					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: PII19					Naziv dokumenta: **Politika privatnosti zaposlenika**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard / propis	Točka / kontrola / članak	Primjenjivost	Vrsta pokrivenosti	Napomena
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokazi o privatnosti zaposlenika i operativna kontrola
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Praćenje, nesukladnosti i korektivne radnje
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	Svrhe u području ljudskih resursa, povezanost s pravnom osnovom, okidač za DPIA-u, zajednička odgovornost i zapisi
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	Ugovori s izvršiteljima obrade u području ljudskih resursa, upute, pomoć i zapisi
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	Obveze i prava zaposlenika te usmjeravanje automatiziranog donošenja odluka
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	Povezanost prikupljanja, obrade, minimizacije i pravila zadržavanja
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	Zapisi o otkrivanju podataka i postupanje s pravno obvezujućim otkrivanjima
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Zaštita zapisa u području ljudskih resursa i dokazi o zapisivanju događaja
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Načela privatnosti zaposlenika i odgovornost

GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Zakonitost, posebne kategorije podataka i podaci iz sigurnosnih provjera
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparentnost i obavijesti za zaposlenike
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Prava zaposlenika i usmjeravanje automatiziranog donošenja odluka
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Upravljanje, zajednički voditelji obrade, izvršitelji obrade, zapisi, sigurnost, DPIA i savjetovanje
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Svrha, prikupljanje, minimizacija, uporaba, zadržavanje i otkrivanje
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparentnost, sudjelovanje, odgovornost, sigurnost i usklađenost
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	Svrha osobnih podataka (PII), prikupljanje, minimizacija, zadržavanje i sudjelovanje ispitanika
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Kontrole životnog ciklusa radne snage koje štite osobne podatke (PII)
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Procjena izvršitelja obrade u području ljudskih resursa, praćenje i kontrola promjena
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Povezanost rizika za privatnost u području ljudskih

				resursa i okidača za DPIA-u
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	Zaštita osobnih podataka (PII) i životni ciklus informacijske sigurnosti radne snage
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Aktivnosti zapisivanja događaja i praćenja

1. Opseg

1.1 Ova politika utvrđuje zahtjeve privatnosti zaposlenika za prikupljanje, uporabu, otkrivanje, povezanost s pravilima zadržavanja, obavješćivanje, postupanje s pravima, praćenje, podršku izvršitelja obrade i upravljanje dokazima u vezi s osobnim podacima (PII) zaposlenika unutar Sustava upravljanja informacijama o privatnosti.

1.2 Za potrebe ove politike, „osobni podaci (PII) zaposlenika" uključuju osobne podatke (PII) koji se odnose na zaposlenike, kandidate za posao, bivše zaposlenike, ugovorne izvođače, privremeno osoblje, vježbenike, upućene radnike i druge sudionike radne snage kada organizacija obrađuje njihove osobne podatke (PII) u svrhe povezane s radnom snagom, zapošljavanjem, radnim odnosom, angažmanom, naknadama, pogodnostima, sigurnošću, usklađenošću, administracijom radnog mjesta ili povezanim poslovnim svrhama.

1.3 Ova politika primjenjuje se na kontekste voditelja obrade i zajedničkog voditelja obrade kada organizacija određuje svrhe i sredstva obrade osobnih podataka (PII) zaposlenika.

1.4 Ova politika primjenjuje se i na kontekste izvršitelja obrade i podizvršitelja obrade kada organizacija obrađuje osobne podatke (PII) zaposlenika u ime klijenta, višeg izvršitelja obrade ili drugog voditelja obrade prema dokumentiranim uputama.

1.5 Ova politika obuhvaća sljedeća područja privatnosti zaposlenika:

1.5.1 prikupljanje podataka zaposlenika;

1.5.2 svrhe obrade u području ljudskih resursa;

1.5.3 obavijesti o privatnosti zaposlenika;

1.5.4 postupanje s pravima zaposlenika;

1.5.5 povezanost s pravilima zadržavanja;

1.5.6 praćenje zaposlenika;

1.5.7 interno otkrivanje;

1.5.8 kontrole izvršitelja obrade u području ljudskih resursa, obračuna plaća, HRIS-a, pogodnosti, sigurnosnih provjera i vanjsko ugovorenih HR usluga, gdje je primjenjivo;

1.5.9 incidente u vezi s osobnim podacima (PII) zaposlenika, nesukladnosti, korektivne radnje i dokaze o poboljšanju.

1.6 Ova politika ne uspostavlja zaseban HR registar privatnosti, registar privatnosti zaposlenika, HR registar obrade, registar praćenja zaposlenika, registar sigurnosnih provjera, registar HR dobavljača, registar prava zaposlenika ili registar incidenata zaposlenika.

1.7 Dokazi o obradi zaposlenika evidentiraju se u REG02, REG04, REG06, REG07, REG08, REG10 i REG12.

1.8 Ova politika ne pruža savjete iz područja radnog prava, savjete o radnim odnosima, pravne komentare o radničkim vijećima, sadržaj stegovnog postupka, sadržaj operativnog postupka obračuna plaća ni predloške radnopravnih dokumenata specifične za pojedinu jurisdikciju.

1.9 Ova politika ne duplicira sljedeći sadržaj povezanih politika:

1.9.1 upravljanje PIMS-om u PII01;

1.9.2 odgovornost uloga u PII02;

1.9.3 popis aktivnosti obrade i vlasništvo nad pravnom osnovom u PII03;

1.9.4 upravljanje sadržajem obavijesti o privatnosti u PII04;

1.9.5 provedbu privola i preferencija u PII05;

1.9.6 radni tok za prava ispitanika u PII06;

1.9.7 metodologiju rizika za privatnost i DPIA-e u PII07;

1.9.8 kontrolne točke ugrađene zaštite privatnosti u PII08;

1.9.9 osnovna pravila prikupljanja, uporabe, otkrivanja i dijeljenja u PII09;

1.9.10 provedbu zadržavanja, brisanja i zbrinjavanja u PII10;

1.9.11 upravljanje točnošću i kvalitetom u PII11;

1.9.12 upravljanje životnim ciklusom izvršitelja obrade, podizvršitelja obrade i trećih strana u PII12;

1.9.13 kontrole mehanizama međunarodnog prijenosa u PII13;

1.9.14 implementaciju sigurnosti i kontrole pristupa u PII14;

1.9.15 postupanje s incidentima i povredama u PII15;

1.9.16 upravljanje obukom i podizanjem svijesti u PII16;

1.9.17 kontrolu dokumentiranih informacija u PII17;

1.9.18 upravljanje praćenjem, revizijom i poboljšanjem PIMS-a u PII18;

1.9.19 kontrole umjetne inteligencije i automatiziranog donošenja odluka u PII21, kada je ta neobvezna politika uključena.

2. Svrha

2.1 Svrha ove politike jest osigurati da se osobni podaci (PII) zaposlenika obrađuju samo za dokumentirane, odobrene, transparentne, razmjerne i odgovorne svrhe povezane s radnom snagom te da se dokazi o privatnosti zaposlenika održavaju u kanonskim PIMS registrima bez stvaranja zasebnog HR sloja dokaza o privatnosti.

2.2 Ova politika podupire dosljedno postupanje s obradom zaposlenika povezivanjem aktivnosti obrade zaposlenika s REG02, obavijesti o privatnosti zaposlenika s REG07, zahtjeva za ostvarivanje prava zaposlenika s REG06, rizika za privatnost u području ljudskih resursa i okidača za DPIA-u s REG04, izvršitelja obrade u području ljudskih resursa i dobavljača za obračun plaća ili HRIS s REG08, incidenata u vezi s osobnim podacima (PII) zaposlenika s REG10 te iznimaka, nesukladnosti, korektivnih radnji i dokaza praćenja s REG12.

3. Ciljevi

3.1 Ciljevi ove politike jesu:

3.1.1 održavati dokaze popisa aktivnosti obrade zaposlenika u REG02;

3.1.2 dokumentirati izvore prikupljanja podataka zaposlenika, kategorije osobnih podataka (PII), svrhe, sustave, primatelje i povezanost s pravilima zadržavanja;

3.1.3 održavati dokaze obavijesti o privatnosti zaposlenika u REG07;

3.1.4 usmjeravati rizike za privatnost u području ljudskih resursa i okidače za DPIA-u kroz REG04;

3.1.5 usmjeravati zahtjeve za ostvarivanje prava zaposlenika kroz REG06;

3.1.6 održavati dokaze o izvršiteljima obrade u području ljudskih resursa, obračunu plaća, HRIS-u, pogodnostima, sigurnosnim provjerama i vanjsko ugovorenim HR uslugama u REG08;

3.1.7 osigurati da je praćenje zaposlenika dokumentirano, razmjerno, pregledano i eskalirano kroz REG04 i REG12 gdje je primjenjivo;

3.1.8 usmjeravati sumnje na incidente u vezi s osobnim podacima (PII) zaposlenika kroz REG10;

3.1.9 evidentirati iznimke privatnosti zaposlenika, nesukladnosti, korektivne radnje i radnje poboljšanja u REG12;

3.1.10 izbjegavati savjete iz područja radnog prava i pravne komentare o radničkim vijećima unutar operativnih odredbi;

3.1.11 izbjegavati duplicirane registre, uloge, obrasce, nadzorne ploče ili objekte dokaza specifične za HR.

4. Izjave politike

4.1 Popis aktivnosti obrade zaposlenika i svrhe obrade u području ljudskih resursa

4.1.1 [Controller] Process Owner / Business Owner mora evidentirati svaku aktivnost obrade zaposlenika u REG02 prije nego što se osobni podaci (PII) zaposlenika prikupe, generiraju, uvezu, upotrijebe ili otkriju.

4.1.2 [Controller] Process Owner / Business Owner mora u REG02 dokumentirati kategorije osobnih podataka (PII) zaposlenika, populaciju zaposlenika, izvor prikupljanja, svrhu obrade, sustav, kategoriju internog primatelja, kategoriju vanjskog primatelja i povezanost s pravilima zadržavanja prije odobrenja aktivnosti obrade.

4.1.3 [Controller] Privacy Lead / PIMS Manager mora pregledati svaku novu ili značajno promijenjenu aktivnost obrade zaposlenika u REG02 prije odobrenja aktivnosti obrade za operativnu uporabu.

4.1.4 [Conditional] Data Protection Officer / Privacy Advisor mora evidentirati savjet o privatnosti u REG04 prije odobrenja obrade zaposlenika koja uključuje posebne kategorije osobnih podataka (PII), podatke o kaznenim djelima, sigurnosne provjere, podatke o zdravlju na radu, biometriju, podatke o lokaciji, praćenje zaposlenika ili obradu koja može značajno utjecati na zaposlenika.

4.1.5 [Processor] Privacy Lead / PIMS Manager mora u REG08 evidentirati uputu klijenta, svrhu usluge, kategorije osobnih podataka (PII) zaposlenika klijenta i povezanost s ulogom izvršitelja obrade prije obrade osobnih podataka (PII) zaposlenika klijenta kao vanjsko ugovorene HR usluge, usluge obračuna plaća, pogodnosti, HRIS-a, provjere ili podrške radnoj snazi.

4.1.6 [Joint Controller] Privacy Lead / PIMS Manager mora u REG08 evidentirati raspodjelu odgovornosti zajedničkog voditelja obrade za obradu osobnih podataka (PII) zaposlenika prije početka zajedničke aktivnosti obrade zaposlenika.

4.2 Prikupljanje podataka zaposlenika i obavijesti o privatnosti zaposlenika

4.2.1 [Controller] Process Owner / Business Owner mora ograničiti prikupljanje osobnih podataka (PII) zaposlenika na kategorije dokumentirane u REG02 prije početka prikupljanja u okviru zapošljavanja, uvođenja u posao, administracije radnog odnosa, administracije pogodnosti, obračuna plaća, provjera, praćenja ili izlaznog procesa.

4.2.2 [Controller] Process Owner / Business Owner mora evidentirati izvor osobnih podataka (PII) zaposlenika prikupljenih od trećih strana u REG02 prije uporabe izvora prikupljanja od treće strane.

4.2.3 [Controller] Privacy Lead / PIMS Manager mora održavati zapis obavijesti o privatnosti zaposlenika u REG07 prije izravnog ili neizravnog prikupljanja osobnih podataka (PII) zaposlenika za novu ili značajno promijenjenu svrhu.

4.2.4 [Controller] Process Owner / Business Owner mora potvrditi da je važeća obavijest o privatnosti zaposlenika evidentirana u REG07 dostupna prije prikupljanja u okviru zapošljavanja, prikupljanja pri uvođenju u posao, aktivacije praćenja, upisa u pogodnosti, sigurnosne provjere ili značajne promjene obrade zaposlenika.

4.2.5 [Conditional] Data Protection Officer / Privacy Advisor mora pregledati zapis obavijesti o privatnosti zaposlenika u REG07 prije objave kada obavijest obuhvaća praćenje zaposlenika, sigurnosnu provjeru, posebne kategorije osobnih podataka (PII), podatke o kaznenim djelima, automatizirano donošenje odluka ili značajno promijenjenu svrhu obrade zaposlenika.

4.2.6 [Processor] Vendor / Procurement Owner mora evidentirati odgovornosti za kanale prikupljanja usmjerene prema zaposlenicima u REG08 prije nego što HR usluga, obračun plaća, HRIS, pogodnosti, provjere ili vanjsko ugovorena HR usluga kojom upravlja izvršitelj obrade prikuplja osobne podatke (PII) zaposlenika u ime klijenta.

9. Iznimke

9.1.1 [All] Process Owner / Business Owner mora evidentirati zahtjev za iznimku u REG12 prije odstupanja od bilo kojeg zahtjeva ove politike.

9.1.2 [Conditional] Data Protection Officer / Privacy Advisor mora evidentirati savjet u REG12 prije odobrenja iznimke koja utječe na praćenje zaposlenika, postupanje s pravima zaposlenika, sigurnosne provjere, posebne kategorije osobnih podataka (PII), podatke o kaznenim djelima ili obradu zaposlenika s visokim utjecajem.

9.1.3 [Conditional] Top Management mora odobriti iznimke privatnosti zaposlenika u REG12 prije aktivacije kada iznimka utječe na visokorizičnu obradu zaposlenika, praćenje zaposlenika, vanjsko otkrivanje, oslanjanje na izvršitelja obrade ili neriješenu korektivnu radnju.

9.1.4 [All] Privacy Lead / PIMS Manager mora dodijeliti datum isteka koji ne premašuje 90 dana svakoj iznimci privatnosti zaposlenika u REG12 prije aktivacije iznimke.

9.1.5 [All] Privacy Lead / PIMS Manager mora pregledati svaku iznimku privatnosti zaposlenika u REG12 u roku od pet radnih dana prije isteka.

9.1.6 [All] Privacy Lead / PIMS Manager mora zatvoriti ili eskalirati svaku isteklu iznimku privatnosti zaposlenika u REG12 u roku od pet radnih dana nakon isteka.

10. Provedba

10.1.1 [All] Privacy Lead / PIMS Manager mora evidentirati nesukladnost u REG12 u roku od pet radnih dana kada obradi osobnih podataka (PII) zaposlenika nedostaju potrebni dokazi iz REG02, REG07, REG08, REG04 ili REG06.

10.1.2 [Conditional] Incident Response Coordinator mora evidentirati sumnju na neovlašteni pristup, otkrivanje, gubitak ili kompromitaciju osobnih podataka (PII) zaposlenika u REG10 u roku od jednog radnog dana od utvrđivanja.

10.1.3 [Controller] Privacy Lead / PIMS Manager mora spriječiti odobrenje novog praćenja zaposlenika u REG12 kada nedostaju potrebni dokazi iz REG02, REG04 ili REG07.

10.1.4 [Both] Vendor / Procurement Owner mora obustaviti novo otkrivanje osobnih podataka (PII) zaposlenika HR dobavljaču u REG08 kada nedostaju potrebni dokazi o izvršitelju obrade, podizvršitelju obrade, uputi ili pomoći.

10.1.5 [All] Top Management mora pregledati ponovljene nesukladnosti privatnosti zaposlenika u REG12 kada se ista kategorija pojavi dva ili više puta u pomičnom razdoblju od 12 mjeseci.

10.1.6 [All] Internal Audit / Compliance Reviewer mora provjeriti dokaze zatvaranja u REG12 prije zatvaranja nalaza revizije koji uključuju obradu osobnih podataka (PII) zaposlenika, obavijesti zaposlenicima, praćenje zaposlenika, prava zaposlenika ili HR dobavljače.

11. Pregled i održavanje

11.1.1 [All] Privacy Lead / PIMS Manager mora pregledati ovu politiku u REG12 najmanje jednom godišnje.

11.1.2 [Conditional] Privacy Lead / PIMS Manager mora pregledati ovu politiku u REG12 u roku od 30 dana od značajne promjene obrade zaposlenika, praćenja zaposlenika, HR sustava, aranžmana obračuna plaća, pružatelja HRIS-a, pružatelja pogodnosti, pružatelja sigurnosnih provjera ili vanjsko ugovorenih HR usluga.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor mora pregledati predložene značajne promjene ove politike u REG12 prije odobrenja od strane Top Management.

11.1.4 [All] Top Management mora odobriti značajne promjene ove politike u REG12 prije objave.

11.1.5 [All] Privacy Lead / PIMS Manager mora ažurirati REG02, REG07 ili REG08 u roku od 15 radnih dana nakon što odobrena promjena politike utječe na zapise obrade zaposlenika, obavijesti o privatnosti zaposlenika ili dokaze HR dobavljača.

11.1.6 [All] Internal Audit / Compliance Reviewer mora evidentirati opažanja o djelotvornosti pregleda ove politike u REG12 tijekom planiranog ciklusa interne revizije PIMS-a.

12. Povezane politike

12.1 Ovu politiku podupiru sljedeće povezane politike:

12.2 PII01 - Politika Sustava upravljanja informacijama o privatnosti

12.3 PII02 - Politika uloga, odgovornosti i odgovornosti za privatnost

12.4 PII03 - Politika popisa aktivnosti obrade osobnih podataka (PII) i pravne osnove

12.5 PII04 - Politika obavijesti o privatnosti i transparentnosti

12.6 PII05 - Politika upravljanja privolama i preferencijama

12.7 PII06 - Politika upravljanja pravima ispitanika

12.8 PII07 - Politika procjene rizika za privatnost i DPIA-e

12.9 PII08 - Politika ugrađene i zadane zaštite privatnosti

12.10 PII09 - Politika prikupljanja, uporabe, otkrivanja i dijeljenja osobnih podataka (PII)

12.11 PII10 - Politika zadržavanja, brisanja i zbrinjavanja osobnih podataka (PII)

12.12 PII11 - Politika točnosti i kvalitete osobnih podataka (PII)

12.13 PII12 - Politika upravljanja privatnošću izvršitelja obrade, podizvršitelja obrade i trećih strana

12.14 PII13 - Politika međunarodnog prijenosa osobnih podataka (PII)

12.15 PII14 - Politika sigurnosti i kontrole pristupa osobnim podacima (PII)

12.16 PII15 - Politika upravljanja incidentima i povredama osobnih podataka (PII)

12.17 PII16 - Politika osposobljavanja, podizanja svijesti i kompetencija u području privatnosti

12.18 PII17 - Politika upravljanja dokumentiranim informacijama i dokazima PIMS-a

12.19 PII18 - Politika praćenja, revizije i poboljšanja PIMS-a

12.20 PII21 - Politika privatnosti za umjetnu inteligenciju i automatizirano donošenje odluka, kada je uključena u opseg neobveznog dodatnog izdanja

13. Referentni standardi i okviri

13.1 Ova politika mapirana je na sljedeće standarde i propise. Mapiranje objašnjava kako politika podupire navedene zahtjeve i identificira interne odredbe koje ih provode ili podupiru.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapirano na dokumentirane dokaze o privatnosti zaposlenika, operativne kontrolne točke odobrenja, zapise izvršitelja obrade u području ljudskih resursa, obavijesti o privatnosti zaposlenika, zapise praćenja, postupanje s iznimkama i dokaze implementacije. 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** - Mapirano na praćenje privatnosti zaposlenika, metrike, revizijske dokaze, uzorkovanje praćenja zaposlenika, postupanje s nesukladnostima, korektivne radnje i poboljšanje. 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** - Mapirano na svrhe obrade zaposlenika, povezanost s pravnom osnovom, usmjeravanje rizika za privatnost i DPIA-e, raspodjelu zajedničkog voditelja obrade i zapise o obradi u REG02 i 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** - Mapirano na ugovore s izvršiteljima obrade u području ljudskih resursa, dokumentirane upute, obradu

osobnih podataka (PII) zaposlenika klijenta, pomoć izvršitelja obrade i zapise izvršitelja obrade u 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** - Mapirano na postupanje s pravima zaposlenika, savjete za složena prava i usmjeravanje automatiziranog donošenja odluka ili obrade s visokim utjecajem kroz REG06 i 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** - Mapirano na ograničenje prikupljanja podataka zaposlenika, odobrenu internu uporabu, minimizaciju, povezanost s pravilima zadržavanja i usmjeravanje iznimki zadržavanja. 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** - Mapirano na vanjska otkrivanja osobnih podataka (PII) zaposlenika, zapise o dijeljenju podataka, odobrenje otkrivanja od strane izvršitelja obrade i usmjeravanje incidenata povezanih s otkrivanjem. 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** - Mapirano na zaštitu zapisa o privatnosti zaposlenika, dokaze dnevnika praćenja zaposlenika i sumnju na zlouporabu ili kompromitaciju podataka praćenja zaposlenika. 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)** - Mapirano na zakonitu, poštenu, transparentnu, svrhom ograničenu, minimiziranu, s pravilima zadržavanja povezanu i odgovornu obradu osobnih podataka (PII) zaposlenika. 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** - Mapirano na povezanost s pravnom osnovom, usmjeravanje posebnih kategorija osobnih podataka (PII) zaposlenika, usmjeravanje osjetljivih osobnih podataka (PII) povezanih sa zdravljem na radu i radnim odnosom te usmjeravanje podataka o kaznenim djelima ili sigurnosnim provjerama. 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** - Mapirano na transparentnost prema zaposlenicima, zapise obavijesti o privatnosti zaposlenika, okidače obavještavanja pri izravnom i neizravnom prikupljanju te dokaze obavijesti o praćenju. 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** - Mapirano na usmjeravanje prava zaposlenika, dokaze zahtjeva, savjete za složene zahtjeve i usmjeravanje automatiziranog donošenja odluka. 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** - Mapirano na upravljanje voditelja obrade, raspodjelu zajedničkog voditelja obrade, upravljanje izvršiteljima obrade u području ljudskih resursa, zapise o obradi, sigurno postupanje, usmjeravanje DPIA-e i uključivanje savjetodavne uloge za privatnost. 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** - Mapirano na određivanje svrhe obrade zaposlenika, ograničenje prikupljanja, minimizaciju, ograničenje uporabe, ograničenje zadržavanja i ograničenje otkrivanja. 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** - Mapirano na transparentnost, sudjelovanje zaposlenika, podršku pravima zaposlenika, odgovornost,

informacijsku sigurnost i dokaze usklađenosti s privatnošću. 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** - Mapirano na zapise svrhe osobnih podataka (PII), kontrole prikupljanja, minimizaciju, povezanost s pravilima zadržavanja, ograničenje otkrivanja i podršku sudjelovanju ili pristupu zaposlenika. 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** - Mapirano na kontrole životnog ciklusa radne snage koje štite osobne podatke (PII) i relevantne su za provjere, uvjete, povezanost s provedbom u slučaju povrede privatnosti te pregled zadržavanja pri prestanku ili promjeni zaposlenja. 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** - Mapirano na procjenu izvršitelja obrade u području ljudskih resursa, praćenje izvršitelja obrade u području ljudskih resursa, pregled HR dobavljača i dokaze promjene usluge u 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** - Mapirano na koristi procjene učinka na privatnost i utvrđivanje rizika za privatnost u području ljudskih resursa ili okidača za DPIA-u za praćenje zaposlenika i HR obradu s visokim utjecajem bez dupliciranja metode DPIA-e. 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 - Mapirano na zaštitu osobnih podataka (PII), provjere, uvjete za radnu snagu, odgovornosti nakon promjene zaposlenja i očekivanja povjerljivosti kao kontrole životnog ciklusa radne snage koje podupiru osobne podatke (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 - Mapirano na dnevnike praćenja zaposlenika, aktivnosti praćenja, ograničenje svrhe dnevnika i pregled dokaza praćenja. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].