| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ange namnet på den registrerade juridiska personen här | | | | | | | |
| Dokumentnummer:<br>PII19 | | | | | Dokumenttitel:<br>**Policy för anställdas integritet** | | | | | | | |
| Version:<br>1.0 | | Ikraftträdandedatum:<br>01.01.2025 | | | Dokumentägare: | | | | | | | |
| X | Policy | | Standard | | Rutin | | Formulär | | Register | | Övrigt | |

| **Revisionshistorik** | | | | |
|---|---|---|---|---|
| **Revisionsnummer** | **Revisionsdatum** | **Ändringar** | **Granskad av** | **Processägare** |
| | | | | |
| | | | | |

| **Godkännanden** | | | |
|---|---|---|---|
| **Namn** | **Titel** | **Datum** | **Underskrift** |
| | | | |
| | | | |

## Ansluten till standarder och regelverk

| Standard / regelverk | Klausul / kontroll / artikel | Tillämplighet | Täckningstyp | Kommentar |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 7.5; Clause 8.1 | Both | Primary | Underlag för anställdas integritet och operativ styrning |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Övervakning, avvikelse och korrigerande åtgärder |
| 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 | HR-ändamål, koppling till rättslig grund, DPIA-utlösare, gemensamt ansvar och register |
| 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 | Avtal med HR-personuppgiftsbiträden, instruktioner, stöd och register |
| 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 | Skyldigheter, rättigheter och dirigering vid automatiserade beslut för anställda |
| 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 | Koppling för insamling, behandling, minimering och bevarande |
| 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 | Register över utlämnanden och hantering av rättsligt bindande utlämnanden |
| ISO/IEC 27701:2025 | Annex A.3.14; Annex A.3.25 | Both | Supporting | Skydd av HR-poster och loggningsunderlag |
| GDPR | Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2) | Controller | Primary | Principer för anställdas integritet och ansvarsskyldighet |
| GDPR | Article 6; Article 9; Article 10 | Controller | Supporting | Laglighet, särskilda kategorier och uppgifter för bakgrundsscreening |
| GDPR | Article 12; Article 13; Article 14 | Controller | Primary | Transparens och meddelanden för anställda |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 15;<br>Article 16;<br>Article 17;<br>Article 18;<br>Article 21;<br>Article 22 | Controller | Supporting | Anställdas rättigheter och dirigering vid automatiserade beslut |
| GDPR | Article 24;<br>Article 26;<br>Article 28;<br>Article 30;<br>Article 32;<br>Article 35;<br>Article 39 | Both | Supporting | Styrning, gemensamt personuppgiftsansvariga, personuppgiftsbiträden, register, säkerhet, DPIA och rådgivning |
| ISO/IEC 29100:2020 | Clause 5.3;<br>Clause 5.4;<br>Clause 5.5;<br>Clause 5.6 | Controller | Supporting | Ändamål, insamling, minimering, användning, bevarande och utlämnande |
| ISO/IEC 29100:2020 | Clause 5.8;<br>Clause 5.9;<br>Clause 5.10;<br>Clause 5.11;<br>Clause 5.12 | Both | Supporting | Transparens, deltagande, ansvarsskyldighet, säkerhet och efterlevnad |
| ISO/IEC 29151:2022 | Annex A.3;<br>Annex A.4;<br>Annex A.5;<br>Annex A.7;<br>Annex A.10 | Controller | Supporting | PII-ändamål, insamling, minimering, bevarande och registrerades deltagande |
| ISO/IEC 29151:2022 | Clause 7.1.2;<br>Clause 7.1.3;<br>Clause 7.2.4;<br>Clause 7.3.2 | Controller | Supporting | Livscykelkontroller för personal som skyddar PII |
| ISO/IEC 29151:2022 | Clause 15.1.2;<br>Clause 15.2.2;<br>Clause 15.2.3 | Both | Supporting | Utvärdering, övervakning och ändringsstyrning av HR-personuppgiftsbiträden |
| ISO/IEC 29134:2020 | Clause 5.1;<br>Clause 6.2 | Controller | Supporting | Koppling till HR-integritetsrisk och DPIA-utlösare |
| ISO/IEC 27002:2022 | Controls 5.34; 6.1; 6.2; 6.5; 6.6 | Both | Supporting | PII-skydd och informationssäkerhetslivscykel för personal |
| ISO/IEC 27002:2022 | Controls 8.15; 8.16 | Both | Supporting | Loggnings- och övervakningsaktiviteter |

## 1. Omfattning

1.1 Denna policy fastställer krav på anställdas integritet för insamling, användning, utlämnande, bevarandekoppling, integritetsmeddelanden, hantering av rättigheter, övervakning, stöd från personuppgiftsbiträden och hantering av underlag för personuppgifter om anställda inom ledningssystemet för hantering av integritetsinformation.

1.2 I denna policy omfattar ”personuppgifter om anställda” PII som avser anställda, arbetssökande, tidigare anställda, uppdragstagare, tillfällig personal, praktikanter, utsända medarbetare och andra deltagare i personalstyrkan när organisationen behandlar deras PII för ändamål som rör personal, rekrytering, anställning, engagemang, ersättning, förmåner, säkerhet, efterlevnad, arbetsplatsadministration eller relaterade affärsändamål.

1.3 Denna policy gäller i sammanhang där organisationen är personuppgiftsansvarig eller gemensamt personuppgiftsansvarig och fastställer ändamål och medel för behandling av personuppgifter om anställda.

1.4 Denna policy gäller även i sammanhang där organisationen är personuppgiftsbiträde eller underbiträde och behandlar personuppgifter om anställda för en kunds, ett uppströms personuppgiftsbiträdes eller en annan personuppgiftsansvarigs räkning enligt dokumenterade instruktioner.

**1.5 Denna policy omfattar:**

1.5.1 insamling av uppgifter om anställda;

1.5.2 HR-behandlingsändamål;

1.5.3 integritetsmeddelanden till anställda;

1.5.4 hantering av anställdas rättigheter;

1.5.5 bevarandekoppling;

1.5.6 övervakning av anställda;

1.5.7 internt utlämnande;

1.5.8 kontroller för HR-personuppgiftsbiträden, löner, HR-informationssystem, förmåner, bakgrundsscreening och utlagda HR-tjänster där det är tillämpligt;

1.5.9 incidenter som rör personuppgifter om anställda, avvikelser, korrigerande åtgärder och förbättringsunderlag.

1.6 Denna policy skapar inte något separat HR-integritetsregister, register över anställdas integritet, HR-behandlingsregister, register över övervakning av anställda, register över bakgrundsscreening, HR-leverantörsregister, register över anställdas rättigheter eller incidentregister för anställda. Underlag för behandling av anställdas uppgifter registreras i REG02, REG04, REG06, REG07, REG08, REG10 och REG12.

1.7 Denna policy tillhandahåller inte rådgivning inom arbetsrätt, rådgivning om arbetsmarknadsrelationer, juridiska kommentarer om företagsråd, innehåll för disciplinära förfaranden, innehåll för lönehanteringsrutiner eller anställningsdokumentmallar för specifika jurisdiktioner.

**1.8 Denna policy duplicerar inte:**

1.8.1 PIMS-styrning i PII01;

1.8.2 rollansvar i PII02;

1.8.3 behandlingsförteckning och ägarskap för rättslig grund i PII03;

1.8.4 styrning av innehåll i integritetsmeddelanden i PII04;

1.8.5 hantering av samtycke och preferenser i PII05;

1.8.6 arbetsflöde för registrerades PII-rättigheter i PII06;

1.8.7 metodik för integritetsrisk och DPIA i PII07;

1.8.8 grindar för inbyggt dataskydd i PII08;

1.8.9 basregler för insamling, användning, utlämnande och delning i PII09;

1.8.10 genomförande av bevarande, radering och bortskaffning i PII10;

1.8.11 styrning av korrekthet och kvalitet i PII11;

1.8.12 livscykelstyrning för personuppgiftsbiträden, underbiträden och tredje parter i PII12;

1.8.13 kontroller av mekanismer för internationell överföring i PII13;

1.8.14 genomförande av säkerhet och åtkomstkontroll i PII14;

1.8.15 incident- och personuppgiftsincidenthantering i PII15;

1.8.16 hantering av utbildning och medvetenhet i PII16;

1.8.17 styrning av dokumenterad information i PII17;

1.8.18 styrning av PIMS-övervakning, revision och förbättring i PII18;

1.8.19 kontroller för AI och automatiserat beslutsfattande i PII21, där den valfria policyn ingår.

## 2. Syfte

2.1 Syftet med denna policy är att säkerställa att personuppgifter om anställda endast behandlas för dokumenterade, godkända, transparenta, proportionerliga och ansvarsskyldiga personaländamål, och att underlag för anställdas integritet upprätthålls i de kanoniska PIMS-registren utan att ett separat HR-integritetslager för underlag skapas.

2.2 Denna policy stödjer konsekvent hantering av behandling som rör anställda genom att koppla behandlingsaktiviteter för anställda till REG02, integritetsmeddelanden till anställda till REG07, rättighetsbegäranden från anställda till REG06, HR-integritetsrisk och DPIA-utlösare till REG04, HR-personuppgiftsbiträden och löne- eller HRIS-leverantörer till REG08, incidenter som rör personuppgifter om anställda till REG10 samt undantag, avvikelser, korrigerande åtgärder och övervakningsunderlag till REG12.

## 3. Mål

### 3.1 Målen med denna policy är att:

3.1.1 upprätthålla underlag för behandlingsförteckning avseende anställda i REG02;

3.1.2 dokumentera insamlingskällor, PII-kategorier, ändamål, system, mottagare och bevarandekoppling för anställda;

3.1.3 upprätthålla underlag för integritetsmeddelanden till anställda i REG07;

3.1.4 dirigera HR-integritetsrisk och DPIA-utlösare via REG04;

3.1.5 dirigera rättighetsbegäranden från anställda via REG06;

3.1.6 upprätthålla underlag för HR-personuppgiftsbiträden, löner, HR-informationssystem, förmåner, bakgrundsscreening och utlagda HR-tjänster i REG08;

3.1.7 säkerställa att övervakning av anställda dokumenteras, är proportionerlig, granskas och eskaleras via REG04 och REG12 där det är tillämpligt;

3.1.8 dirigera misstänkta incidenter som rör personuppgifter om anställda via REG10;

3.1.9 registrera undantag, avvikelser, korrigerande åtgärder och förbättringsåtgärder som rör anställdas integritet i REG12;

3.1.10 undvika arbetsrättslig rådgivning och juridiska kommentarer om företagsråd i operativa klausuler;

3.1.11 undvika duplicerade register, roller, formulär, kontrollpaneler eller HR-specifika underlagsobjekt.

## 4. Policyuttalanden

### 4.1 Behandlingsförteckning för anställda och HR-behandlingsändamål

4.1.1 [Controller] The Process Owner / Business Owner MUST registrera varje behandlingsaktivitet som rör anställda i REG02 innan personuppgifter om anställda samlas in, genereras, importeras, används eller lämnas ut.

4.1.2 [Controller] The Process Owner / Business Owner MUST dokumentera kategorier av personuppgifter om anställda, personalgrupp, insamlingskälla, behandlingsändamål, system, intern mottagarkategori, extern mottagarkategori och bevarandekoppling i REG02 innan behandlingsaktiviteten godkänns.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST granska varje ny eller väsentligt ändrad behandlingsaktivitet som rör anställda i REG02 innan behandlingsaktiviteten godkänns för drift.

4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST registrera integritetsrådgivning i REG04 innan godkännande av behandling av anställda som innefattar PII i särskild kategori, uppgifter om brott, bakgrundsscreening, företagshälsouppgifter, biometri, platsdata, övervakning av anställda eller behandling som väsentligt kan påverka en anställd.

4.1.5 [Processor] The Privacy Lead / PIMS Manager MUST registrera kundinstruktion, tjänsteändamål, kundens kategorier av personuppgifter om anställda och koppling till rollen som personuppgiftsbiträde i REG08 innan kundens personuppgifter om anställda behandlas som en utlagd HR-, löne-, förmåns-, HRIS-, screening- eller personalstödstjänst.

4.1.6 [Joint Controller] The Privacy Lead / PIMS Manager MUST registrera ansvarsfördelningen för gemensamt personuppgiftsansvar vid behandling av personuppgifter om anställda i REG08 innan den gemensamma behandlingsaktiviteten som rör anställda inleds.

### 4.2 Insamling av uppgifter om anställda och integritetsmeddelanden till anställda

4.2.1 [Controller] The Process Owner / Business Owner MUST begränsa insamlingen av personuppgifter om anställda till de kategorier som dokumenterats i REG02 innan insamling för rekrytering, introduktion, anställningsadministration, förmånsadministration, lönehantering, screening, övervakning eller avslut av anställning eller uppdrag inleds.

4.2.2 [Controller] The Process Owner / Business Owner MUST registrera källan till personuppgifter om anställda som samlas in från tredje parter i REG02 innan insamlingskällan från tredje part används.

4.2.3 [Controller] The Privacy Lead / PIMS Manager MUST upprätthålla en post för integritetsmeddelande till anställda i REG07 innan personuppgifter om anställda samlas in direkt eller indirekt för ett nytt eller väsentligt ändrat ändamål.

4.2.4 [Controller] The Process Owner / Business Owner MUST bekräfta att det aktuella integritetsmeddelandet till anställda som registrerats i REG07 är tillgängligt innan insamling för rekrytering, introduktionsinsamling, aktivering av övervakning, inskrivning i förmåner, bakgrundsscreening eller en väsentlig ändring av behandling som rör anställda.

4.2.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST granska REG07-posten för integritetsmeddelande till anställda innan publicering när meddelandet omfattar övervakning av anställda, bakgrundsscreening, PII i särskild kategori, uppgifter om brott, automatiserat beslutsfattande eller ett väsentligt ändrat behandlingsändamål som rör anställda.

4.2.6 [Processor] The Vendor / Procurement Owner MUST registrera ansvar för insamlingskanaler riktade till anställda i REG08 innan en HR-, löne-, HRIS-, förmåns-, screening- eller utlagd HR-tjänst som drivs av ett personuppgiftsbiträde samlar in personuppgifter om anställda för en kunds räkning.

[ ... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ... ]

## 9. Undantag

9.1.1 [All] The Process Owner / Business Owner MUST registrera en undantagsbegäran i REG12 innan avvikelse görs från något krav i denna policy.

9.1.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST registrera rådgivning i REG12 innan godkännande av ett undantag som påverkar övervakning av anställda, hantering av anställdas rättigheter, bakgrundsscreening, PII i särskild kategori, uppgifter om brott eller behandling av anställda med hög påverkan.

9.1.3 [Conditional] Top Management MUST godkänna undantag som rör anställdas integritet i REG12 innan aktivering när undantaget påverkar högriskbehandling av anställda, övervakning av anställda, externt utlämnande, beroende av personuppgiftsbiträde eller olöst korrigerande åtgärd.

9.1.4 [All] The Privacy Lead / PIMS Manager MUST tilldela ett utgångsdatum som inte överstiger 90 dagar till varje undantag som rör anställdas integritet i REG12 innan undantaget aktiveras.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST granska varje undantag som rör anställdas integritet i REG12 inom fem arbetsdagar före utgång.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST stänga eller eskalera varje utgånget undantag som rör anställdas integritet i REG12 inom fem arbetsdagar efter utgång.

## 10. Efterlevnad av policyn

10.1.1 [All] The Privacy Lead / PIMS Manager MUST registrera en avvikelse i REG12 inom fem arbetsdagar när behandling av personuppgifter om anställda saknar nödvändigt underlag i REG02, REG07, REG08, REG04 eller REG06.

10.1.2 [Conditional] The Incident Response Coordinator MUST registrera misstänkt obehörig åtkomst till, utlämnande, förlust eller kompromettering av personuppgifter om anställda i REG10 inom en arbetsdag från identifiering.

10.1.3 [Controller] The Privacy Lead / PIMS Manager MUST förhindra godkännande av ny övervakning av anställda i REG12 när nödvändigt underlag i REG02, REG04 eller REG07 saknas.

10.1.4 [Both] The Vendor / Procurement Owner MUST stoppa nytt utlämnande av personuppgifter om anställda till en HR-leverantör i REG08 när nödvändigt underlag om personuppgiftsbiträde, underbiträde, instruktion eller stöd saknas.

10.1.5 [All] Top Management MUST granska upprepade avvikelser som rör anställdas integritet i REG12 när samma kategori inträffar två eller fler gånger under en rullande 12-månadersperiod.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verifiera stängningsunderlag i REG12 innan revisionsiakttagelser som rör behandling av anställdas uppgifter, meddelanden till anställda, övervakning av anställda, anställdas rättigheter eller HR-leverantörer stängs.

## 11. Granskning och underhåll

11.1.1 [All] The Privacy Lead / PIMS Manager MUST granska denna policy i REG12 minst årligen.

11.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST granska denna policy i REG12 inom 30 dagar från en väsentlig ändring av behandling av anställda, övervakning av anställda, HR-system, lönearrangemang, HRIS-leverantörer, förmånsleverantörer, leverantörer av bakgrundsscreening eller utlagda HR-tjänster.

11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST granska föreslagna väsentliga ändringar av denna policy i REG12 innan Top Management godkänner dem.

11.1.4 [All] Top Management MUST godkänna väsentliga ändringar av denna policy i REG12 innan publicering.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST uppdatera REG02, REG07 eller REG08 inom 15 arbetsdagar efter att en godkänd policyändring påverkar behandlingsposter för anställda, integritetsmeddelanden till anställda eller HR-leverantörsunderlag.

11.1.6 [All] The Internal Audit / Compliance Reviewer MUST registrera observationer om granskningens effektivitet för denna policy i REG12 under den schemalagda interna PIMS-revisionscykeln.

## 12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.4 PII03 - Policy för PII-behandlingsförteckning och rättslig grund

12.5 PII04 - Policy för integritetsmeddelanden och transparens

12.6 PII05 - Policy för hantering av samtycke och preferenser

12.7 PII06 - Policy för hantering av registrerades PII-rättigheter

12.8 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.9 PII08 - Policy för integritetsskydd genom design och som standard

12.10 PII09 - Policy för insamling, användning, utlämnande och delning av PII

12.11 PII10 - Policy för bevarande, radering och bortskaffning av PII

12.12 PII11 - Policy för korrekthet och kvalitet för PII

12.13 PII12 - Policy för integritetshantering av personuppgiftsbiträden, underbiträden och tredje parter

12.14 PII13 - Policy för internationell överföring av PII

12.15 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.16 PII15 - Policy för incident- och personuppgiftsincidenthantering avseende PII

12.17 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.18 PII17 - Policy för PIMS-dokumenterad information och underlagshantering

12.19 PII18 - Policy för PIMS-övervakning, revision och förbättring

12.20 PII21 - Policy för AI och automatiserat beslutsfattande avseende integritet, där den ingår i den valfria tilläggsreleaseomfattningen

## 13. Referensstandarder och ramverk

13.1 Denna policy är mappad till följande standarder och regelverk. Mappningen förklarar hur policyn stödjer de angivna kraven och identifierar de interna klausuler som genomför eller stödjer dem.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mappat till dokumenterat underlag för anställdas integritet, operativa godkännandegrindar, HR-personuppgiftsbiträdesregister, meddelanden till anställda, övervakningsposter, undantagshantering och genomförandeunderlag. 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** - Mappat till övervakning av anställdas integritet, mätetal, revisionsunderlag, stickprov av övervakning av anställda, hantering av avvikelser, korrigerande åtgärder och förbättring. 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** - Mappat till behandlingsändamål för anställda, koppling till rättslig grund, integritetsrisk och DPIA-

dirigering, ansvarsfördelning för gemensamt personuppgiftsansvar och behandlingsposter i REG02 och 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** - Mappat till avtal med HR-personuppgiftsbiträden, dokumenterade instruktioner, behandling av kundens personuppgifter om anställda, stöd från personuppgiftsbiträden och register över personuppgiftsbiträden i 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** - Mappat till hantering av anställdas rättigheter, rådgivning vid komplexa rättigheter och dirigering av automatiserat beslutsfattande eller behandling med hög påverkan via REG06 och 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** - Mappat till insamlingsbegränsning för anställda, godkänd intern användning, minimering, bevarandekoppling och dirigering av bevarandeundantag. 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** - Mappat till externa utlämnanden av personuppgifter om anställda, register över datadelning, godkännande av utlämnande för personuppgiftsbiträden och dirigering av incidenter relaterade till utlämnande. 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** - Mappat till skydd av integritetsposter för anställda, loggunderlag för övervakning av anställda och misstänkt missbruk eller kompromettering av övervakningsdata om anställda. 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)** - Mappat till laglig, rättvis, transparent, ändamålsbegränsad, minimerad, bevarandekopplad och ansvarsskyldig behandling av personuppgifter om anställda. 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** - Mappat till koppling till rättslig grund, dirigering av PII i särskild kategori för anställda, dirigering av företagshälsouppgifter och anställningsrelaterad känslig PII samt dirigering av uppgifter om brott eller bakgrundsscreening. 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** - Mappat till transparens för anställda, poster över integritetsmeddelanden till anställda, utlösare för meddelanden vid direkt och indirekt insamling samt underlag för övervakningsmeddelanden. 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** - Mappat till dirigering av anställdas rättigheter, underlag för begäranden, rådgivning vid komplexa begäranden och dirigering av automatiserade beslut. 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** - Mappat till styrning för personuppgiftsansvarig, ansvarsfördelning för gemensamt personuppgiftsansvar, styrning av HR-personuppgiftsbiträden, behandlingsregister, säker hantering, DPIA-dirigering och medverkan av integritetsrådgivare. 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** - Mappat till specificering av ändamål för anställda, insamlingsbegränsning, minimering, användningsbegränsning,

bevarandebegränsning och utlämnandebegränsning. 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** - Mappat till transparens, anställdas deltagande, stöd för anställdas rättigheter, ansvarsskyldighet, informationssäkerhet och underlag för efterlevnad av integritetskrav. 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** - Mappat till PII-ändamålsposter, insamlingskontroller, minimering, bevarandekoppling, utlämnandebegränsning och stöd för anställdas deltagande eller åtkomst. 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** - Mappat till PII-skyddande livscykelkontroller för personal som är relevanta för screening, villkor, koppling till tillämpning vid integritetsincidenter och granskning av bevarande vid upphörande eller ändring av anställning. 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** - Mappat till utvärdering av HR-personuppgiftsbiträden, övervakning av HR-personuppgiftsbiträden, granskning av HR-leverantörer och underlag för tjänsteförändringar i 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** - Mappat till nyttan med konsekvensbedömning avseende integritet och fastställande av HR-integritetsrisk eller DPIA-utlösare för övervakning av anställda och HR-behandling med hög påverkan utan att duplicera DPIA-metoden. 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 - Mappat till PII-skydd, screening, arbetsvillkor, ansvar efter anställningsändring och sekretessförväntningar som PII-stödjande livscykelkontroller för personal. 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 - Mappat till loggar för övervakning av anställda, övervakningsaktiviteter, ändamålsbegränsning för loggar och granskning av övervakningsunderlag. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].