

				Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII19				Tytuł dokumentu: Polityka prywatności pracowników							
Wersja: 1.0		Data wejścia w życie: 01.01.2025		Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne

Historia zmian				
Numer zmiany	Data zmiany	Zmiany	Przegląd wykonał	Właściciel procesu

Zatwierdzenia			
Imię i nazwisko	Stanowisko	Data	Podpis

<p>Nota prawna (prawa autorskie i ograniczenia użytkowania) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody. Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych. W sprawach licencjonowania prosimy o kontakt: info@clarysec.com</p>
--

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/środek kontrolny/artykuł	Stosowalność	Typ pokrycia	Komentarz
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dowody dotyczące prywatności pracowników i kontrola operacyjna
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie, niezgodności i działania korygujące
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	Cele HR, powiązanie z podstawą prawną, wyzwalacz DPIA, wspólna odpowiedzialność i rejestry
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	Umowy z podmiotami przetwarzającymi HR, polecenia, wsparcie i rejestry
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	Obowiązki pracowników, prawa i kierowanie spraw dotyczących zautomatyzowanego podejmowania decyzji
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	Powiązanie gromadzenia, przetwarzania, minimalizacji i okresu przechowywania
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	Rejestry ujawnień i obsługa ujawnień prawnie wiążących
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrona dokumentacji HR i dowody rejestrowania
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Zasady prywatności pracowników i rozliczalność

GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Zgodność z prawem, dane szczególnych kategorii i dane ze sprawdzenia przeszłości
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Przejrzystość wobec pracowników i klauzule informacyjne
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Prawa pracowników i kierowanie spraw dotyczących zautomatyzowanego podejmowania decyzji
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Nadzór, współadministratorzy, podmioty przetwarzające, rejstry, bezpieczeństwo, DPIA i doradztwo
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Cel, gromadzenie, minimalizacja, wykorzystanie, przechowywanie i ujawnianie
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Przejrzystość, uczestnictwo, rozliczalność, bezpieczeństwo i zgodność
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	Cel PII, gromadzenie, minimalizacja, przechowywanie i udział osoby, której dane dotyczą
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Środki kontrolne cyklu życia personelu chroniące PII
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Ocena, monitorowanie i kontrola zmian podmiotów przetwarzających HR

ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Ryzyko dla prywatności w HR i powiązanie z wyzwaczem DPIA
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	Ochrona PII i cykl życia bezpieczeństwa informacji dotyczący personelu
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Działania w zakresie rejestrowania i monitorowania

1. Zakres

- 1.1 Niniejsza polityka określa wymagania dotyczące prywatności pracowników w zakresie gromadzenia, wykorzystywania, ujawniania, powiązania z okresem przechowywania, informowania, obsługi praw, monitorowania, wsparcia podmiotów przetwarzających oraz zarządzania dowodami dotyczącymi PII pracowników w ramach systemu zarządzania informacjami o prywatności.
- 1.2 Na potrzeby niniejszej polityki „PII pracowników” obejmuje PII dotyczące pracowników, kandydatów do pracy, byłych pracowników, kontraktorów, personelu tymczasowego, stażystów, pracowników oddelegowanych oraz innych uczestników personelu, gdy organizacja przetwarza ich PII w celach dotyczących personelu, rekrutacji, zatrudnienia, współpracy, wynagradzania, świadczeń, bezpieczeństwa, zgodności, administracji miejsca pracy lub powiązanych celach biznesowych.
- 1.3 Niniejsza polityka ma zastosowanie do kontekstów administratora i współadministratora, w których organizacja określa cele i sposoby przetwarzania PII pracowników.
- 1.4 Niniejsza polityka ma również zastosowanie do kontekstów podmiotu przetwarzającego i podwykonawcy przetwarzania, w których organizacja przetwarza PII pracowników w imieniu klienta, nadrzędnego podmiotu przetwarzającego lub innego administratora na podstawie udokumentowanych poleceń.

1.5 Niniejsza polityka obejmuje:

- 1.5.1 gromadzenie danych pracowników;
 - 1.5.2 cele przetwarzania HR;
 - 1.5.3 klauzule informacyjne dla pracowników;
 - 1.5.4 obsługę praw pracowników;
 - 1.5.5 powiązanie z okresem przechowywania;
 - 1.5.6 monitorowanie pracowników;
 - 1.5.7 ujawnienia wewnętrzne;
 - 1.5.8 środki kontrolne dotyczące podmiotów przetwarzających HR, naliczania wynagrodzeń, HRIS, świadczeń, sprawdzenia przeszłości oraz usług HR realizowanych w outsourcingu, gdzie ma to zastosowanie;
 - 1.5.9 incydenty PII pracowników, niezgodności, działania korygujące i dowody doskonalenia.
- 1.6 Niniejsza polityka nie tworzy odrębnego rejestru prywatności HR, rejestru prywatności pracowników, rejestru przetwarzania HR, rejestru monitorowania pracowników, rejestru sprawdzenia przeszłości, rejestru dostawców HR, rejestru praw pracowników ani rejestru incydentów pracowniczych. Dowody przetwarzania dotyczącego pracowników są rejestrowane w REG02, REG04, REG06, REG07, REG08, REG10 i REG12.
- 1.7 Niniejsza polityka nie stanowi porady z zakresu prawa pracy, doradztwa dotyczącego stosunków pracy, komentarza prawnego dotyczącego rady pracowników, treści procedur dyscyplinarnych, treści procedur operacyjnych naliczania wynagrodzeń ani właściwych dla jurysdykcji wzorów dokumentów pracowniczych.

1.8 Niniejsza polityka nie powiela:

- 1.8.1 zarządzania PIMS w PII01;
- 1.8.2 rozliczalności ról w PII02;
- 1.8.3 inwentaryzacji przetwarzania i własności podstawy prawnej w PII03;
- 1.8.4 zarządzania treścią klauzul informacyjnych w PII04;
- 1.8.5 działania zgody i preferencji w PII05;
- 1.8.6 procesu obsługi praw osoby, której dane dotyczą, w PII06;

- 1.8.7 metodyki ryzyka dla prywatności i DPIA w PII07;
- 1.8.8 bramek privacy-by-design w PII08;
- 1.8.9 bazowych zasad gromadzenia, wykorzystywania, ujawniania i udostępniania w PII09;
- 1.8.10 wykonywania przechowywania, usuwania i utylizacji w PII10;
- 1.8.11 zarządzania prawidłowością i jakością w PII11;
- 1.8.12 zarządzania cyklem życia podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich w PII12;
- 1.8.13 środków kontrolnych mechanizmów transferu międzynarodowego w PII13;
- 1.8.14 wdrożenia bezpieczeństwa i kontroli dostępu w PII14;
- 1.8.15 obsługi incydentów i naruszeń w PII15;
- 1.8.16 zarządzania szkoleniami i świadomością w PII16;
- 1.8.17 kontroli udokumentowanej informacji w PII17;
- 1.8.18 zarządzania monitorowaniem, audytem i doskonaleniem PIMS w PII18;
- 1.8.19 środków kontrolnych dotyczących AI i zautomatyzowanego podejmowania decyzji w PII21, jeżeli ta opcjonalna polityka jest uwzględniona.

2. Cel

- 2.1 Celem niniejszej polityki jest zapewnienie, aby PII pracowników były przetwarzane wyłącznie w udokumentowanych, zatwierdzonych, przejrzystych, proporcjonalnych i rozliczalnych celach dotyczących personelu oraz aby dowody dotyczące prywatności pracowników były utrzymywane w kanonicznych rejestrach PIMS bez tworzenia odrębnej warstwy dowodowej prywatności HR.
- 2.2 Niniejsza polityka wspiera spójną obsługę przetwarzania dotyczącego pracowników przez powiązanie czynności przetwarzania pracowników z REG02, klauzul informacyjnych dla pracowników z REG07, wniosków o realizację praw pracowników z REG06, ryzyka dla prywatności HR i wyzwalaczy DPIA z REG04, podmiotów przetwarzających HR oraz dostawców naliczania wynagrodzeń lub HRIS z REG08, incydentów PII pracowników z REG10, a także wyjątków, niezgodności, działań korygujących i dowodów monitorowania z REG12.

3. Cele szczegółowe

3.1 Celami niniejszej polityki są:

- 3.1.1 utrzymywanie dowodów inwentaryzacji przetwarzania dotyczącego pracowników w REG02;
- 3.1.2 dokumentowanie źródeł gromadzenia danych pracowników, kategorii PII, celów, systemów, odbiorców i powiązania z okresem przechowywania;
- 3.1.3 utrzymywanie dowodów klauzul informacyjnych dla pracowników w REG07;
- 3.1.4 kierowanie ryzyka dla prywatności pracowników i wyzwalaczy DPIA przez REG04;
- 3.1.5 kierowanie wniosków o realizację praw pracowników przez REG06;
- 3.1.6 utrzymywanie dowodów dotyczących podmiotów przetwarzających HR, naliczania wynagrodzeń, HRIS, świadczeń, sprawdzenia przeszłości i usług HR realizowanych w outsourcingu w REG08;
- 3.1.7 zapewnienie, aby monitorowanie pracowników było udokumentowane, proporcjonalne, przeglądane i eskalowane przez REG04 oraz REG12, gdzie ma to zastosowanie;
- 3.1.8 kierowanie podejrzewanych incydentów PII pracowników przez REG10;
- 3.1.9 rejestrowanie wyjątków dotyczących prywatności pracowników, niezgodności, działań korygujących i działań doskonalących w REG12;
- 3.1.10 unikanie porad z zakresu prawa pracy i komentarzy prawnych dotyczących rad pracowników w klauzulach operacyjnych;

3.1.11 unikanie duplikowania rejestrów, ról, formularzy, pulpitów lub obiektów dowodowych właściwych dla HR.

4. Postanowienia polityki

4.1 Inwentaryzacja przetwarzania dotyczącego pracowników i cele przetwarzania HR

4.1.1 [Controller] The Process Owner / Business Owner MUSI zarejestrować każdą czynność przetwarzania dotyczącą pracowników w REG02, zanim PII pracowników zostaną zebrane, wygenerowane, zaimportowane, wykorzystane lub ujawnione.

4.1.2 [Controller] The Process Owner / Business Owner MUSI udokumentować kategorie PII pracowników, populację pracowników, źródło gromadzenia, cel przetwarzania, system, kategorię odbiorców wewnętrznych, kategorię odbiorców zewnętrznych oraz powiązanie z okresem przechowywania w REG02, zanim czynność przetwarzania zostanie zatwierdzona.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUSI przejrzeć każdą nową lub istotnie zmienioną czynność przetwarzania dotyczącą pracowników w REG02, zanim czynność przetwarzania zostanie zatwierdzona do działania.

4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUSI zarejestrować poradę dotyczącą prywatności w REG04 przed zatwierdzeniem przetwarzania dotyczącego pracowników obejmującego PII szczególnych kategorii, dane dotyczące przestępstw, sprawdzenie przeszłości, dane z zakresu medycyny pracy, dane biometryczne, dane lokalizacyjne, monitorowanie pracowników lub przetwarzanie, które może istotnie wpłynąć na pracownika.

4.1.5 [Processor] The Privacy Lead / PIMS Manager MUSI zarejestrować polecenie klienta, cel usługi, kategorie PII pracowników klienta oraz powiązanie z rolą podmiotu przetwarzającego w REG08 przed przetwarzaniem PII pracowników klienta jako usługi HR realizowanej w outsourcingu, naliczania wynagrodzeń, świadczeń, HRIS, sprawdzania lub wsparcia personelu.

4.1.6 [Joint Controller] The Privacy Lead / PIMS Manager MUSI zarejestrować podział odpowiedzialności współadministratorów za przetwarzanie PII pracowników w REG08, zanim wspólna czynność przetwarzania dotycząca pracowników się rozpocznie.

4.2 Gromadzenie danych pracowników i klauzule informacyjne dla pracowników

4.2.1 [Controller] The Process Owner / Business Owner MUSI ograniczyć gromadzenie PII pracowników do kategorii udokumentowanych w REG02, zanim rozpocznie się gromadzenie w ramach rekrutacji, onboarding, administracji zatrudnienia, administracji świadczeń, naliczania wynagrodzeń, sprawdzania, monitorowania lub offboarding.

4.2.2 [Controller] The Process Owner / Business Owner MUSI zarejestrować źródło PII pracowników zebranych od stron trzecich w REG02, zanim źródło gromadzenia od strony trzeciej zostanie wykorzystane.

4.2.3 [Controller] The Privacy Lead / PIMS Manager MUSI utrzymywać zapis klauzuli informacyjnej dla pracowników w REG07, zanim PII pracowników zostaną zebrane bezpośrednio lub pośrednio dla nowego lub istotnie zmienionego celu.

4.2.4 [Controller] The Process Owner / Business Owner MUSI potwierdzić, że aktualna klauzula informacyjna dla pracowników zarejestrowana w REG07 jest dostępna przed gromadzeniem w ramach rekrutacji, gromadzeniem w ramach onboarding, aktywacją monitorowania, zapisaniem do świadczeń, sprawdzeniem przeszłości lub istotną zmianą przetwarzania dotyczącego pracowników.

4.2.5 [Conditional] The Data Protection Officer / Privacy Advisor MUSI przejrzeć zapis klauzuli informacyjnej dla pracowników w REG07 przed publikacją, gdy klauzula obejmuje monitorowanie pracowników, sprawdzenie przeszłości, PII szczególnych kategorii, dane

dotyczące przestępstw, zautomatyzowane podejmowanie decyzji lub istotnie zmieniony cel przetwarzania dotyczącego pracowników.

- 4.2.6 [Processor] The Vendor / Procurement Owner MUSI zarejestrować odpowiedzialności dotyczące kanałów gromadzenia skierowanych do pracowników w REG08, zanim obsługiwana przez podmiot przetwarzający usługa HR, naliczania wynagrodzeń, HRIS, świadczeń, sprawdzania lub usługa HR realizowana w outsourcingu zacznie gromadzić PII pracowników w imieniu klienta.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wyjątki

- 9.1.1 [All] The Process Owner / Business Owner MUSI zarejestrować wnioski o wyjątek w REG12 przed odstąpieniem od dowolnego wymagania niniejszej polityki.
- 9.1.2 [Conditional] The Data Protection Officer / Privacy Advisor MUSI zarejestrować poradę w REG12 przed zatwierdzeniem wyjątku wpływającego na monitorowanie pracowników, obsługę praw pracowników, sprawdzenie przeszłości, PII szczególnych kategorii, dane dotyczące przestępstw lub przetwarzanie dotyczące pracowników o istotnym wpływie.
- 9.1.3 [Conditional] Top Management MUSI zatwierdzić wyjątki dotyczące prywatności pracowników w REG12 przed aktywacją, gdy wyjątek wpływa na przetwarzanie wysokiego ryzyka dotyczące pracowników, monitorowanie pracowników, ujawnienie zewnętrzne, poleganie na podmiocie przetwarzającym lub nierozwiązane działanie korygujące.
- 9.1.4 [All] The Privacy Lead / PIMS Manager MUSI przypisać każdemu wyjątkowi dotyczącemu prywatności pracowników w REG12 datę wygaśnięcia nieprzekraczającą 90 dni przed aktywacją wyjątku.
- 9.1.5 [All] The Privacy Lead / PIMS Manager MUSI przejrzeć każdy wyjątek dotyczący prywatności pracowników w REG12 w ciągu pięciu dni roboczych przed wygaśnięciem.
- 9.1.6 [All] The Privacy Lead / PIMS Manager MUSI zamknąć lub eskalować każdy wygasły wyjątek dotyczący prywatności pracowników w REG12 w ciągu pięciu dni roboczych po wygaśnięciu.

10. Egzekwowanie postanowień

- 10.1.1 [All] The Privacy Lead / PIMS Manager MUSI zarejestrować niezgodność w REG12 w ciągu pięciu dni roboczych, gdy przetwarzaniu PII pracowników brakuje wymaganych dowodów w REG02, REG07, REG08, REG04 lub REG06.
- 10.1.2 [Conditional] The Incident Response Coordinator MUSI zarejestrować podejrzewany nieuprawniony dostęp do PII pracowników, ujawnienie, utratę lub naruszenie bezpieczeństwa w REG10 w ciągu jednego dnia roboczego od identyfikacji.
- 10.1.3 [Controller] The Privacy Lead / PIMS Manager MUSI uniemożliwić zatwierdzenie nowego monitorowania pracowników w REG12, gdy brakuje wymaganych dowodów w REG02, REG04 lub REG07.
- 10.1.4 [Both] The Vendor / Procurement Owner MUSI wstrzymać nowe ujawnienie PII pracowników dostawcy HR w REG08, gdy brakuje wymaganych dowodów dotyczących podmiotu przetwarzającego, podwykonawcy przetwarzania, polecenia lub wsparcia.
- 10.1.5 [All] Top Management MUSI przejrzeć powtarzające się niezgodności dotyczące prywatności pracowników w REG12, gdy ta sama kategoria wystąpi dwa lub więcej razy w krotzącym okresie 12 miesięcy.
- 10.1.6 [All] The Internal Audit / Compliance Reviewer MUSI zweryfikować dowody zamknięcia w REG12 przed zamknięciem ustaleń audytowych dotyczących przetwarzania związanego z

prywatnością pracowników, klauzul informacyjnych dla pracowników, monitorowania pracowników, praw pracowników lub dostawców HR.

11. Przegląd i utrzymanie

- 11.1.1 [All] The Privacy Lead / PIMS Manager MUSI przeglądać niniejszą politykę w REG12 co najmniej raz w roku.
- 11.1.2 [Conditional] The Privacy Lead / PIMS Manager MUSI przejrzeć niniejszą politykę w REG12 w ciągu 30 dni od istotnej zmiany przetwarzania dotyczącego pracowników, monitorowania pracowników, systemów HR, uzgodnień dotyczących naliczania wynagrodzeń, dostawców HRIS, dostawców świadczeń, dostawców sprawdzenia przeszłości lub usług HR realizowanych w outsourcingu.
- 11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUSI przejrzeć proponowane istotne zmiany niniejszej polityki w REG12 przed zatwierdzeniem przez Top Management.
- 11.1.4 [All] Top Management MUSI zatwierdzić istotne zmiany niniejszej polityki w REG12 przed publikacją.
- 11.1.5 [All] The Privacy Lead / PIMS Manager MUSI zaktualizować REG02, REG07 lub REG08 w ciągu 15 dni roboczych po zatwierdzonej zmianie polityki, jeżeli wpływa ona na zapisy przetwarzania dotyczącego pracowników, klauzule informacyjne dla pracowników lub dowody dotyczące dostawców HR.
- 11.1.6 [All] The Internal Audit / Compliance Reviewer MUSI rejestrować obserwacje dotyczące skuteczności przeglądu niniejszej polityki w REG12 podczas zaplanowanego cyklu audytu wewnętrznego PIMS.

12. Powiązane polityki

- 12.1 Niniejsza polityka jest wspierana przez następujące powiązane polityki:
- 12.2 PII01 - Polityka systemu zarządzania informacjami o prywatności
- 12.3 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności
- 12.4 PII03 - Polityka inwentaryzacji przetwarzania PII i podstawy prawnej
- 12.5 PII04 - Polityka klauzul informacyjnych i przejrzystości
- 12.6 PII05 - Polityka zarządzania zgodą i preferencjami
- 12.7 PII06 - Polityka zarządzania prawami osoby, której dane dotyczą
- 12.8 PII07 - Polityka oceny ryzyka dla prywatności i DPIA
- 12.9 PII08 - Polityka privacy by design i privacy by default
- 12.10 PII09 - Polityka gromadzenia, wykorzystywania, ujawniania i udostępniania PII
- 12.11 PII10 - Polityka przechowywania, usuwania i utylizacji PII
- 12.12 PII11 - Polityka prawidłowości i jakości PII
- 12.13 PII12 - Polityka zarządzania prywatnością podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich
- 12.14 PII13 - Polityka międzynarodowego transferu PII
- 12.15 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu
- 12.16 PII15 - Polityka zarządzania incydentami i naruszeniami PII
- 12.17 PII16 - Polityka szkoleń, świadomości i kompetencji w zakresie prywatności
- 12.18 PII17 - Polityka zarządzania udokumentowaną informacją i dowodami PIMS
- 12.19 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS
- 12.20 PII21 - Polityka prywatności dotycząca AI i zautomatyzowanego podejmowania decyzji, jeżeli jest uwzględniona w zakresie opcjonalnego wydania dodatkowego

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest zmapowana do następujących norm i regulacji. Mapowanie wyjaśnia, w jaki sposób polityka wspiera przywołane wymagania, oraz wskazuje klauzule wewnętrzne, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Zmapowano do udokumentowanych dowodów dotyczących prywatności pracowników, bramek zatwierdzenia operacyjnego, zapisów podmiotów przetwarzających HR, klauzul informacyjnych dla pracowników, zapisów monitorowania, obsługi wyjątków i dowodów wdrożenia. 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** - Zmapowano do monitorowania prywatności pracowników, metryk, dowodów audytowych, próbkowania monitorowania pracowników, obsługi niezgodności, działań korygujących i doskonalenia. 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** - Zmapowano do celów przetwarzania dotyczącego pracowników, powiązania z podstawą prawną, ścieżki ryzyka dla prywatności i DPIA, podziału odpowiedzialności współadministratorów oraz zapisów przetwarzania w 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** - Zmapowano do umów z podmiotami przetwarzającymi HR, udokumentowanych poleceń, przetwarzania PII pracowników klienta, wsparcia podmiotu przetwarzającego i zapisów podmiotu przetwarzającego w 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** - Zmapowano do obsługi praw pracowników, doradztwa w złożonej obsłudze praw oraz kierowania spraw dotyczących zautomatyzowanego podejmowania decyzji lub przetwarzania o istotnym wpływie przez 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** - Zmapowano do ograniczenia gromadzenia danych pracowników, zatwierdzonego wykorzystania wewnętrznego, minimalizacji, powiązania z okresem przechowywania i kierowania wyjątków dotyczących okresu przechowywania. 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** - Zmapowano do zewnętrznych ujawnień PII pracowników, zapisów udostępniania danych, autoryzacji ujawnienia przez podmiot przetwarzający i ścieżki incydentów związanych z ujawnieniem. 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** - Zmapowano do ochrony zapisów dotyczących prywatności pracowników, dowodów logów monitorowania pracowników oraz podejrzanego nadużycia lub naruszenia bezpieczeństwa danych z monitorowania pracowników. 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)** - Zmapowano do zgodnego z prawem, rzetelnego, przejrzystego, ograniczonego celem, zminimalizowanego, powiązanego z okresem przechowywania i rozliczalnego przetwarzania PII pracowników. 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** - Zmapowano do powiązania z podstawą prawną, ścieżki PII pracowników szczególnych kategorii, ścieżki wrażliwych PII dotyczących medycyny pracy i zatrudnienia oraz ścieżki danych dotyczących przestępstw lub sprawdzenia przeszłości. 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** - Zmapowano do przejrzystości wobec pracowników, zapisów klauzul informacyjnych dla pracowników, wyzwalaczy informowania przy gromadzeniu bezpośrednim i pośrednim oraz dowodów informowania o monitorowaniu. 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** - Zmapowano do kierowania praw pracowników, dowodów wniosków, doradztwa w sprawach złożonych wniosków i ścieżki zautomatyzowanego podejmowania decyzji. 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** - Zmapowano do zarządzania przez administratora, podziału odpowiedzialności współadministratorów, zarządzania podmiotami przetwarzającymi HR, zapisów przetwarzania, bezpiecznej obsługi, ścieżki DPIA i udziału doradztwa w zakresie prywatności. 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** - Zmapowano do określenia celu dotyczącego pracowników, ograniczenia gromadzenia, minimalizacji, ograniczenia wykorzystania, ograniczenia przechowywania i ograniczenia ujawniania. 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** - Zmapowano do przejrzystości, udziału pracowników, wsparcia praw pracowników, rozliczalności, bezpieczeństwa informacji i dowodów zgodności w zakresie prywatności. 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** - Zmapowano do zapisów celów PII, środków kontrolnych gromadzenia, minimalizacji, powiązania z okresem przechowywania, ograniczenia ujawniania oraz wsparcia udziału lub dostępu pracowników. 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** - Zmapowano do środków kontrolnych cyklu życia personelu chroniących PII, istotnych dla sprawdzania, warunków, powiązania egzekwowania naruszeń prywatności oraz przeglądu okresu przechowywania przy zakończeniu lub zmianie zatrudnienia. 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** - Zmapowano do oceny podmiotów przetwarzających HR, monitorowania podmiotów przetwarzających HR, przeglądu dostawców HR i dowodów zmiany usługi w 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** - Zmapowano do korzyści z oceny skutków dla prywatności oraz ustalenia ryzyka dla prywatności HR lub wyzwalacza DPIA dla monitorowania pracowników i przetwarzania HR o istotnym wpływie bez powielania metody 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 - Zmapowano do ochrony PII, sprawdzania, warunków dotyczących personelu, odpowiedzialności po zmianie zatrudnienia i oczekiwań poufności jako środków kontrolnych cyklu życia personelu wspierających 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 - Zmapowano do logów monitorowania pracowników, działań monitorujących, ograniczenia celu logów i przeglądu dowodów monitorowania. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].