4.2.2 [Controller] The Process Owner / Business Owner MUST zaznamenať zdroj osobných údajov zamestnancov získaných od tretích strán v REG02 pred použitím zdroja zberu tretej strany.
- 4.2.3 [Controller] The Privacy Lead / PIMS Manager MUST udržiavať záznam o oznámení o ochrane údajov pre zamestnancov v REG07 pred tým, ako sa osobné údaje zamestnancov zhromaždia priamo alebo nepriamo na nový alebo podstatne zmenený účel.
- 4.2.4 [Controller] The Process Owner / Business Owner MUST potvrdiť, že aktuálne oznámenie o ochrane údajov pre zamestnancov zaznamenané v REG07 je dostupné pred zberom pri nábore, zberom pri onboardingu, aktiváciou monitorovania, zápisom do benefitov, previerkou spoľahlivosti alebo podstatnou zmenou spracúvania zamestnancov.
- 4.2.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST preskúmať záznam oznámenia o ochrane údajov pre zamestnancov v REG07 pred zverejnením, ak oznámenie pokrýva monitorovanie zamestnancov, previerky spoľahlivosti, osobitné kategórie PII, údaje o trestných činoch, automatizované rozhodovanie alebo podstatne zmenený účel spracúvania zamestnancov.
- 4.2.6 [Processor] The Vendor / Procurement Owner MUST zaznamenať zodpovednosti za kanály zberu smerované na zamestnancov v REG08 pred tým, ako služba HR, miezd, HRIS, benefitov, preverovania alebo outsourcovaná HR služba prevádzkovaná sprostredkovateľom začne zhromažďovať osobné údaje zamestnancov v mene zákazníka.

[ ... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ... ]

## **9. Výnimky**

- 9.1.1 [All] The Process Owner / Business Owner MUST zaznamenať žiadosť o výnimku v REG12 pred odchýlením sa od akejkoľvek požiadavky tejto politiky.
- 9.1.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST zaznamenať poradenstvo v REG12 pred schválením výnimky ovplyvňujúcej monitorovanie zamestnancov, vybavovanie práv zamestnancov, preverky spoľahlivosti, osobitné kategórie PII, údaje o trestných činoch alebo spracúvanie zamestnancov s vysokým dopadom.
- 9.1.3 [Conditional] Top Management MUST schváliť výnimky ochrany súkromia zamestnancov v REG12 pred aktiváciou, ak výnimka ovplyvňuje vysokorizikové spracúvanie zamestnancov, monitorovanie zamestnancov, externé poskytnutie, spoliehanie sa na sprostredkovateľa alebo nevyriešené nápravné opatrenie.
- 9.1.4 [All] The Privacy Lead / PIMS Manager MUST priradiť každej výnimke ochrany súkromia zamestnancov dátum uplynutia platnosti nepresahujúci 90 dní v REG12 pred aktiváciou výnimky.
- 9.1.5 [All] The Privacy Lead / PIMS Manager MUST preskúmať každú výnimku ochrany súkromia zamestnancov v REG12 do piatich pracovných dní pred uplynutím platnosti.
- 9.1.6 [All] The Privacy Lead / PIMS Manager MUST uzavrieť alebo eskalovať každú výnimku ochrany súkromia zamestnancov po uplynutí platnosti v REG12 do piatich pracovných dní po uplynutí platnosti.

## **10. Uplatňovanie politiky**

- 10.1.1 [All] The Privacy Lead / PIMS Manager MUST zaznamenať nezhodu v REG12 do piatich pracovných dní, ak spracúvaniu osobných údajov zamestnancov chýbajú požadované dôkazy v REG02, REG07, REG08, REG04 alebo REG06.
- 10.1.2 [Conditional] The Incident Response Coordinator MUST zaznamenať podozrenie na neoprávnený prístup k osobným údajom zamestnancov, poskytnutie, stratu alebo kompromitáciu v REG10 do jedného pracovného dňa od zistenia.
- 10.1.3 [Controller] The Privacy Lead / PIMS Manager MUST zabrániť schváleniu nového monitorovania zamestnancov v REG12, ak chýbajú požadované dôkazy v REG02, REG04 alebo REG07.
- 10.1.4 [Both] The Vendor / Procurement Owner MUST pozastaviť nové poskytnutie osobných údajov zamestnancov HR dodávateľovi v REG08, ak chýbajú požadované dôkazy o sprostredkovateľovi, ďalšom sprostredkovateľovi, pokyne alebo súčinnosti.
- 10.1.5 [All] Top Management MUST preskúmať opakované nezhody ochrany súkromia zamestnancov v REG12, ak sa rovnaká kategória vyskytne dvakrát alebo viackrát v kľzavom období 12 mesiacov.
- 10.1.6 [All] The Internal Audit / Compliance Reviewer MUST overiť dôkazy uzavretia v REG12 pred uzavretím auditných zistení zahŕňajúcich spracúvanie v oblasti ochrany súkromia zamestnancov, oznámenia pre zamestnancov, monitorovanie zamestnancov, práva zamestnancov alebo HR dodávateľov.

## **11. Preskúmanie a údržba**

- 11.1.1 [All] The Privacy Lead / PIMS Manager MUST preskúmať túto politiku v REG12 aspoň raz ročne.
- 11.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST preskúmať túto politiku v REG12 do 30 dní od podstatnej zmeny spracúvania zamestnancov, monitorovania zamestnancov, HR

systémov, mzdových usporiadaní, poskytovateľov HRIS, poskytovateľov benefitov, poskytovateľov previerok spoľahlivosti alebo outsourcovaných HR služieb.

11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST preskúmať navrhované podstatné zmeny tejto politiky v REG12 pred schválením zo strany Top Management.

11.1.4 [All] Top Management MUST schváliť podstatné zmeny tejto politiky v REG12 pred zverejnením.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST aktualizovať REG02, REG07 alebo REG08 do 15 pracovných dní po tom, ako schválená zmena politiky ovplyvní záznamy spracúvania zamestnancov, oznámenia o ochrane údajov pre zamestnancov alebo dôkazy HR dodávateľov.

11.1.6 [All] The Internal Audit / Compliance Reviewer MUST zaznamenať pozorovania účinnosti preskúmania tejto politiky v REG12 počas plánovaného cyklu interného auditu PIMS.

## 12. Súvisiace politiky

- 12.1 Túto politiku podporujú nasledujúce súvisiace politiky:
- 12.2 PII01 - Politika Privacy Information Management System
- 12.3 PII02 - Politika rolí, zodpovedností a preukázateľnej zodpovednosti v oblasti ochrany súkromia
- 12.4 PII03 - Politika evidencie spracúvania PII a právneho základu
- 12.5 PII04 - Politika oznámení o ochrane údajov a transparentnosti
- 12.6 PII05 - Politika správy súhlasov a preferencií
- 12.7 PII06 - Politika správy práv dotknutých osôb
- 12.8 PII07 - Politika posudzovania rizík ochrany súkromia a DPIA
- 12.9 PII08 - Politika ochrany súkromia už od návrhu a štandardne
- 12.10 PII09 - Politika zberu, používania, poskytovania a zdieľania PII
- 12.11 PII10 - Politika uchovávanía, výmazu a likvidácie PII
- 12.12 PII11 - Politika presnosti a kvality PII
- 12.13 PII12 - Politika správy ochrany súkromia sprostredkovateľov, ďalších sprostredkovateľov a tretích strán
- 12.14 PII13 - Politika medzinárodného prenosu PII
- 12.15 PII14 - Politika bezpečnosti PII a riadenia prístupu
- 12.16 PII15 - Politika riadenia incidentov a porušení ochrany PII
- 12.17 PII16 - Politika školenia, povedomia a kompetencií v oblasti ochrany súkromia
- 12.18 PII17 - Politika správy zdokumentovaných informácií a dôkazov PIMS
- 12.19 PII18 - Politika monitorovania, auditu a zlepšovania PIMS
- 12.20 PII21 - Politika ochrany súkromia pri AI a automatizovanom rozhodovaní, ak je zahrnutá v rozsahu voliteľného doplnkového vydania

## 13. Referenčné normy a rámce

13.1 Táto politika je mapovaná na nasledujúce normy a predpisy. Mapovanie vysvetľuje, ako politika podporuje citované požiadavky, a identifikuje interné ustanovenia, ktoré ich implementujú alebo podporujú.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapované na zdokumentované dôkazy ochrany súkromia zamestnancov, prevádzkové schvaľovacie brány, záznamy sprostredkovateľov HR, oznámenia pre zamestnancov, záznamy monitorovania, vybavovanie výnimiek a implementačné dôkazy. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].

- 13.2.2 **Clause 9.1; Clause 10.2** - Mapované na monitorovanie ochrany súkromia zamestnancov, metriky, auditné dôkazy, vzorkovanie monitorovania zamestnancov, vybavovanie nezhôd, nápravné opatrenia a zlepšovanie. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].
- 13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mapované na účely spracúvania zamestnancov, väzbu na právny základ, smerovanie rizika ochrany súkromia a DPIA, rozdelenie zodpovedností spoločných prevádzkovateľov a záznamy spracúvania v REG02 a REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].
- 13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mapované na zmluvy so sprostredkovateľmi HR, zdokumentované pokyny, spracúvanie osobných údajov zamestnancov zákazníka, súčinnosť sprostredkovateľa a záznamy sprostredkovateľa v REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].
- 13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Mapované na vybavovanie práv zamestnancov, poradenstvo pri komplexných právach a smerovanie automatizovaného rozhodovania alebo spracúvania s vysokým dopadom cez REG06 a REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].
- 13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Mapované na obmedzenie zberu údajov zamestnancov, schválené interné použitie, minimalizáciu, väzbu na uchovávanie a smerovanie výnimiek uchovávania. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].
- 13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapované na externé poskytovanie osobných údajov zamestnancov, záznamy zdieľania údajov, oprávnenie sprostredkovateľa na poskytnutie a smerovanie incidentov súvisiacich s poskytnutím. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].
- 13.2.8 **Annex A.3.14; Annex A.3.25** - Mapované na ochranu záznamov ochrany súkromia zamestnancov, dôkazy logov monitorovania zamestnancov a podozrenie na zneužitie alebo kompromitáciu údajov z monitorovania zamestnancov. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

### 13.3 **GDPR**

- 13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Mapované na zákonné, spravodlivé, transparentné, účelovo obmedzené, minimalizované, na uchovávanie naviazané a preukázateľne zodpovedné spracúvanie osobných údajov zamestnancov. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].
- 13.3.2 **Article 6; Article 9; Article 10** - Mapované na väzbu na právny základ, smerovanie osobitných kategórií PII zamestnancov, smerovanie citlivých PII súvisiacich s pracovným zdravím a zamestnaním a smerovanie údajov o trestných činoch alebo údajov z previerok spoľahlivosti. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].
- 13.3.3 **Article 12; Article 13; Article 14** - Mapované na transparentnosť voči zamestnancom, záznamy oznámení o ochrane údajov pre zamestnancov, spúšťače oznámení pri priamom a nepriamom zbere a dôkazy oznámení o monitorovaní. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].
- 13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Mapované na smerovanie práv zamestnancov, dôkazy žiadostí, poradenstvo pri komplexných žiadostiach a smerovanie automatizovaného rozhodovania. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mapované na správu prevádzkovateľa, rozdelenie zodpovedností spoločných prevádzkovateľov, správu sprostredkovateľov HR, záznamy o spracúvaní, bezpečné zaobchádzanie, smerovanie DPIA a zapojenie poradenstva v oblasti ochrany súkromia. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

#### 13.4 **ISO/IEC 29100:2020**

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapované na špecifikáciu účelu pre zamestnancov, obmedzenie zberu, minimalizáciu, obmedzenie použitia, obmedzenie uchovávanía a obmedzenie poskytovania. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mapované na transparentnosť, účasť zamestnancov, podporu práv zamestnancov, preukázateľnú zodpovednosť, informačnú bezpečnosť a dôkazy súladu ochrany súkromia. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

#### 13.5 **ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mapované na záznamy účelu PII, kontroly zberu, minimalizáciu, väzbu na uchovávanie, obmedzenie poskytovania a podporu účasti alebo prístupu zamestnancov. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Mapované na kontroly životného cyklu pracovnej sily chrániace PII, ktoré sú relevantné pre previerky, podmienky, väzbu na uplatnenie pri porušení ochrany údajov a preskúmanie uchovávanía pri skončení alebo zmene zamestnania. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Mapované na hodnotenie sprostredkovateľov HR, monitorovanie sprostredkovateľov HR, preskúmanie HR dodávateľov a dôkazy zmien služieb v REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

#### 13.6 **ISO/IEC 29134:2020**

13.6.1 **Clause 5.1; Clause 6.2** - Mapované na prínosy posúdenia vplyvu na ochranu súkromia a určenie rizika ochrany súkromia v HR alebo spúšťača DPIA pre monitorovanie zamestnancov a HR spracúvanie s vysokým dopadom bez duplikovania metódy DPIA. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

#### 13.7 **ISO/IEC 27002:2022**

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Mapované na ochranu PII, previerky, podmienky pracovnej sily, zodpovednosti po zmene zamestnania a očakávania dôvernosti ako kontroly životného cyklu pracovnej sily podporujúce PII. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Mapované na logy monitorovania zamestnancov, monitorovacie činnosti, obmedzenie účelu logov a preskúmanie dôkazov monitorovania. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].