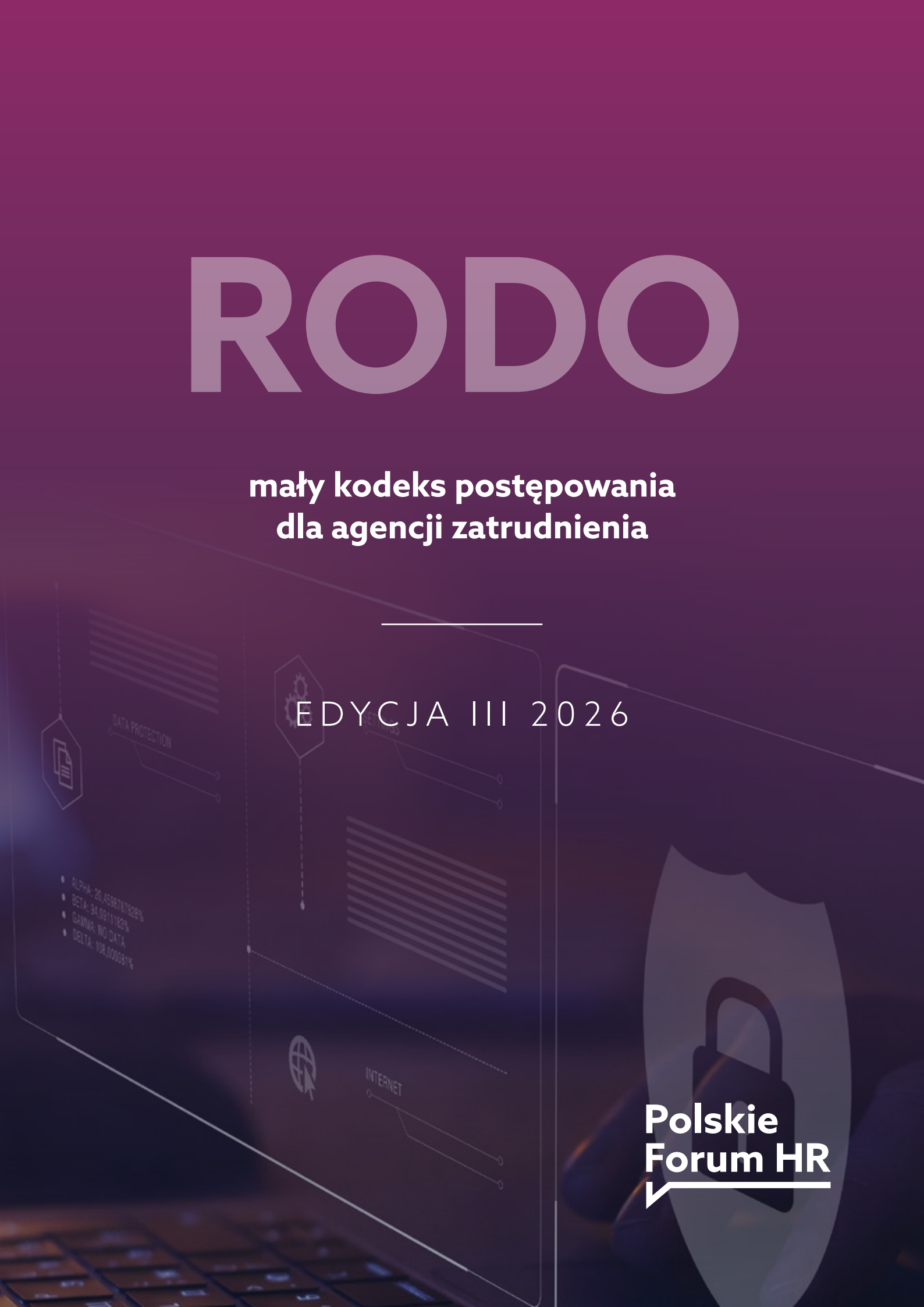
RODO

mały kodeks postępowania dla agencji zatrudnienia

EDYCJA III 2026



Polskie Forum HR

Polskie Forum HR

RODO

mały kodeks postępowania dla agencji zatrudnienia

EDYCJA III 2026

Redakcja:

r. pr. Liliana Strupp, CIPP/E

Autorzy opracowania:

Katarzyna Białożyt
Małgorzata Brańska, CISA, CIPP/E
r. pr. Anna Czubak
Adam Kop
adw. Karolina Kot
Bartosz Kozak
Ewelina Książkiewicz
Monika Kwiatkowska
Michał Madecki
Zuzanna Spaltenstein-Kotas
r. pr. Liliana Strupp, CIPP/E
r. pr. Aleksandra Wójcicka
r. pr. Iwona Wypart

Pierwsza edycja: RODO mały kodeks postępowania, 2018,
redakcja: r. pr. Liliana Strupp,

autorzy opracowania:
Barbara Drabich, Paweł Olejniczak, r. pr. Małgorzata Sitkiewicz,
r. pr. Piotr Stolarczyk, r. pr. Liliana Strupp, r. pr. dr Małgorzata Wilińska

Druga edycja: RODO mały kodeks postępowania, 2021,
redakcja: r. pr. Liliana Strupp,

autorzy opracowania:
Małgorzata Brańska, CISA, CIPP/E,
r. pr. Dominika Domiańska-Drzazga, Przemysław Frańczak,
r. pr. Olga Gierada-Jabłonka, apl. adw. Karolina Kot, Anna Prokulska,
apl. adw. Marzena Przeworska, r. pr. Piotr Stolarczyk, r. pr. Liliana Strupp

RODO

mały kodeks postępowania dla agencji zatrudnienia

EDYCJA III 2026

Spis treści

ROZDZIAŁ I
Podstawy prawne przetwarzania danych osobowych przez agencje zatrudnienia **4**

ROZDZIAŁ II
Prawa osób, których dane dotyczą **8**

ROZDZIAŁ III
Usługi agencji zatrudnienia **15**
Usługi rekrutacyjne 18
Praca tymczasowa 25
Delegowanie pracowników do pracy za granicą w ramach świadczenia usług 30
Legalizacja zatrudnienia obywateli państw trzecich 31
Referencje 32
Testy w rekrutacji 32

ROZDZIAŁ IV
Główne obowiązki administratora danych **35**

ROZDZIAŁ V
AI w działalności agencji zatrudnienia i podmiotów HR **39**

ROZDZIAŁ VI
Sankcje **47**

ROZDZIAŁ VII
Suplement **48**
Wybrane techniczne i organizacyjne środki zabezpieczeń danych osobowych

Podstawy prawne przetwarzania danych osobowych przez agencje zatrudnienia

Działalność agencji zatrudnienia uregulowana jest w Ustawie z dnia 20 marca 2025 r. o rynku pracy i służbach zatrudnienia[1] (dalej: „ustawa"). Zgodnie z art. 305 ust. 1 tej ustawy agencjami zatrudnienia są podmioty wpisane do rejestru agencji zatrudnienia, świadczące usługi w zakresie pośrednictwa pracy oraz pracy tymczasowej. Usługi pośrednictwa pracy polegają – zgodnie z ustawą – na udzielaniu pomocy w uzyskaniu zatrudnienia lub innej pracy zarobkowej bezrobotnym, poszukującym pracy i osobom niezarejestrowanym (w tym biernym zawodowo), a także na udzielaniu pracodawcom pomocy w pozyskiwaniu kandydatów do pracy. Są one realizowane m.in. przez: pozyskiwanie i upowszechnianie ofert pracy, udzielanie pracodawcom informacji o kandydatach do pracy oraz inicjowanie i organizowanie kontaktów pracodawców z osobami poszukującymi pracy. Z kolei usługa pracy tymczasowej polega na zatrudnianiu pracowników i kierowaniu tych pracowników oraz osób niebędących pracownikami do wykonywania pracy tymczasowej na rzecz i pod kierownictwem pracodawcy użytkownika, na zasadach określonych w przepisach o zatrudnianiu pracowników tymczasowych.

Już z samych definicji legalnych zawartych ustawie wynika, że działalność agencji zatrudnienia opiera się w głównej mierze na przetwarzaniu danych osobowych kandydatów i pracowników. Aby procesy rekrutacyjne oraz zatrudnianie przebiegały zgodnie z prawem, każda operacja dokonywana z udziałem danych osobowych musi być oparta na jednej z przesłanek legalizujących, wskazanych w art. 6 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO"). Poniżej omówiono kluczowe podstawy prawne, które mają najczęstsze zastosowanie w codziennej działalności agencji zatrudnienia.

Przetwarzanie w celu wypełnienia obowiązku prawnego (art. 6 ust. 1 lit. c RODO)

Działając na podstawie ustawy, agencje zatrudnienia realizują szereg obowiązków związanych z funkcjonowaniem rynku pracy, co wiąże się z obowiązkami nałożonymi na nie z mocy prawa. Z tego względu w wielu przypadkach podstawą przetwarzania danych będzie konieczność wypełnienia prawnego obowiązku ciążącego na administratorze (art. 6 ust. 1 lit. c RODO w zw. z odpowiednim przepisem ustawy). Przykładowo, ustawa nakłada na agencje zatrudnienia realizację zadań państwa w zakresie aktywności zawodowej i rynku pracy, więc przetwarzanie danych w tym celu będzie wykonywane na podstawie art. 6 ust. 1 lit. c RODO w zw. z art. 5 ustawy. Kolejne przykłady to: obowiązek współpracy z organami zatrudnienia (art. 320 ustawy) czy obowiązki sprawozdawcze wobec marszałka województwa (art. 323 ustawy).

W przypadku zatrudniania pracowników tymczasowych agencja zatrudnienia staje się ich bezpośrednim pracodawcą, a zatem także administrato-

1 Dz.U. z 2025 r. poz. 620

rem danych osobowych przetwarzanych do celu nawiązania, realizacji lub ustania stosunku pracy. W związku z tym agencja przetwarza dane osobowe pracowników tymczasowych na podstawie art. 6 ust. 1 lit. c RODO w celu wypełnienia licznych obowiązków prawnych wynikających z przepisów prawa pracy, przepisów o zatrudnianiu cudzoziemców lub przepisów o ubezpieczeniach społecznych. Do takich obowiązków należą m.in.: zgłoszenie do ubezpieczeń społecznych, obliczanie wynagrodzenia, prowadzenie dokumentacji pracowniczej (w tym z zakresu medycyny pracy, BHP i dokumentacji wypadkowej) oraz gromadzenie dokumentacji niezbędnej do legalizacji zatrudnienia cudzoziemców.

Działanie w celu zawarcia i wykonania umowy (art. 6 ust. 1 lit. b RODO)

Podstawą prawną, wokół której ogniskuje się większość usług rekrutacyjnych (w ustawie określonych jako usługi pośrednictwa pracy), jest art. 6 ust. 1 lit. b RODO. Przepis ten legalizuje przetwarzanie danych, które jest niezbędne do wykonania umowy lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed jej zawarciem. Z uwagi na to, że głównym celem usług rekrutacyjnych jest dopasowanie umiejętności kandydata do potrzeb przyszłego pracodawcy oraz jak najszybsze znalezienie mu zatrudnienia, zachodzi bezpośredni związek przyczynowy między działaniami podejmowanymi w procesie rekrutacyjnym a zawarciem umowy. Kiedy kandydat zgłasza się do agencji (bezpośrednio w odpowiedzi na konkretne ogłoszenie lub podając swoje dane do bazy danych kandydatów), to działania agencji, takie jak tworzenie profilu zawodowego kandydata, weryfikacja kompetencji czy bezpośrednie zbieranie informacji podczas wywiadów rekrutacyjnych, stanowią z prawnego punktu widzenia działania przedumowne. Zmierzają one do zawarcia umowy z potencjalnym pracodawcą, którym może być sama agencja (w usłudze pracy tymczasowej) albo inny podmiot (w usłudze pośrednictwa pracy).

> Co niezwykle istotne, do podjęcia tych podstawowych kroków rekrutacyjnych wymóg uzyskania formalnej zgody kandydata nie ma zastosowania. Należy przyjąć, że samo przekazanie CV, zarejestrowanie się w bazie kandydatów czy odpowiedź na konkretne ogłoszenie o pracę jest wyraźnym sygnałem chęci zawarcia umowy w bliskiej lub dalszej przyszłości.

W ramach art. 6 ust. 1 lit. b RODO należy również wyodrębnić sytuację, w której agencja zatrudnienia nie ogranicza się do działań reaktywnych (aplikacja samego kandydata w odpowiedzi na ogłoszenie o pracę), ale proaktywnie proponuje rozwiązania systemowe, umożliwiające zawarcie z kandydatem umowy o świadczenie usług rekrutacyjnych drogą elektroniczną. Mechanizm świadczenia takiej usługi polega na tym, że kandydat na stronie internetowej agencji zakłada indywidualne konto, akceptuje regulamin świadczenia usług oraz zapoznaje się zintegrowaną z nim polityką prywatności. Z momentem zatwierdzenia tych dokumentów dochodzi do zawarcia umowy cywilnoprawnej pomiędzy kandydatem (użytkownikiem konta) a agencją. Regulamin, który akceptuje kandydat, precyzuje kluczowe aspekty świadczenia usług rekrutacyjnych, w szczególności: uprawnienia w zakresie zarządzania profilem (możliwość edycji profilu, aktualizacji danych, prawo do usunięcia konta, uprawnienie do zarządzania historią aplikacji rekrutacyjnych itp.), opis usług (np. automatyczne dopasowywania kompetencji do nowych ofert pracy, wysyłanie powiadomień o ofertach pracy spełniających kryteria kandydata bezpośrednio na jego adres e-mail lub telefon) oraz jasny cel przetwarzania danych znajdujących

się w profilu użytkownika konta (realizacja usługi rekrutacyjnej). Powyższe rozwiązanie pozwala na przetwarzanie danych w sposób ciągły (do czasu rozwiązania umowy lub usunięcia konta), bez konieczności uzyskiwania akceptacji kandydata na prezentację każdej kolejnej oferty pracy.

Prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO)

Poza wypełnianiem obowiązków prawnych i realizacją umów agencja zatrudnienia może opierać przetwarzanie danych osobowych w wybranych procesach także na przesłance uzasadnionego interesu (art. 6 ust. 1 lit f RODO). Podstawa ta znajduje zastosowanie w sytuacjach, gdy interes agencji (jako podmiotu prowadzącego działalność w zakresie pośrednictwa pracy) jest nadrzędny wobec standardowej ochrony prywatności, przynależnej kandydatom do pracy. Przykładem jest weryfikacja kompetencji za pomocą testów: kompetencyjnych, predyspozycji, osobowości. Testy te służą sprawdzeniu umiejętności twardych (np. znajomość języków, testy logiczne), co jest niezbędne do rzetelnej oceny przydatności kandydata na danym stanowisku, jak również miękkich, pozwalających ocenić szczególne predyspozycje wymagane na danym stanowisku pracy (np. przywódcze na stanowisku menedżerskim). Przetwarzanie wyników tych testów na podstawie art. 6 ust. 1 lit. f RODO uzasadnia się potrzebą zapewnienia wysokiej jakości usług pośrednictwa pracy i minimalizacją ryzyka nietrafionej rekrutacji.

Uzasadnienie wykorzystania testów kompetencji znajduje także pośrednie umocowanie w art. 22^1 Kodeksu pracy, który definiuje zakres danych, jakich pracodawca ma prawo żądać od kandydata. Art. 22^1 § 1 pkt 5 i 6 Kodeksu pracy stanowią, że pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie danych osobowych obejmujących m.in. wykształcenie, kwalifikacje zawodowe oraz przebieg dotychczasowego zatrudnienia. Wiarygodne, certyfikowane testy kompetencji (np. językowe, techniczne czy analityczne) są niewątpliwie narzędziem służącym potwierdzeniu tych informacji. Skoro ustawodawca przyznaje pracodawcy prawo do uzyskania informacji o wykształceniu i kwalifikacjach kandydata, to agencja zatrudnienia ma uzasadniony interes w tym, aby za pomocą obiektywnych narzędzi (takich jak testy) zweryfikować prawdziwość i poziom tych kwalifikacji jeszcze przed podjęciem decyzji o rekomendacji kandydata.

Art. 6 ust. 1 lit. f RODO stanowi dla agencji zatrudnienia także podstawę prawną do przetwarzania danych w celu: badania satysfakcji kandydatów i jakości usług, obrony przed potencjalnymi roszczeniami po zakończeniu procesu rekrutacyjnego oraz prowadzenia analityki procesów rekrutacyjnych na potrzeby biznesowe agencji. Wykorzystując tę podstawę przetwarzania danych należy jednak zawsze pamiętać o konieczności przeprowadzenia testu równowagi, aby upewnić się, że cele, dla których agencja zatrudnienia chce przetwarzać dane w oparciu o tę podstawę są rzeczywiście nadrzędne wobec praw i wolności kandydatów.

Koncepcja zgody kandydata na przetwarzanie danych (art. 6 ust. 1 lit. a RODO)

Zgoda na przetwarzanie danych (art. 6 ust. 1 lit. a RODO) bywa często nadużywana w procesach HR jako zabezpieczenie „na wszelki wypadek". W rzeczywistości jej zastosowanie powinno mieć charakter posiłkowy i dotyczyć wyłącznie sytuacji wykraczających poza standardowy proces rekrutacji i weryfikacji przedumownej. Zgoda ta musi być zawsze dobrowolna, świadoma oraz musi istnieć możliwość jej łatwego wycofania. Powinna być rezerwowana wyłącznie dla tych operacji, które

nie wynikają ze ścisłych obowiązków ustawowych ani z działań niezbędnych do zawarcia umowy, np. gdy agencja chce zebrać o kandydacie informacje dodatkowe, które nie są kluczowe i niezbędne do samego zatrudnienia, ale mogą pomóc w lepszej rekomendacji jego kandydatury.

Przykładem jest sytuacja, w której rekruter chce skontaktować się z poprzednim pracodawcą kandydata w celu sprawdzenia jego referencji zawodowych i ewentualnego przekazania tych ustaleń nowemu pracodawcy. Zbieranie informacji od podmiotów trzecich głębiej wkracza w prywatność kandydata, dlatego agencja może podjąć taki krok wyłącznie pod warunkiem uzyskania od niego uprzedniej, w pełni dobrowolnej i wyraźnej zgody. Wyraźnej zgody wymaga również pozyskiwanie i wykorzystywanie danych kandydatów z mediów społecznościowych w celu oceny ich profilu zawodowego. Podobna sytuacja zachodzi wtedy, gdy dane wcześniej zebrane w jednym celu miałyby być wykorzystane do jakiegokolwiek innego celu niż ten, o którym kandydat został poinformowany na początku procesu rekrutacji, a brak jest innej, silniejszej podstawy prawnej do przetwarzania jego danych.

Prawidłowe przyporządkowanie podstaw prawnych z RODO jest fundamentem legalnego działania agencji zatrudnienia. Rzetelne opieranie się na prawnym obowiązku (art. 6 ust. 1 lit. c RODO) w relacjach z organami państwa, stosowanie przesłanki działań przedumownych (art. 6 ust. 1 lit. b RODO) przy podstawowych operacjach rekrutacyjnych oraz świadome zawężenie stosowania uzasadnionego interesu (art. 6 ust. 1 lit. f RODO) i zgody (art. 6 ust. 1 lit. a RODO), gwarantują zgodność z zasadami ochrony prywatności.

Prawa osób, których dane dotyczą

Osoba, której dane dotyczą, może żądać od agencji zatrudnienia realizacji wszystkich przysługujących jej praw, które zostały wymienione w niniejszym rozdziale.

Prawo do informacji – art. 12 – 14 RODO

Administrator danych jest obowiązany udzielać osobie żądającej informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Osoba, której dane dotyczą, ma prawo oczekiwać informacji m. in. o tożsamości administratora, celach i podstawie prawnej przetwarzania, a także o możliwości wycofania zgody udzielonej na przetwarzanie danych. Informacji z art. 13 i 14 RODO można udzielać „warstwowo". Jest to odejście od konieczności umieszczania całej, obszernej informacji w jednym miejscu. Konstrukcja warstwowa (ang. layered approach) jest zalecanym podejściem, ponieważ pozwala administratorowi wywiązać się z formalnego obowiązku informacyjnego, jednocześnie dbając o komfort i faktyczne zrozumienie treści przez osobę, której dane dotyczą.

Na czym polega warstwowe udzielanie informacji?

Warstwowy obowiązek informacyjny dzieli przekaz na dwie lub więcej sekcji, w których:

1. pierwsza warstwa to najważniejsze informacje:

- jest to komunikat krótki i natychmiast dostępny (np. pod linkiem, pod ikoną informacyjną, w widocznym miejscu formularza);
- obejmuje kluczowe dane, w tym m.in. tożsamość administratora oraz główne cele przetwarzania danych;

2. druga warstwa to pełny zakres informacji, np. pełna Polityka Prywatności:

- zawiera informacje, których brakowało w warstwie pierwszej, w tym katalog praw przysługujących osobom fizycznym, podstawy prawne dla wszystkich celów przetwarzania, okresy retencji, informacje o odbiorcach danych, oraz wszelkie inne prawnie wymagane elementy;
- dostęp do tej warstwy jest realizowany poprzez odesłanie (np. hiperłącze) z pierwszej warstwy.

Należy pamiętać, że obowiązki informacyjne z art. 13 i 14 RODO są spełniane przez agencję i pracodawcę użytkownika we własnym zakresie, ponieważ każdy administrator danych odpowiada za spełnienie swoich obowiązków wynikających z przepisów prawa. Klauzule informacyjne powinny m.in. uwzględniać wszystkie cele przetwarzania danych osobowych, w tym także cele związane z audytami.

W agencjach zatrudnienia, które korzystają z baz danych i systemów wspierających rekrutację na zasadzie „wyszukiwarki" (poprzez wprowadzenie odpowiednich kryteriów wyszukiwania tzw. tagów, uzyskuje się zbiór kandydatów spełniających wpisane kryteria), nie mamy do czynienia z tzw. profilowaniem kwalifikowanym (o którym mowa w art. 22 RODO), wymagającym uzyskania wyraźnej zgody kandydata, ponieważ korzystanie z systemów baz danych kandydatów jest co do zasady

elementem współistniejącym z czynnikiem ludzkim, a decyzja, który kandydat zostanie zarekomendowany klientowi lub który pracownik zostanie zatrudniony w celu skierowania go do klienta, jest podejmowana przez człowieka. W większości prowadzonych procesów rekrutacji pracownik agencji bierze w nich aktywny udział, korzystając np. z przygotowanych przez sztuczną inteligencję podsumowań czy rekomendacji. Jednak ostateczna decyzja o rekomendacji zawsze należy do konsultanta agencji. Agencja, która zamierza poddawać profilowaniu dane osobowe kandydatów lub pracowników, powinna ująć w swoim obowiązku informacyjnym następujące elementy:

- informację, że proces profilowania będzie wykonywany,
- opis konsekwencji i znaczenie profilowania dla danej osoby (dotyczy wyłącznie profilowania bez udziału czynnika ludzkiego),
- pouczenie o prawie wniesienia sprzeciwu względem profilowania, gdy przetwarzanie danych jest oparte na art. 6 ust 1 lit. f RODO.

WAŻNE: jeżeli rekrutacja kandydatów odbywa się wyłącznie przy użyciu systemów informatycznych, które samodzielnie dokonują ostatecznego wyboru (tj. wprowadzenie kryteriów do systemu kończy się przedstawieniem przez system wiążacej listy optymalnych kandydatów), mamy do czynienia z profilowaniem kwalifikowanym, wymagającym uzyskania zgody kandydata.

Prawo dostępu do danych – art. 15 RODO

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora danych potwierdzenia, czy przetwarza on dane osobowe jej dotyczące. Jeżeli tak, osoba ta może żądać np. udzielenia jej informacji o celu przetwarzania, czy też okresie, przez jaki dane będą przetwarzane. Administrator ma obowiązek wydać podmiotowi żądającemu kopię jego danych, przy czym domyślną formą wydania kopii jest kopia elektroniczna. Kopia danych powinna być przygotowana w powszechnie stosowanym i możliwym do odczytu pliku, np. plik txt, csv, xls lub pdf.

Prawo do sprostowania danych – art. 16 RODO

Osoba, której dane dotyczą, może w dowolnym momencie żądać od agencji zatrudnienia, z uwzględnieniem celów przetwarzania, sprostowania dotyczących jej danych osobowych, które są nieprawidłowe lub ich uzupełnienia, jeżeli są niekompletne.

Prawo do usunięcia danych (bycia zapomnianym) – art. 17 RODO

Osoba, której dane dotyczą, może w dowolnym momencie żądać od agencji usunięcia wszystkich dotyczących jej danych osobowych. Prawo do bycia zapomnianym realizowane jest poprzez usunięcie wszelkich danych danej osoby z wszystkich systemów ICT, w których są one przetwarzane. Ponadto agencja musi dołożyć wszelkich starań, aby podmioty przetwarzające dokonały takiego usunięcia ze swoich systemów. Agencja powinna także przekazać taki wniosek odbiorcom danych, np. klientom usług rekrutacyjnych, do których zostały przesłane dane potencjalnego kandydata, czy pracodawcom użytkownikom, którzy przetwarzają dane pracowników tymczasowych.

Kluczowym zagadnieniem przy realizacji prawa do zapomnienia w kontekście systemów sztucznej inteligencji jest mechanizm „unlearning" (tzw.

„oduczenie modelu"), polegający na usunięciu wpływu danych konkretnej osoby na model bez konieczności jego całkowitego usuwania i ponownego, kosztownego trenowania. Modele AI, zwłaszcza głębokie sieci neuronowe, nie przechowują danych osobowych w łatwych do usunięcia rekordach. Informacja o konkretnej osobie jest rozproszona. Usunięcie danych osobowych konkretnego podmiotu danych jest technicznie bardzo skomplikowane i często niewykonalne.

Prawa osób fizycznych są realizowane w sposób elektroniczny lub pisemny poprzez przesłanie żądania wraz z danymi umożliwiającymi identyfikację składającego żądanie. Szczególne ograniczenia w realizacji prawa do bycia zapomnianym występują w odniesieniu do pracowników i byłych pracowników. W tym zakresie sposób i czas przetwarzania danych osobowych są regulowane odrębnymi przepisami, np. w odniesieniu do dokumentacji pracowniczej (co do zasady przechowywanej 10 lub 50 lat od zakończenia zatrudnienia), protokołu ustalenia okoliczności i przyczyn wypadku przy pracy wraz z dokumentacją powypadkową (10 lat), nagrań z monitoringu wizyjnego (3 miesiące) czy kopii deklaracji rozliczeniowych i imiennych raportów miesięcznych składanych do ZUS (5 lat).

Prawo do sprzeciwu – art. 21 RODO

Prawo to przysługuje **wyłącznie** osobie, której dane przetwarzane są:

- w interesie publicznym lub w ramach sprawowania władzy publicznej,
- do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią,
- do celów marketingu bezpośredniego.

Zgłoszenie sprzeciwu w powyższych sytuacjach powoduje, że dalsze przetwarzanie danych staje się co do zasady niemożliwe.

> **WAŻNE:** prawo do sprzeciwu nie przysługuje osobie, której dane są przetwarzane na podstawie zgody lub w związku z realizacją umowy. W stosunku do tych osób, aby uniknąć wprowadzenia w błąd, w obowiązku informacyjnym nie powinno się wskazywać prawa do sprzeciwu (osoby te mają jednak prawo do wycofania zgody) albo należy zaznaczyć, że prawo to stosuje się tylko w określonych przypadkach.

Prawo do sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego powinno być zakomunikowane osobie, której dane dotyczą, oddzielnie i w sposób zrozumiały.

Prawo do ograniczenia przetwarzania danych – art. 18 RODO

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania jej danych, między innymi w przypadkach, gdy:

- kwestionuje ona prawidłowość danych osobowych lub gdy przetwarzanie jest niezgodne z prawem, a osoba ta sprzeciwia się usunięciu danych, żądając w zamian ograniczenia ich wykorzystywania.

PRZYKŁAD:

Jeżeli osoba fizyczna zgłasza błąd w swoim nazwisku, to do czasu jego poprawienia we wszystkich systemach błędne dane mogą być przeniesione do innego systemu lub

oznaczone „do poprawy" tak, aby osoby mające dostęp do systemów informatycznych nie korzystały z błędnych danych.

- administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń.

PRZYKŁAD:

Jeżeli pracownik pozostawił w kwestionariuszu osobowym dane osoby do kontaktu alarmowego (np. imię, nazwisko, nr telefonu), to po zakończeniu zatrudnienia były pracownik może zwrócić się z wnioskiem o ograniczenie przetwarzania tych danych.

Prawo do przenoszenia danych – art. 20 RODO

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie (np. csv, xls), dane osobowe jej dotyczące, a także przesłać je innemu administratorowi bez przeszkód ze strony dotychczasowego administratora, któremu dostarczono te dane osobowe. Poza tym, ma prawo żądać przesłania danych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Aby podmiot danych mógł skorzystać z tego uprawnienia muszą być spełnione łącznie następujące warunki:

- przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy,
- przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonywanie prawa do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

Prawo do bycia poinformowanym o tym, że administrator sprostował, usunął lub ograniczył przetwarzanie danych – art. 19 RODO

Administrator ma obowiązek poinformowania o sprostowaniu, usunięciu lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe (chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku), a jeżeli zainteresowany tego zażąda – poinformowania go o odbiorcach danych.

Prawo do niebycia poddanym zautomatyzowanej decyzji – art. 22 RODO

Każda osoba, której dane dotyczą, ma prawo do tego, aby nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu jej danych, w tym profilowaniu. Zakaz podejmowania automatycznych decyzji, o którym mowa w art. 22 RODO, wymaga spełnienia dwóch przesłanek łącznie:

- decyzja, której miałby podlegać podmiot danych, opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu (tj. bez merytorycznego udziału człowieka), oraz
- decyzja ta wywołuje wobec podmiotu danych skutki prawne lub w podobny sposób na nią wpływa.

Aby móc poddać podmiot danych decyzji, która opiera się na wyłącznie zautomatyzowanym przetwarzaniu (w tym profilowaniu), należy spełnić jedną z przesłanek z art. 22 ust. 2 RODO, np. uzyskać wyraźną zgodę podmiotu danych.

PROCEDURA OBSŁUGI WNIOSKÓW OSÓB FIZYCZNYCH, KTÓRYCH DANE DOTYCZĄ

W związku z koniecznością realizacji wniosków osób fizycznych na podstawie RODO agencja powinna opracować procedurę obsługi wniosków osób fizycznych zawierającą poniższe elementy:

1. Zakres, cel i forma wniosków

CEL I ZAKRES

Jasne określenie, że procedura dotyczy realizacji wszystkich praw podmiotów danych wynikających z RODO (dostęp do danych, sprostowanie, usunięcie, ograniczenie przetwarzania, przenoszenie danych, sprzeciw).

KANAŁY SKŁADANIA WNIOSKÓW

Określenie i uwzględnienie wszystkich kanałów, którymi wnioski mogą być składane (np. dedykowany adres e-mail, formularz na stronie internetowej, forma papierowa, osobiste zgłoszenie w siedzibie). W dokumencie zaleca się podanie co najmniej dwóch alternatywnych form kontaktu.

WYMAGANE ELEMENTY WNIOSKU

Wskazanie, jakie dane powinny zostać podane we wniosku, aby umożliwić identyfikację osoby składającej żądanie. Administrator ma prawo zażądać dodatkowych informacji, jeśli jest to niezbędne do spełnienia żądania osoby fizycznej.

POTWIERDZENIE WPŁYWU

Wskazanie na dobrą praktykę stosowania automatycznej informacji zwrotnej potwierdzającej wpłynięcie wniosku (zwłaszcza w przypadku wniosków mailowych). Należy także regularnie sprawdzać folder "spam", aby prawidłowo obsłużyć składane wnioski trafiające do tego folderu.

2. Weryfikacja tożsamości i ocena wniosku

WERYFIKACJA TOŻSAMOŚCI

Określenie, w jaki sposób tożsamość osoby składającej wniosek zostanie potwierdzona na podstawie danych zawartych we wniosku, aby uniknąć udostępnienia danych nieuprawnionemu odbiorcy, co mogłoby stanowić naruszenie ochrony danych.

OCENA WNIOSKU

Procedura powinna zawierać wskazówki umożliwiające stwierdzenie:

- czy przechowywanie danych osobowych nie jest wymagane przez przepisy prawa (np. przepisy kadrowo-płacowe, przepisy dotyczące ZUS czy US),
- czy interes agencji (np. ochrona przed potencjalnymi roszczeniami) nie jest nadrzędny względem interesu składającego żądanie,
- czy składający żądanie nie wprowadza agencji w błąd,
- jakie dokumenty są wymagane, gdy wniosek składa pełnomocnik lub np. rodzic (np. upoważnienie/pełnomocnictwo z określonym zakresem umocowania; tok postępowania w razie braku upoważnienia).

3. Terminy i komunikacja

- Obowiązek udzielenia osobie, której dane dotyczą, informacji o działaniach podjętych w związku z jej żądaniem niezwłocznie, ale nie później niż w terminie jednego miesiąca od otrzymania żądania;

- Możliwość wydłużenia terminu realizacji maksymalnie o kolejne dwa miesiące ze względu na skomplikowany charakter żądania lub dużą liczbę wniosków;

- W przypadku wydłużenia terminu, konieczność poinformowania osoby, której dane dotyczą, w ciągu miesiąca od otrzymania żądania, o wydłużeniu terminu realizacji i przyczynach opóźnienia lub przyczynach niepodjęcia działań;

- Zalecenie cyklicznego (np. raz na tydzień) audytu wszystkich zdefiniowanych kanałów składania wniosków (e-mail, formularz, forma papierowa) przez wyznaczoną osobę w celu wczesnego wykrycia i obsługi potencjalnych wniosków, które mogły zostać pominięte, co jest niezbędne do dotrzymania miesięcznego terminu realizacji.

4. Zasada braku odpłatności

Realizacja praw podmiotów danych odbywa się bezpłatnie. Pobieranie opłat może mieć miejsce w sytuacjach wyjątkowych, jeżeli żądania są nieuzasadnione lub nadmierne, w szczególności, jeżeli są ustawiczne albo żądający zwróci się o kolejne kopie swoich danych osobowych. Wysokość opłaty nie powinna przewyższać zwykłych kosztów administracyjnych poniesionych na spełnienie żądania (koszty wysyłki, wykonania kopii itp.).

5. Rola podmiotu przetwarzającego

- W procedurze należy jasno określić, że podmiot przetwarzający (procesor) może odpowiadać na wnioski osób fizycznych jedynie, jeśli takie postanowienie zostało zawarte w umowie z administratorem danych;

- W przypadku gdy procesor otrzyma wniosek dotyczący danych osobowych, których nie jest administratorem, musi niezwłocznie przekazać go administratorowi danych, aby ten mógł prawidłowo i w terminie zrealizować wniosek.

Prawa osoby fizycznej a podstawy prawne przetwarzania danych osobowych – art. 6 ust. 1 RODO

Prawo osoby fizycznej (RODO)	Zgoda (lit. a)	Umowa (lit. b)	Obowiązek prawny (lit. c)	Żywotny interes (lit. d)	Interes publiczny (lit. e)	Prawnie uzasadniony interes (lit. f)
Dostęp do danych	TAK	TAK	TAK	TAK	TAK	TAK
Sprostowanie danych	TAK	TAK	TAK	TAK	TAK	TAK
Usunięcie danych ("bycie zapomnianym")	TAK	TAK	NIE	TAK	NIE	TAK
Ograniczenie przetwarzania	TAK	TAK	TAK	TAK	TAK	TAK
Przenoszenie danych	TAK	TAK	NIE	NIE	NIE	NIE
Sprzeciw	NIE	NIE	NIE	NIE	NIE	TAK
Wycofanie zgody	TAK	x	x	x	x	x

Dodatkowe uwagi do tabeli:

- Prawo do usunięcia danych nie przysługuje, gdy przetwarzanie jest niezbędne do wywiązania się z obowiązku prawnego (np. przechowywanie danych osobowych pracownika przez 10 lat od zakończenia stosunku pracy);
- Prawo do przenoszenia danych przysługuje tylko wtedy, gdy dane są przetwarzane na podstawie zgody lub umowy i jednocześnie przetwarzanie odbywa się w sposób zautomatyzowany (czyli np. nie dotyczy kartotek papierowych);
- Z prawa do sprzeciwu osoba fizyczna może skorzystać wtedy, gdy przetwarzanie opiera się na prawnie uzasadnionym interesie administratora — np. składając sprzeciw wobec działań z zakresu marketingu bezpośredniego;
- Cofnięcie zgody. Choć nie jest to „prawo" w tabelarycznym ujęciu art. 15-22 RODO, to w przypadku przetwarzania na podstawie zgody, osoba fizyczna ma prawo ją cofnąć w dowolnym momencie bez podawania przyczyny.

Rejestr wniosków podmiotów danych

Agencja, aby udowodnić spełnienie zasady rozliczalności (art. 5 ust. 2 RODO), powinna prowadzić formalny rejestr wszystkich otrzymanych wniosków od podmiotów danych oraz dokumentować cały przebieg procesu.

Rejestr taki zawiera:

- datę wpływu wniosku i kanał jego złożenia,
- wyszczególnienie żądanego prawa (np. dostępu, usunięcia, sprzeciwu),
- podjęte działania lub powód niepodjęcia działań,
- datę wysłania odpowiedzi oraz kopię tej odpowiedzi.

Konsekwencje niespełnienia żądań podmiotów danych

W przypadku, gdyby administrator nie spełnił żądania uzupełnienia, uaktualnienia, sprostowania danych albo czasowego lub stałego wstrzymania ich przetwarzania, osoba, której dane dotyczą, ma prawo złożyć do organu nadzorczego wniosek o nakazanie dopełnienia tego obowiązku.

Każdy administrator realizuje żądania podmiotów danych we własnym zakresie i zgodnie z obowiązującymi w firmie procedurami, w terminach zgodnych z przepisami prawa.

Warto pamiętać, że treść wniosków osób fizycznych może być dowolna, np. osoba fizyczna może „cofnąć zgodę na marketing", odnosząc się do wyrażenia sprzeciwu. To jednak nie zwalnia administratora danych z wykonania tego wniosku (czyli zanotowania wyrażenia sprzeciwu i zaprzestania komunikacji marketingowej). Administrator nie może wymagać dokładnego zacytowania przepisu przez osobę składającą wniosek. W przypadku wątpliwości co do złożonego wniosku, jeżeli nie ma jasności co do intencji osoby składającej dany wniosek, należy wysłać prośbę o jego doprecyzowanie.

II Usługi agencji zatrudnienia

USŁUGI REKRUTACYJNE

Charakterystyka usługi

Polski prawodawca nie wprowadził odrębnej definicji pojęcia „usługi rekrutacyjne" – jest to potoczne określenie świadczeń, które ustawa z dnia 20 marca 2025 r. o rynku pracy i służbach zatrudnienia[1] (dalej: „ustawa") formalnie nazywa usługami pośrednictwa pracy. Zakres obu tych pojęć w praktyce dotyczy jednak tego samego obszaru działania.

Zgodnie z art. 81 ustawy pośrednictwo pracy polega na udzielaniu pomocy bezrobotnym, poszukującym pracy i osobom niezarejestrowanym, w tym osobom biernym zawodowo, w uzyskaniu zatrudnienia lub innej pracy zarobkowej oraz pracodawcom pomocy w pozyskaniu kandydatów do pracy.

Przetwarzanie danych osobowych jest niezbędnym elementem świadczenia usług rekrutacyjnych. Dane osobowe osób poszukujących pracy są pozyskiwane i wykorzystywane w celu dopasowania ofert pracy, a także do weryfikacji, czy profil zawodowy danej osoby odpowiada wymogom danego stanowiska. Mając na względzie zasady określone w art. 21^{1} – 22^{1b} Kodeksu pracy oraz wskazany tam katalog danych, w ramach procesu rekrutacji gromadzone są przede wszystkim dane identyfikacyjne, wskazane przez kandydata dane kontaktowe, jak również informacje w zakresie doświadczenia zawodowego i wykształcenia. Wszystkie te informacje stanowią dane osobowe dotyczące danego kandydata niezależnie od tego, czy zostały podane bezpośrednio przez kandydata, czy też są zawarte w materiałach wytworzonych przez rekrutera w trakcie procesu rekrutacyjnego, np. w formie notatek czy rekomendacji.

Zakres danych zbieranych o kandydacie

Dane osobowe przetwarzane w związku z rekrutacją powinny być gromadzone w sposób celowy i ograniczony, tak aby informacje zbierane oraz tworzone w toku rekrutacji były rzeczywiście niezbędne do realizacji celów danego procesu. Oznacza to, że rozmowy rekrutacyjne, pytania oraz przechowywane informacje o kandydacie powinny pozostawać w bezpośrednim związku z oceną dopasowania do stanowiska, na jakie ubiega się kandydat, lub pozwalać na wyszukanie dla niego zatrudnienia spełniającego jego oczekiwania. Niedopuszczalne jest zbieranie informacji nieistotnych z punktu widzenia poszukiwanego zatrudnienia, w szczególności dotyczących życia prywatnego.

Szczególnej uwagi wymaga pozyskiwanie danych osobowych szczególnych kategorii czy dokumentów, co może mieć miejsce w przypadku m.in. weryfikacji karalności kandydatów, sprawdzenia legalności pobytu lub pracy cudzoziemców, a także weryfikacji tożsamości kandydatów[2]. Podejmowanie takich działań wymaga odrębnej oceny prawnej, w tym w zakresie weryfikacji obowiązujących

1 Dz. U. z 2025 r. poz. 620

2 Tytułem przykładu, obowiązek lub uprawnienie do pozyskania informacji o niekaralności może wynikać z przepisów szczególnych, jak np.: ustawa z dnia 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego; art. 21 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich.

regulacji prawnych oraz wytycznych właściwych organów pod kątem ustalenia istnienia podstaw prawnych. Zbieranie tego rodzaju danych może mieć miejsce wyłącznie w przypadkach, w sposób i w zakresie wyraźnie przewidzianych przepisami prawa, a ich realizacja przez agencję w procesie rekrutacji może prowadzić do przyjęcia roli podmiotu przetwarzającego.

Podstawowe role pełnione przez agencję i klientów usług rekrutacyjnych

Agencja jako administrator danych

Najczęściej występującym modelem prowadzenia rekrutacji z udziałem agencji jest model, w którym agencja i jej klient działają jako odrębni administratorzy danych osobowych[2].

Agencja przetwarza dane w ramach własnej bazy kandydatów, wykorzystując je na potrzeby projektów rekrutacyjnych dla różnych klientów. Działanie w takim modelu charakteryzuje się tym, że agencja wykorzystuje własne zasoby, posługuje się własnymi metodami, korzysta z własnego know-how, metodologii, narzędzi i systemów oraz działa według wewnętrznie ustalonych schematów operacyjnych. Współpraca z klientem polega na udostępnieniu danych osobowych wybranych, rekomendowanych kandydatów klientowi. Klient agencji, po otrzymaniu danych, staje się odrębnym administratorem i przetwarza je we własnych celach (weryfikacja kandydata, podjęcie decyzji o zatrudnieniu lub odrzuceniu danej kandydatury). Na tym etapie klient samodzielnie decyduje o celach (zatrudnienie pracownika o poszukiwanych cechach) i środkach przetwarzania (analiza rekomendacji, spotkanie z kandydatem).

Wyjątki od zasady ogólnej

Od opisanego wyżej, podstawowego modelu działania agencji – jako administratora danych – istnieją wyjątki. Pamiętać należy, że rola administratora lub procesora zależy od tego, jak faktycznie odbywa się przetwarzanie danych w ramach konkretnej współpracy pomiędzy agencją a jej klientem. Dlatego też rola Agencji może ulec modyfikacji w zależności od sposobu ukształtowania usługi świadczonej przez agencję na rzecz jej klienta, a zakres obowiązków agencji czy sposób ich realizacji mogą powodować, że będzie pełnić ona dodatkowo lub wyłącznie rolę podmiotu przetwarzającego[3].

Mając to na uwadze, można wskazać kilka najczęściej spotykanych wyjątków, gdzie agencja może działać jako podmiot przetwarzający. Do takich sytuacji można zaliczyć usługi:

- tworzenia bazy kandydatów dedykowanej konkretnemu klientowi;
- prowadzenia procesów rekrutacyjnych według zasad i instrukcji klienta (np. w zakresie obowiązkowego procesu weryfikacji kandydatów, wymaganych screeningów dopuszczalnych w świetle polskiego prawa, weryfikacji niekaralności osoby ubiegającej się o zatrudnienie, zbierania zgód na rzecz klienta, wytycznych w zakresie metodologii prowadzenia procesu

2 Por. World Employment Confederation, Controller or Processor? Guidelines on Data Processing Roles for HR Service Providers, 2024, część dotycząca usług Direct recruitment oraz Recruitment process outsourcing (RPO), https://wecglobal.org/uploads/2019/07/WEC-guidelines-data-processing-roles-2024.pdf, dostęp z dnia: 06.07.2026.

3 Zob. EROD, Wytyczne 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO, wersja 2.0, 7.07.2021 r., szczególnie Załącznik 1 – Schemat stosowania w praktyce pojęć administratora, podmiotu przetwarzającego i współadministratorów, https://www.edpb.europa.eu/system/files/documents/2023-10/edpb_guidelines_202007_controllerprocessor_final_pl.pdf, dostęp z dnia: 06.07.2026.

rekrutacyjnego, dedykowanych testów służących do oceny predyspozycji kandydata);

- prowadzenia procesów rekrutacyjnych wyłącznie w celu realizacji celów rekrutacyjnych klienta (usługi typu *recruitment process outsourcing*).

W podanych przykładach agencja nie realizuje własnych celów przetwarzania, a działa według wytycznych i instrukcji klienta. Kandydaci w takich procesach nie są kandydatami agencji, a kandydatami klienta. Przekazywanie danych między agencją a klientem odbywa się na podstawie umowy powierzenia, która reguluje zasady przetwarzania danych przez agencję na rzecz klienta (w szczególności zakres powierzanych danych, powierzane procesy oraz wykorzystywane narzędzia).

Powyższe przykłady stanowią jedynie ogólne wytyczne. Choć w przypadku usług rekrutacyjnych agencja najczęściej będzie pełniła rolę odrębnego administratora, a umowa powierzenia nie będzie wymagana, każda sytuacja wymaga indywidualnej analizy. Szczegółowe postanowienia umowy z klientem mogą prowadzić do zmiany roli agencji, lub przypisania jej różnych ról do poszczególnych elementów usługi.

Podstawy prawne przetwarzania danych kandydatów w procesie rekrutacji[4]

Każdy cel przetwarzania musi posiadać odrębną, właściwą podstawę prawną. W przypadku, gdy dla tego samego celu mogą mieć zastosowanie różne podstawy prawne, administrator powinien wybrać taką, która po starannym rozważeniu kontekstu przetwarzania jest najbardziej adekwatna. Co istotne, wybór podstawy prawnej może wpłynąć na prawa kandydatów do ich danych osobowych – o nich szerzej w rozdziale IV.

W kontekście rekrutacji możliwe do wykorzystania podstawy prawne to:

- umowa na świadczenie usług rekrutacyjnych lub działania przedumowne (art. 6 ust. 1 lit. b RODO),
- obowiązek prawny (art. 6 ust. 1 lit. c RODO),
- uzasadniony interes (art. 6 ust. 1 lit. f RODO),
- zgoda kandydata (art. 6 ust. 1 lit. a RODO).

Bardziej wyczerpujące informacje dotyczące wskazanych wyżej podstaw prawnych oraz możliwości oparcia na nich przetwarzania danych znajdują się w rozdziale I.

Należy pamiętać, że udostępnienie danych do klienta także jest czynnością przetwarzania danych, dlatego powinno być powiązane z adekwatną i udokumentowaną podstawą prawną. Należy także zapewnić, aby kandydat został poinformowany, jakiemu klientowi zostaną przedstawione jego dane osobowe lub profil.

4 Por. CNIL, Guide recrutement: les fondamentaux en matière de protection des données personnelles et questions-réponses, fiche n° 4, s. 23–29, https://www.cnil.fr/fr/le-guide-du-recrutement, dostęp z dnia: 06.07.2026. Źródło: CNIL – https://www.cnil.fr. Warunki ponownego wykorzystania: Mentions légales CNIL; licencja wskazana przez CNIL dla treści udostępnianych na cnil.fr: CC BY-NC-SA 4.0, o ile przy danym materiale nie wskazano inaczej. Wykorzystanie materiałów CNIL nie oznacza zatwierdzenia niniejszego opracowania przez CNIL.

III PRACA TYMCZASOWA

Charakterystyka usługi pracy tymczasowej

Praca tymczasowa jest usługą zdefiniowaną w ustawie z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych[1] (dalej również: „ustawa"). Polega ona na zatrudnianiu pracowników tymczasowych przez pracodawcę będącego agencją pracy tymczasowej oraz kierowaniu tych pracowników i osób niebędących pracownikami agencji pracy tymczasowej do wykonywania pracy tymczasowej na rzecz i pod kierownictwem pracodawcy użytkownika.

Agencja pracy tymczasowej może zatrudniać i kierować do wykonywania pracy tymczasowej na rzecz pracodawcy użytkownika zarówno pracowników tymczasowych zatrudnionych na podstawie umów o pracę na czas określony, jak i osoby niebędące pracownikami, świadczące pracę na podstawie umów cywilnoprawnych. W dalszej części rozdziału obie te grupy będą dla uproszczenia określane wspólnie mianem pracowników tymczasowych.

W ustawie uregulowana została szczególna, odbiegająca od klasycznego modelu stosunku pracy, relacja trójstronna pomiędzy pracownikiem tymczasowym, agencją pracy tymczasowej a pracodawcą użytkownikiem. Istotą tej konstrukcji jest fakt, że umowa o pracę (lub umowa cywilnoprawna) zawierana jest przez agencję wyłącznie w celu skierowania pracownika tymczasowego do wykonywania pracy tymczasowej na rzecz pracodawcy użytkownika. Agencja pracy tymczasowej pozostaje formalnym pracodawcą, podczas gdy faktyczne kierownictwo oraz nadzór nad wykonywaną pracą sprawuje pracodawca użytkownik. Ta specyfika prowadzi do swoistego podziału funkcji pracodawcy, co ma istotne znaczenie w kontekście definicji stosunku pracy określonej w art. 22 § 1 Kodeksu pracy. Zgodnie z tym przepisem przez nawiązanie stosunku pracy pracownik zobowiązuje się do wykonywania pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem oraz w miejscu i czasie wyznaczonym przez pracodawcę, a pracodawca do zatrudniania pracownika za wynagrodzeniem. Na gruncie ustawy definicja ta ulega jednak modyfikacji, ponieważ kluczowe elementy stosunku pracy, takie jak:

- wykonywanie pracy określonego rodzaju,
- wykonywanie pracy „na rzecz" danego podmiotu,
- kierownictwo nad pracownikiem,
- wyznaczanie miejsca i czasu pracy,

realizowane są przez pracodawcę użytkownika lub na jego rzecz. W konsekwencji należy przyjąć, że zasadnicza część funkcji pracodawcy, wynikająca z art. 22 Kodeksu pracy, wykonywana jest przez pracodawcę użytkownika, który działa we własnym imieniu, przy wykorzystaniu własnych środków oraz dla realizacji własnych celów gospodarczych.

1 Dz.U. z 2025 r. poz. 236

Podstawowe role pełnione przez agencję pracy tymczasowej i pracodawcę użytkownika w kontekście danych osobowych pracowników tymczasowych

Na etapie rekrutacji kandydatów do wykonywania pracy tymczasowej rolę administratora danych osobowych pełni agencja pracy tymczasowej.

Na gruncie ustawy oraz przepisów Kodeksu pracy na etapie zawierania umowy o pracę (lub umowy cywilnoprawnej) status administratora danych osobowych przysługuje wyłącznie agencji pracy tymczasowej. To ona występuje w tej relacji jako pracodawca i zawiera umowę z pracownikiem tymczasowym, określa jej warunki oraz realizuje obowiązki wynikające z przepisów prawa pracy – w szczególności w zakresie prowadzenia dokumentacji pracowniczej, naliczania i wypłaty wynagrodzenia oraz realizacji zobowiązań publicznoprawnych. W konsekwencji to agencja ustala cele i sposoby przetwarzania danych osobowych pracownika tymczasowego w związku z nawiązaniem stosunku pracy (stosunku cywilnoprawnego), co – zgodnie z art. 4 pkt 7 RODO – przesądza o jej statusie administratora. Przetwarzanie danych osobowych pracowników tymczasowych na tym etapie odbywa się przede wszystkim w celu zawarcia i wykonania umowy o pracę (lub umowy cywilnoprawnej) oraz wypełnienia obowiązków prawnych ciążących na pracodawcy, przy czym zakres danych wyznaczają przepisy art. 22^1 Kodeksu pracy oraz regulacje szczególne. W uzasadnionych sytuacjach możliwe jest udostępnianie pracodawcy użytkownikowi wybranych danych rekrutacyjnych kandydatów na podstawie prawnie uzasadnionych interesów pracodawcy użytkownika, którymi mogą być: potwierdzenie kwalifikacji zawodowych kandydatów czy weryfikacja okresów zatrudnienia.

Po zawarciu umowy o pracę (lub umowy cywilnoprawnej) status administratora danych osobowych pracownika tymczasowego nie przysługuje wyłącznie jednemu podmiotowi. Ze względu na szczególną konstrukcję zatrudnienia tymczasowego oraz podział funkcji pracodawcy, rola administratora danych również ulega podziałowi pomiędzy agencję pracy tymczasowej a pracodawcę użytkownika. Agencja, jako podmiot zawierający umowę o pracę z pracownikiem tymczasowym i występujący w roli pracodawcy formalnego, pozostaje administratorem w zakresie wynikającym z nawiązania i trwania stosunku pracy. Dotyczy to w szczególności prowadzenia dokumentacji pracowniczej, naliczania i wypłaty wynagrodzenia oraz realizacji obowiązków publicznoprawnych, co znajduje podstawę w przepisach kodeksu pracy oraz regulacjach szczególnych. Jednocześnie pracodawca użytkownik – który zgodnie z ustawą organizuje pracę pracownika tymczasowego, sprawuje nad nim kierownictwo oraz wyznacza miejsce i czas wykonywania pracy – przetwarza jego dane osobowe w zakresie niezbędnym do realizacji tych zadań, działając we własnym imieniu i dla własnych celów gospodarczych. Brak jest regulacji prawnych dających podstawę do przyjęcia, że pracodawca użytkownik wykonuje te obowiązki w imieniu agencji pracy tymczasowej na zasadzie zlecenia. W konsekwencji należy uznać, że pracodawca użytkownik posiada status administratora danych osobowych w rozumieniu art. 4 pkt 7 RODO, oraz że pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem nie zachodzi relacja administrator – podmiot przetwarzający, gdyż każdy z tych podmiotów samodzielnie określa cele i sposoby przetwarzania danych osobowych, wykonując własne obowiązki wynikające z przepisów prawa. W analizowanym modelu mamy zatem do czynienia z równoległym przetwarzaniem danych osobowych pra-

cowników tymczasowych przez dwóch odrębnych administratorów, działających w różnych, choć funkcjonalnie powiązanych zakresach.

Za tezą, że pracodawca użytkownik jest pełnoprawnym i niezależnym administratorem danych osobowych pracowników tymczasowych przemawiają poniżej wskazane ustawowe prawa i obowiązki pracodawcy użytkownika:

- pracodawca użytkownik sprawuje nadzór i kierownictwo nad pracownikiem tymczasowym na takich samych zasadach jak tradycyjny pracodawca, co oznacza, że ma prawo wydawać pracownikowi tymczasowemu bieżące polecenia służbowe, zarządzać jego czasem pracy itp. (art. 2 pkt 1 i pkt 2 ustawy);

- pracodawca użytkownik wyznacza pracownikowi tymczasowemu zadania i kontroluje ich wykonanie (art. 2 pkt 1 ustawy);

- pracodawca użytkownik informuje agencję pracy tymczasowej o wynagrodzeniu przysługującym pracownikowi tymczasowemu, a także o obowiązujących u siebie wewnętrznych regulacjach (art. 9 ust. 2 pkt 1 ustawy) oraz o ich zmianie (art. 9a ustawy);

- pracodawca użytkownik dostarcza pracownikowi tymczasowemu odzież i obuwie robocze oraz środki ochrony indywidualnej, zapewnia napoje i posiłki profilaktyczne, przeprowadza szkolenia w zakresie bezpieczeństwa i higieny pracy, ustala okoliczności i przyczyny wypadku przy pracy, przeprowadza ocenę ryzyka zawodowego oraz informuje o tym ryzyku (art. 9 ust. 2a ustawy);

- pracodawca użytkownik wykonuje obowiązki i korzysta z praw przysługujących pracodawcy w zakresie niezbędnym do organizowania pracy z udziałem pracownika tymczasowego (art. 14 ust. 1 ustawy);

- pracodawca użytkownik jest obowiązany zapewnić pracownikowi tymczasowemu bezpieczne i higieniczne warunki pracy w miejscu wyznaczonym do wykonywania pracy tymczasowej (art. 14 ust. 2 pkt 1 ustawy);

- pracodawca użytkownik prowadzi ewidencję czasu pracy pracownika tymczasowego w zakresie i na zasadach obowiązujących w stosunku do pracowników (art. 14 ust. 2 pkt 2 ustawy);

- pracodawca użytkownik prowadzi ewidencję osób wykonujących pracę tymczasową (art. 14a ustawy);

- poprzez sprawowanie kierownictwa nad wykonywaniem pracy tymczasowej i organizowaniem pracy z udziałem pracownika tymczasowego, pracodawca użytkownik ustala zasady np. przyznawania premii lub nagrody (art. 2 pkt 2 i art. 14 ust. 1 ustawy);

- pracodawca użytkownik ma obowiązek stosować wobec pracowników tymczasowych tzw. zasadę równego traktowania w zakresie warunków pracy i innych warunków zatrudnienia (art. 15 ust. 1 ustawy).

Powyższe wyliczenie jednoznacznie wskazuje, że praktycznie od momentu przekazania pracodawcy użytkownikowi przez agencję pracy tymczasowej listy pracowników tymczasowych, którzy mają stawić się do wykonywania pracy tymczasowej w jego zakładzie pracy, pracodawca użytkownik zaczyna przetwarzać dane osobowe tych pracowników tymczasowych wyłącznie dla własnych

celów związanych z prowadzeniem własnego przedsiębiorstwa, we własnym imieniu, przy pomocy własnych środków i wykonując w stosunku do pracowników tymczasowych obowiązki pracodawcy. Pracodawca użytkownik jest także jedynym odbiorcą pracy tymczasowej wykonywanej przez pracownika tymczasowego i tylko on korzysta z jej materialnych efektów. Jest to samodzielna rola, w której pracodawca użytkownik nie działa na zlecenie agencji pracy tymczasowej ani nie wykonuje czynności w jej imieniu. Przykładami działania pracodawcy użytkownika we własnym imieniu z wykorzystaniem danych osobowych pracowników tymczasowych są: wydawanie bieżących poleceń służbowych, przypisywanie podległości pracownika tymczasowego w strukturze pracodawcy użytkownika, prowadzenie szkoleń wprowadzających oraz szkoleń z zakresu BHP, ustalanie rozkładów i harmonogramów czasu pracy oraz prowadzenie ewidencji czasu pracy, prowadzenie postępowania w sprawie ustalenia okoliczności i przyczyn wypadku przy pracy oraz sporządzanie protokołów powypadkowych, prowadzenie ewidencji okresów zatrudnienia, wydawanie kart dostępowych do zakładu pracy, wydawanie identyfikatorów pracownika, sporządzanie list pracowników na poszczególnych zmianach, stosowanie do pracowników regulaminów premiowania obowiązujących u pracodawcy użytkownika, uwzględnianie pracowników tymczasowych w planach benefitowych pracodawcy użytkownika, przekazywanie list zatrudnionych pracowników związkom zawodowym, raportowanie danych o takich pracownikach do własnych struktur organizacyjnych itp.

Ponadto, należy także zwrócić uwagę na przepis art. 5 ustawy, zgodnie z którym w zakresie nieuregulowanym odmiennie przepisami ustawy również do pracodawcy użytkownika (a nie tylko do agencji pracy tymczasowej) stosuje się odpowiednio przepisy prawa pracy dotyczące pracodawcy.

Nie ma przeszkód, aby w umowie o świadczenie usług pracy tymczasowej zawartej pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem doprecyzować lub rozszerzyć zakres obowiązków pracodawcy użytkownika, o ile nie prowadzi to do naruszenia przepisów ustawy ani do zmiany ustawowego podziału ról pomiędzy tymi podmiotami. Przykładem takiej modyfikacji może być uzgodnienie zakresu przejęcia przez pracodawcę użytkownika obowiązków pracodawcy dotyczących bezpieczeństwa i higieny pracy innych, niż określone w art. 9 ust. 2a ustawy, lub zakresu przejęcia przez pracodawcę użytkownika obowiązku pracodawcy dotyczącego wypłacania należności na pokrycie kosztów związanych z podróżą służbową. Powyższe nie wpływa jednak na status tych podmiotów na gruncie przepisów o ochronie danych osobowych ponieważ zarówno agencja pracy tymczasowej, jak i pracodawca użytkownik nadal pozostają odrębnymi administratorami danych osobowych, przetwarzającymi dane we własnych celach oraz w zakresie wynikającym z realizowanych przez nich obowiązków określonych przepisami prawa.

Mając na uwadze powyższe należy przyjąć, że w zakresie wykonywania wskazanych powyżej czynności pracodawca użytkownik występuje jako odrębny administrator danych osobowych, przetwarzający dane we własnych celach oraz przy wykorzystaniu samodzielnie określonych środków przetwarzania. Stanowisko takie prezentuje również WEC-Europe, wskazując, że zarówno agencja pracy tymczasowej, jak i pracodawca użytkownik mogą posiadać status niezależnych administratorów danych osobowych w zakresie realizowanych przez siebie zadań i obowiązków[2].

2 https://wecglobal.org/uploads/2019/07/WEC-guidelines-data-processing-roles-2024.pdf

Najważniejsze obszary relacji pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem

1. Zawarcie umowy na świadczenie usług pracy tymczasowej pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem

Zawarcie umowy na świadczenie usług pracy tymczasowej pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem wiąże się z wzajemnym udostępnianiem danych osobowych osób uczestniczących w procesie, w szczególności danych osobowych osób reprezentujących strony umowy oraz osób wskazanych do kontaktu. W takim wypadku każda ze stron występuje w roli samodzielnego administratora danych osobowych tych osób.

Podstawą prawną przetwarzania powyżej wskazanych danych osobowych jest prawnie uzasadniony interes stron umowy zgodnie z art. 6 ust. 1 lit. f RODO.

WAŻNE: Nierekomendowane jest, ze względu na związane z tym ryzyka prawne i operacyjne, przejmowanie przez agencję pracy tymczasowej wypełniania obowiązków informacyjnych pracodawcy użytkownika wynikających z art. 13 lub 14 RODO. Wykonanie obowiązku informacyjnego stanowi bowiem element przetwarzania danych osobowych i pozostaje bezpośrednio związane ze statusem administratora danych.

Błędem jest utożsamianie udostępniania danych osobowych, o którym mowa m.in. w definicji przetwarzania danych (art. 4 pkt 2 RODO), z powierzeniem przetwarzania danych w rozumieniu art. 28 RODO. Podejście takie prowadzi do zawierania nieprawidłowych umów powierzenia przetwarzania danych pomiędzy podmiotami, które w rzeczywistości występują jako odrębni administratorzy danych osobowych. Warunkiem uznania danego podmiotu za podmiot przetwarzający oraz podstawą do zawarcia umowy powierzenia przetwarzania danych jest bowiem przetwarzanie danych osobowych w imieniu i na udokumentowane polecenie administratora. Samo udostępnienie danych pomiędzy administratorami, realizowane w związku z wykonywaniem własnych obowiązków ustawowych lub prowadzeniem własnej działalności, nie stanowi jeszcze powierzenia przetwarzania danych w rozumieniu art. 28 RODO.

Umowa o świadczenie usług pracy tymczasowej zawarta między agencją pracy tymczasowej a pracodawcą użytkownikiem w żadnym zakresie nie może być podstawą przetwarzania danych osobowych pracowników tymczasowych, ponieważ pracownicy tymczasowi nie są stroną tej umowy.

2. Wykonanie umowy o świadczenie usług pracy tymczasowej pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem

Wykonanie umowy między stronami zasadniczo wiąże się z wypełnieniem obowiązków prawnych każdej ze stron. Pomijając szczególne przypadki, kiedy jedna ze stron zleca wykonanie swojego prawnego obowiązku drugiej stronie, każda ze stron występuje w roli administratora danych osobowych.

2.1. Podstawy prawne przetwarzania danych osób skierowanych do pracy tymczasowej

Podstawą prawną przetwarzania danych osobowych w związku z realizacją umowy zawartej pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem powinien być art. 6 ust. 1 lit. c RODO, tj. niezbędność przetwarzania do wypełnienia obowiązków prawnych ciążących na administratorze – wynikających w szczególności z przepisów ustawy oraz przepisów prawa pracy.

2.2. Udostępnianie danych osób skierowanych do pracy tymczasowej

Realizacja obowiązków wynikających z przepisów prawa przez agencję pracy tymczasowej oraz pracodawcę użytkownika wymaga wzajemnego udostępniania danych osobowych osób skierowanych do wykonywania pracy tymczasowej w zakresie niezbędnym do prawidłowego wykonywania obowiązków ciążących na każdej ze stron. Zakres przekazywanych danych powinien każdorazowo odpowiadać zasadzie minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO, a zatem być adekwatny, stosowny oraz ograniczony wyłącznie do danych niezbędnych do realizacji określonych obowiązków prawnych.

Z uwagi na charakter oraz zakres udostępnianych danych strony powinny również zapewnić odpowiedni poziom ich ochrony, dostosowany do sposobu przekazywania danych oraz zidentyfikowanych ryzyk. W przypadku udostępniania danych w formie elektronicznej zasadne jest stosowanie odpowiednich środków technicznych i organizacyjnych, w szczególności zabezpieczenia danych przy użyciu szyfrowania lub innych mechanizmów zapewniających poufność i integralność przesyłanych informacji.

WAŻNE: Strony umowy o świadczenie usług pracy tymczasowej nie są uprawnione do żądania wzajemnego udostępniania danych osobowych w zakresie wykraczającym poza zasadę minimalizacji danych oraz poza zakres niezbędny do realizacji konkretnych obowiązków prawnych ciążących na danej stronie. W konsekwencji niedopuszczalne jest żądanie przez pracodawcę użytkownika udostępnienia przez agencję pracy tymczasowej danych osobowych osób skierowanych do pracy tymczasowej w zakresie dotyczącym obowiązków prawnych, których realizacja spoczywa wyłącznie na agencji pracy tymczasowej. Brak jest bowiem podstawy prawnej uzasadniającej przekazywanie danych osobowych w zakresie niewiążącym się z obowiązkami realizowanymi przez pracodawcę użytkownika.

2.3. Możliwe zakresy udostępnianych danych osobowych osób skierowanych do wykonywania pracy tymczasowej w oparciu o niezbędność do wypełnienia obowiązków prawnych.

Agencja pracy tymczasowej udostępnia pracodawcy użytkownikowi dane osobowe pracowników tymczasowych w szczególności w następujących celach i zakresach:

- prowadzenie ewidencji osób skierowanych do pracy tymczasowej (ewidencja okresów zatrudnienia, ewidencja czasu pracy): imię, nazwisko, PESEL (lub nr dokumentu tożsamości), okresy zatrudnienia, czas pracy;

- dopuszczenie do pracy: orzeczenie lekarskie dotyczące badań profilaktycznych z zakresu

medycyny pracy (wstępnych, kontrolnych i okresowych);

- weryfikacja możliwości świadczenia pracy lub dostosowanie miejsca wykonywania pracy dla osób z niepełnosprawnościami, informacje o niepełnosprawności;
- informacje o zwolnieniach lekarskich, informacje dotyczące urlopu;
- postępowanie powypadkowe: dane osób wskazanych do kontaktu w przypadku wypadku.

Pracodawca użytkownik udostępnia agencji pracy tymczasowej dane osobowe pracowników tymczasowych w szczególności w następujących celach i zakresie:

- naliczanie wynagrodzeń: ewidencja czasu pracy, informacje o elementach wynagrodzenia, np. o dodatkach, premiach;
- prowadzenie dokumentacji z zakresu bezpieczeństwa i higieny pracy: protokoły szkoleń, dokumentacja powypadkowa;
- weryfikacja okresów pracy wykonywanej na rzecz pracodawcy użytkownika: okres pracy wykonywanej na rzecz pracodawcy użytkownika;
- rozwiązanie umowy, nakładanie kar dyscyplinarnych, kar umownych: informacje dotyczące przyczyn rozwiązania umowy lub nałożenia kar, np. nietrzeźwość, spóźnienia;
- przejęcie przez pracodawcę użytkownika obowiązków pracodawcy dotyczących bezpieczeństwa i higieny pracy – w tym wypadku kategorie danych zależą od zakresu przejętych obowiązków, np. w zakresie kontroli trzeźwości będą to protokoły z kontroli.

III DELEGOWANIE PRACOWNIKÓW DO PRACY ZA GRANICĄ W RAMACH ŚWIADCZENIA USŁUG

Charakterystyka usługi

Delegowanie pracowników do pracy za granicą w ramach swobody świadczenia usług zostało uregulowane w Dyrektywie 96/71/WE Parlamentu Europejskiego i Rady z 16.12.1996 r. dotyczącej delegowania pracowników w ramach świadczenia usług, zmienionej m.in. dyrektywą Parlamentu Europejskiego i Rady (UE) 2018/957, implementowanej na gruncie polskim ustawą z dnia 10 czerwca 2016 r. o delegowaniu pracowników w ramach świadczenia usług[1]. Polega ono na wysyłaniu przez przedsiębiorcę z jednego państwa członkowskiego własnych pracowników w celu tymczasowego świadczenia usługi w przedsiębiorstwie, mającym siedzibę w innym państwie członkowskim (tzw. państwie przyjmującym). Pracownicy delegowani pozostają zatrudnieni w kraju wysyłającym i de facto nie są włączani do rynku pracy państwa przyjmującego. Nie są więc pracownikami migrującymi. Z tego powodu delegowanie odbywa się w ramach swobody świadczenia usług, a nie swobody przepływu osób. Dyrektywa 96/71/WE wyznacza minimalne standardy zatrudnienia pracowników w sytuacji świadczenia usługi transgranicznej.

Przepisy przewidują kilka form delegowania pracowników w obrębie UE. Poza wysyłaniem pracowników bezpośrednio przez pracodawcę i pod jego kierownictwem, delegowanie może przybrać formę, w ramach której agencja zatrudnienia mająca siedzibę w danym państwie członkowskim wynajmuje pracownika tymczasowego przedsiębiorstwu prowadzącemu działalność gospodarczą lub działającemu na terytorium innego państwa członkowskiego.

Podstawowe role pełnione przez pracodawcę delegującego i jego zagranicznego klienta z innego państwa członkowskiego

Delegowanie pracowników w ramach swobody świadczenia usług na podstawie Dyrektywy 96/71/WE najczęściej przybiera postać:

- delegowania pracowników bezpośrednio przez ich pracodawcę: sytuacja, w której dedykowani pracownicy czasowo świadczą pracę na rzecz zagranicznego kontrahenta pracodawcy (np. w ramach realizacji określonego projektu), jego zagranicznego oddziału lub zagranicznej spółki matki,

- wysyłania pracowników tymczasowych świadczących pracę na rzecz i pod kierownictwem zagranicznego pracodawcy użytkownika,

- delegowania osób zatrudnionych na rzecz odbiorców nie będących pracodawcami: sytuacja, w której osoby zatrudnione świadczą usługi na rzecz odbiorców będących osobami fizycznymi, niemających statusu pracodawcy ani pracodawcy użytkownika.

W powyższych przypadkach, zarówno na etapie rekrutacji jak i zatrudnienia, pracodawca (w przypadku zatrudnienia

1 Dz.U. z 2016 r. poz. 868, z późn. zm.

tymczasowego działający w roli agencji zatrudnienia) **występuje w charakterze administratora danych osobowych**. Celem administrowania jest w tym wypadku zatrudnienie danego pracownika i skierowanie go do świadczenia pracy/świadczenia usług w innym państwie członkowskim na rzecz podmiotu trzeciego.

We wspomnianych wariantach odbiorca usługi (np. pracodawca użytkownik, kontrahent pracodawcy, do którego pracownik jest czasowo kierowany), również występuje w charakterze administratora danych delegowanych pracowników. W przypadku pracy tymczasowej wynika to z faktu, że po stronie pracodawcy użytkownika występuje szereg samodzielnych obowiązków i uprawnień, w tym przede wszystkim kierownictwo, wydawanie poleceń, organizowanie i nadzorowanie procesu pracy. Z kolei w przypadku czasowego delegowania pracownika na rzecz zagranicznego kontrahenta pracodawcy, czy też w sytuacji osoby fizycznej będącej odbiorcą usługi, podmiot ten administruje danymi osób delegowanych, np. na potrzeby weryfikacji jakości pracy, czasu w jakim jest ona świadczona czy wydajności procesu pracy.

We omawianych przypadkach przekazanie danych osobowych następuje najczęściej w formule ich udostępnienia pomiędzy odrębnymi administratorami danych. Co do zasady należy wykluczyć instytucję powierzenia przetwarzania danych osobowych, jeżeli każdy z podmiotów działa we własnym imieniu i realizuje własny, odrębny cel przetwarzania. Każdorazowo należy jednak ocenić rzeczywisty zakres decyzyjności stron co do celów i sposobów przetwarzania danych. Udostępnienie danych osobowych delegowanego pracownika zagranicznemu pracodawcy użytkownikowi, kontrahentowi pracodawcy delegującego albo odbiorcy usługi nie powinno co do zasady opierać się na zgodzie pracownika jako podstawowej przesłance przetwarzania. W relacjach zatrudnienia właściwą podstawą przetwarzania będzie najczęściej niezbędność wykonania umowy, wypełnienie obowiązku prawnego ciążącego na administratorze lub prawnie uzasadniony interes administratora, z uwzględnieniem zasady minimalizacji danych i obowiązku informacyjnego wobec pracownika.

Przetwarzanie danych osobowych na poszczególnych etapach delegowania pracowników w ramach swobody świadczenia usług

Co do zasady reguły przetwarzania danych osobowych w przypadku delegowania pracowników są zbieżne z tymi, które obowiązują w przypadku przetwarzania danych osobowych obowiązujących w państwie siedziby delegującego pracodawcy.

Na etapie rekrutacji dane osobowe kandydatów i pracowników delegowanych powinny być przetwarzane na podstawach adekwatnych do celu przetwarzania, w szczególności na podstawie art. 6 ust. 1 lit. b RODO, jeżeli przetwarzanie jest niezbędne do podjęcia działań przed zawarciem umowy lub do wykonania umowy, a także art. 6 ust. 1 lit. c RODO, jeżeli wynika to z obowiązków prawnych ciążących na pracodawcy. Na etapie zatrudnienia podstawą przetwarzania danych osobowych jest przede wszystkim niezbędność przetwarzania do wykonania stosunku pracy albo innego stosunku prawnego, wypełnienie obowiązków prawnych ciążących na administratorze oraz – w uzasadnionych przypadkach – prawnie uzasadniony interes administratora. Zgoda zatrudnionego nie powinna być traktowana jako domyślna podstawa przetwarzania danych w ramach zwykłych procesów kadrowych i delegowania.

W przypadku delegowania pracowników należy dodatkowo odróżnić dane zwykłe od szczególnych kategorii danych osobowych. Jeżeli w toku

delegowania pojawia się konieczność przetwarzania danych szczególnych kategorii, w szczególności danych o zdrowiu, administrator powinien dysponować nie tylko podstawą z art. 6 RODO, ale również odpowiednią przesłanką z art. 9 ust. 2 RODO. Dotyczy to przykładowo sytuacji związanych z medycyną pracy, oceną zdolności do pracy, obowiązkami BHP lub organizacją świadczeń zdrowotnych za granicą. Niedopuszczalne jest rutynowe pozyskiwanie lub przekazywanie takich danych „na zapas".

Wybrane aspekty dodatkowe związane z delegowaniem pracowników w kontekście przetwarzania ich danych osobowych

Na potrzeby delegowania pracownika i potwierdzenia podlegania pod rodzimy system zabezpieczeń społecznych, z udziałem pracodawcy prowadzone jest postępowanie o wydanie dokumentu A1. Należy jednak pamiętać, że w toku właściwego postępowania Zakład Ubezpieczeń Społecznych może żądać szeregu informacji na temat pracownika, które wykraczają poza standardowy katalog; podobnie rzecz ma się w przypadku kwestii związanych z rezydencją podatkową delegowanej osoby (np. dane dot. sytuacji rodzinnej, niezbędne celem ustalenia ośrodka interesów życiowych).

W takich przypadkach pracodawca powinien każdorazowo ocenić, czy zakres danych przekazywanych do organu, kontrahenta lub systemu rejestracyjnego jest adekwatny i niezbędny do realizacji konkretnego obowiązku prawnego. Dotyczy to w szczególności danych dotyczących sytuacji rodzinnej, rezydencji podatkowej, ubezpieczenia społecznego, dokumentów pobytowych oraz dokumentów tożsamości.

Zagraniczne systemy dotyczące delegowania, zgłaszania i ewidencjonowania pracowników delegowanych (np. francuski SIPSI, belgijska LIMOSA, holenderski Posted Workers, jak również systemy obowiązujące w innych państwach przyjmujących) mogą wymagać podania danych wykraczających poza standardowy katalog kadrowy. W każdym takim przypadku pracodawca powinien ustalić podstawę prawną przekazania danych, zakres wymaganych informacji, okres ich przechowywania oraz to, czy wymagane jest jedynie podanie danych identyfikacyjnych czy również przekazanie kopii dokumentów. W praktyce systemy prawne państw przyjmujących mogą wymagać przedstawienia określonych dokumentów dotyczących delegowanych pracowników, w tym dokumentów tożsamości, dokumentów pobytowych, formularzy A1, umów o pracę, ewidencji czasu pracy, pasków płacowych albo dowodów wypłaty wynagrodzenia. Każdorazowo należy jednak ustalić, czy konieczne jest jedynie okazanie dokumentu, podanie z niego określonych danych, czy też sporządzenie i przechowywanie jego kopii. W każdym przypadku delegowania pracowników pracodawca powinien stosować zasadę minimalizacji danych, zasadę ograniczenia celu oraz zasadę ograniczenia przechowywania. Oznacza to, że nie należy przekazywać zagranicznemu kontrahentowi ani pracodawcy użytkownikowi szerszego zakresu danych niż rzeczywiście wymagany przez przepisy lub niezbędny dla organizacji pracy, bezpieczeństwa, legalności zatrudnienia i realizacji obowiązków kontrolnych.

PRZYKŁADY PRAKTYCZNE

Ogólne zasady w zakresie delegowania pracowników do zagranicznego kontrahenta

W przypadku delegowania pracowników do zagranicznego kontrahenta pracodawca delegujący powinien każdorazowo zweryfikować obowiązki wynikające z przepisów państwa przyjmującego, w szczególności

dotyczące zgłoszenia delegowania, warunków zatrudnienia oraz przechowywania i udostępniania dokumentacji. Na potrzeby ewentualnej kontroli należy zapewnić dostępność dokumentów potwierdzających legalność i warunki delegowania, takich jak w szczególności: umowa o pracę, dokumenty płacowe, ewidencja czasu pracy, dowody wypłaty wynagrodzenia, dokumenty zgłoszeniowe oraz formularz A1. Dokumenty powinny być dostępne w miejscu wykonywania pracy lub w innej formie wymaganej przez prawo państwa przyjmującego, w tym cyfrowo. Zakres dokumentów, język, sposób ich przechowywania, obowiązek wyznaczenia osoby kontaktowej oraz okres przechowywania po zakończeniu delegowania mogą różnić się w zależności od państwa. Dlatego przed rozpoczęciem delegowania należy potwierdzić lokalne wymogi oraz ustalić z zagranicznym kontrahentem zasady współpracy w razie kontroli.

Paszporty, dowody osobiste, wizy i dokumenty pobytowe

Przekazywanie kopii paszportów albo innych dokumentów tożsamości delegowanych pracowników nie powinno mieć charakteru automatycznego. Pracodawca powinien najpierw ustalić, czy z przepisów państwa przyjmującego rzeczywiście wynika obowiązek posiadania kopii dokumentu, czy wystarczające jest okazanie dokumentu do wglądu, odnotowanie jego numeru albo potwierdzenie tożsamości pracownika w inny sposób. Jeżeli kopia dokumentu jest rzeczywiście wymagana, należy ograniczyć zakres przetwarzania do minimum, ustalić odbiorcę danych, okres przechowywania oraz zasady zabezpieczenia dokumentu. Szczególną ostrożność należy zachować przy dokumentach zawierających dane zbędne dla celu identyfikacji lub legalności zatrudnienia, w szczególności gdy przepisy wymagają jedynie weryfikacji dokumentu albo odnotowania określonych danych, a nie sporządzenia pełnej kopii.

Organizacja dokumentacji u zagranicznego kontrahenta

Jeżeli polski pracodawca deleguje ekipę instalatorów do realizacji usługi w Holandii, powinien jeszcze przed rozpoczęciem pracy ustalić, kto będzie osobą kontaktową dla Netherlands Labour Authority, gdzie będą przechowywane dokumenty oraz w jaki sposób będą one udostępniane na potrzeby kontroli. Dokumenty nie muszą być wyłącznie w formie papierowej, ale powinny być dostępne bezpośrednio w miejscu pracy albo w wersji cyfrowej możliwej do niezwłocznego okazania. Obejmuje to m.in. umowy o pracę, paski płacowe, zestawienia godzin pracy, formularze A1 oraz dowody płatności, które powinny pozostawać dostępne przez 5 lat po zakończeniu pracy.

Zakres danych dla pracodawcy użytkownika lub odbiorcy usługi

Jeżeli pracownicy wykonują pracę na terenie zakładu zagranicznego klienta, klient może mieć obowiązek weryfikacji tożsamości osób wykonujących pracę na jego terenie lub prowadzenia określonej ewidencji. Nie oznacza to jednak automatycznie, że polski pracodawca powinien przekazać pełne kopie paszportów wszystkich pracowników. W zależności od modelu zatrudnienia i obowiązków danego podmiotu może wystarczyć wgląd do oryginału dokumentu,

odnotowanie wymaganych danych albo prowadzenie ewidencji obejmującej m.in.: imię i nazwisko, datę urodzenia, obywatelstwo, rodzaj i numer dokumentu oraz okres jego ważności.

Pracownik delegowany spoza EOG

Jeżeli delegowany pracownik nie jest obywatelem państwa EOG lub Szwajcarii, pracodawca oraz podmiot korzystający z jego pracy powinni dodatkowo zweryfikować, czy dana osoba jest uprawniona do wykonywania pracy w ramach oddelegowania. W takim przypadku obowiązki dokumentacyjne mogą być dalej idące niż przy obywatelach UE, a przetwarzanie danych z dokumentów pobytowych lub zezwoleń na pracę może być niezbędne do wykazania legalności zatrudnienia.

Podsumowanie

Delegowanie pracowników w ramach świadczenia usług wiąże się nie tylko z obowiązkami z zakresu prawa pracy, ubezpieczeń społecznych i przepisów państwa przyjmującego, ale także z koniecznością prawidłowego ukształtowania zasad przetwarzania danych osobowych. Pracodawca delegujący powinien każdorazowo ustalić swoją rolę oraz rolę zagranicznego kontrahenta lub pracodawcy użytkownika, dobrać właściwą podstawę przetwarzania danych, ograniczyć zakres przekazywanych informacji do minimum oraz zweryfikować szczególne wymogi dokumentacyjne obowiązujące w państwie przyjmującym. Dotyczy to zwłaszcza danych zawartych w dokumentach tożsamości, dokumentach pobytowych, formularzach A1, ewidencji czasu pracy oraz dokumentacji płacowej. W praktyce zgodność z RODO w procesie delegowania wymaga połączenia zasady minimalizacji danych z obowiązkami kontrolnymi i dokumentacyjnymi wynikającymi z prawa państwa przyjmującego.

III LEGALIZACJA ZATRUDNIENIA OBYWATELI PAŃSTW TRZECICH

Jednym z rodzajów usług świadczonych przez agencje zatrudnienia jest wykonywanie czynności z zakresu legalizacji pobytu i zatrudnienia obywateli państw trzecich.

Po dokonaniu legalizacji obywatele ci mogą m.in.:

- zostać zatrudnieni przez agencję zatrudnienia jako pracownicy tymczasowi, świadczący pracę na terenie Polski na rzecz polskich pracodawców użytkowników;

- zostać zatrudnieni bezpośrednio przez pracodawców, którzy jako kontrahenci agencji zlecili jej przeprowadzenie procedur legalizacyjnych.

Należy przyjąć, że w przypadkach, gdy agencja sama zatrudnia cudzoziemca, dla którego uprzednio realizowała czynności z zakresu legalizacji, działa jako **administrator jego danych osobowych**. Z kolei w przypadku, gdy agencja działa na zlecenie swojego kontrahenta, który po zakończeniu procedury legalizacji zatrudnia cudzoziemca, wówczas działa jako **podmiot przetwarzający (procesor)**.

Biorąc pod uwagę fakt, że większość czynności realizowanych jest na etapie poprzedzającym zatrudnienie danego cudzoziemca, jako podstawę przetwarzania danych osobowych w procesie legalizacji pobytu i pracy można wskazać:

- wypełnienie obowiązku prawnego spoczywającego na administratorze (art. 6 ust. 1 lit. c RODO).

Oczywiście, tak jak w każdym innym przypadku, również w przypadku legalizacji należy w stosunku do cudzoziemca spełnić obowiązek informacyjny, wskazując w nim w szczególności kategorie odbiorców danych osobowych (tj. właściwe organy administracji publicznej).

W praktyce wielokrotnie zdarza się, że cudzoziemcy nie są rekrutowani bezpośrednio przez agencje zatrudnienia, lecz „przekazywani" im przez zagranicznych pośredników. W takim kontekście należy pamiętać o wymogu wskazania źródła pochodzenia danych osobowych.

Podczas działań legalizacyjnych nie można wykluczyć sytuacji, w której agencja zatrudnienia działa w imieniu swojego klienta, a przedmiotem świadczonej przez nią usługi będzie np. wyłącznie przygotowanie (wypełnienie) właściwych dokumentów legalizacyjnych czy też reprezentowanie klienta w toku właściwego postępowania legalizującego pracę na terenie Polski – przy czym podmiotem zatrudniającym cudzoziemca pozostaje klient. W takim wypadku, mimo że agencja posiada dane osobowe cudzoziemca, działa ona w charakterze podmiotu przetwarzającego. Występuje bowiem w imieniu klienta, który określa cele przetwarzania powierzonych jej danych osobowych. W takim wypadku konieczne jest zawarcie z klientem umowy o powierzeniu przetwarzania danych osobowych.

Po zakończeniu etapu związanego z legalizacją (a czasem jeszcze w jego trakcie) dochodzi do zatrudnienia cudzoziemca. Wówczas agencja zatrudnienia nadal występuje w roli administratora jego danych osobowych, z tym że wtedy już jako podmiot zatrudniający.

III REFERENCJE

Podstawowym warunkiem legalności pozyskiwania opinii o osobie ubiegającej się o zatrudnienie jest **uzyskanie zgody kandydata**, ponieważ to kandydat powinien być podstawowym źródłem informacji na temat przebiegu jego kariery zawodowej. Uzyskując takie informacje bez zgody kandydata, pracodawca naraża się na zarzut naruszenia przepisów o ochronie danych osobowych oraz dóbr osobistych kandydata. Podjęcie decyzji o niezatrudnieniu kandydata na podstawie niepotwierdzonych lub nieskonfrontowanych z kandydatem informacji może naruszyć dobre imię i prywatność kandydata, stanowić akt dyskryminacji, a w efekcie skutecznie utrudnić kandydatowi znalezienie nowego zatrudnienia.

W tym miejscu należy podkreślić, że udostępnienie pisemnych referencji przez kandydata nie stanowi automatycznie zgody na kontakt z byłym pracodawcą w celu uzyskania opinii o kandydacie. Należy więc zadbać, by kandydat udzielił na to wyraźną, dodatkową zgodę.

Kontakt z byłym pracodawcą w celu uzyskania referencji wiąże się ponadto z przetwarzaniem danych osoby, do której zwracamy się z zapytaniem o udzielenie referencji o kandydacie. Wobec tej osoby należy wykonać obowiązek informacyjny (np. wysyłając wiadomości e-mail ze stosownym dokumentem lub linkiem do dokumentu zawierającego wymagane klauzule). **Ważne jest, żeby uzyskać zgodę kandydata na pozyskanie referencji od danego podmiotu w formie dokumentowej** (np. e-mail, formularz elektroniczny), co pozwoli właściwie udokumentować cały proces. Powyższa rekomendacja wynika z faktu, że proces pozyskiwania referencji powinien być transparentny, a osoba ubiegająca się o zatrudnienie na każdym jego etapie powinna mieć dostęp do informacji, do jakiego podmiotu i w jakim zakresie kierowane są pytania o przebieg jej zatrudnienia.

Krótkiego komentarza wymaga użyte w art. 22^1 § 1 pkt 6 Kodeksu Pracy sformułowanie „przebieg zatrudnienia". W ocenie Sądu Najwyższego pojęcie to należy rozumieć szeroko – nie tylko jako zatrudnienie na podstawie umowy o pracę, ale również na podstawie umów cywilnoprawnych. Wobec powyższego przyjąć należy, że referencje mogą dotyczyć również okresów świadczenia pracy na podstawie umów prawa cywilnego.

Przetwarzanie danych zawartych w referencjach powinno zasadniczo dotyczyć przebiegu dotychczasowego zatrudnienia kandydata, przy czym pracodawcy muszą zachować ostrożność i stosować się do pewnych zasad. Ocenie powinny podlegać przede wszystkim fakty dotyczące przebiegu dotychczasowego zatrudnienia kandydata (np. weryfikacja doświadczenia zawodowego), a nie subiektywne i trudne do weryfikacji oceny byłych współpracowników dotyczące współpracy z kandydatem, dane prywatne czy tym bardziej dane wrażliwe.

Należy podkreślić, że kandydat nie ma prawnego obowiązku udostępniania referencji przyszłemu pracodawcy i z jego odmowy w tym względzie nie powinny być stosowane wobec niego negatywne konsekwencje w procesie rekrutacyjnym. Jeżeli pracodawca otrzyma od kandydata zapytanie z prośbą o wyjaśnienie wpływu pozyskanych referencji na wynik rekrutacji, powinien odpowiedzieć na to pytanie w sposób transparentny i zrozumiały, z poszanowaniem zasad wynikających z Kodeksu pracy oraz z RODO.

1 Wyrok SN z 11.1.2017 r., I PK 25/16

III TESTY W REKRUTACJI

Zgodnie z definicją zawartą w Słowniku Języka Polskiego PWN (sjp.pwn.pl) „testowanie" oznacza poddawanie kogoś testowi. Sam test definiowany jest przez ww. słownik jako zestaw pytań lub zadań służących m.in. sprawdzeniu wiedzy. W praktyce powszechne jest dążenie pracodawców do weryfikacji przydatności kandydata do pracy różnymi metodami, w tym za pomocą testów. Pracodawcy chcą w praktyczny sposób sprawdzić umiejętności kandydatów przed ich zatrudnieniem, tak aby wybrać, według obiektywnych kryteriów, kandydata najlepiej dopasowanego do danej roli. Wykorzystanie testów daje także pracodawcom oszczędność czasu i kosztów umożliwiając szybszą i trafniejszą identyfikację najlepszych kandydatów.

Po omówieniu definicji oraz celów wykorzystania testów w rekrutacji warto wskazać i pogrupować ich poszczególne rodzaje.

Testy wiedzy

Mogą przybrać formę uporządkowanego zestawu pytań, ankiet z pytaniami merytorycznymi, a także zadań praktycznych, których wspólnym mianownikiem jest ocena wiedzy kandydata z danego obszaru. Testy wiedzy wykorzystywane są m.in. w rekrutacjach do działów finansowych, prawnych oraz podatkowych.

Testy manualne

W przypadku pracowników fizycznych testem manualnym będą praktyczne próbki pracy polegające na wykonaniu konkretnych czynności zawodowych, w celu oceny umiejętności, dokładności oraz sprawności kandydatów. Do realizacji testów manualnych wykorzystuje się również różnego rodzaju aparatury.

Testy językowe

Są szczególną kategorią testów oceniających znajomość języków obcych. Obecnie najczęściej spotykamy się z rozmową pomiędzy rekruterem a kandydatem, w trakcie której sprawdzana jest znajomość języka obcego. Forma ta w znacznej mierze wyparła pisemną formę rozwiązywania zadań.

Testy umiejętności, symulacje

W odróżnieniu od testów wiedzy, testy umiejętności mają na celu sprawdzenie, czy kandydat potrafi zastosować swoją wiedzę w praktyce. Test umiejętności może przybrać formę rozwiązania zadania praktycznego (np. sporządzenia umowy lub przygotowania prezentacji), a także symulacji konkretnej sytuacji lub zadania wykonywanego w czasie rzeczywistym.

Testy osobowościowe

Narzędzie to pozwala na ocenę osobowości kandydata. Na bardziej szczegółowym poziomie testy te mają ocenić naturalne wzorce zachowań kandydata i cechy charakteru przyszłego pracownika. Pracodawcy decydują się na zastosowanie tego rodzaju testów, aby jeszcze przed zatrudnieniem poznać pożądane cechy kandydata. Najczęściej dążą do ustalenia, jak pracownik radzi sobie w sytuacjach stresowych, jaki ma styl komunikacji lub jaka jest jego zdolność do podejmowania decyzji oraz elastyczność poznawcza.

Testy psychologiczne

Możliwość stosowania niektórych profesjonalnych testów psychologicznych jest ograniczona do specjalistów posiadających wykształcenie psychologiczne. Dla niektórych kategorii testów psychologicznych istnieje wymóg interpretacji przez psychologa, czyli osobę posiadającą odpowiednie przygotowanie merytoryczne. Ponadto na rynku występują podmioty zajmujące się dystrybucją specjalistycznych testów, które często ograniczają krąg podmiotów uprawnionych do ich zakupów oraz wymagają posiadania odpowiednich kwalifikacji do korzystania z tych narzędzi (np. odbycia kursów uprawniających do korzystania z danej metody). Przepisy dotyczące zawodu psychologa oraz samorządu zawodowego psychologów gwarantują poszanowanie prywatności, godności osobistej ocenianej osoby a także zobowiązanie psychologa do ochrony danych osobowych uzyskanych w związku z wykonywaniem czynności.

W poprzednim stanie prawnym, tj. na gruncie Ustawy z dnia 20 kwietnia 1997 r. o promocji zatrudnienia i instytucjach rynku pracy[1], możliwość korzystania z narzędzi wspomagających proces rekrutacji i selekcji kandydatów wynikała z art. 18 tej ustawy, mieszcząc się w definicji doradztwa personalnego polegającego w szczególności na weryfikacji kandydatów pod względem oczekiwanych przez pracodawcę kwalifikacji i predyspozycji. Działalność ta była zarezerwowana tylko dla agencji zatrudnienia. Aktualnie czynności służące doborowi kandydatów do pracy nie stanowią odrębnie uregulowanej czynności w Ustawie z dnia 20 marca 2025 r. o rynku pracy i służbach zatrudnienia[2]. Działania te należy traktować jako element procesu pozyskiwania kandydatów do pracy oraz przekazywania pracodawcy informacji o kandydatach, o których mowa w art. 81 ust. 1 i ust. 2 pkt 2 ww. ustawy.

Zakres badania przydatności kandydata powinien ograniczać się do niezbędnych kompetencji, predyspozycji i umiejętności niezbędnych na stanowisku, o które się ubiega. Weryfikacja kandydata w zakresie wykraczającym poza te obszary wykracza poza dozwolony prawem zakres. Żaden akt prawny nie reguluje wprost możliwości stosowania testów w rekrutacji. Kluczowy jest jednak art. 5 RODO, który określa zasady przetwarzania danych osobowych. Pracodawcy powinni przeanalizować każdą z nich przed wdrożeniem wybranego rodzaju testu – zarówno na etapie rekrutacji, jak i w trakcie zatrudnienia pracownika.

Oceniając możliwość poddawania kandydatów do pracy różnego rodzajom testom nie sposób nie odnieść się do art. 22^1 Kodeksu pracy, który określa katalog danych, jakich może żądać pracodawca od kandydatów do pracy oraz pracowników. W wyniku przeprowadzenia testu agencja lub pracodawca wejdzie w posiadanie wyników testów lub egzaminu, które wskażą na informacje lub opinie dotyczące danej osoby, w tym przeszłe, obecne czy przyszłe predyspozycje. Należy ostrożnie rozważyć, czy wyniki testów mieszczą się w jednej z kategorii wymienionych przez ustawodawcę, zwracając uwagę na to, czy można je zakwalifikować jako dane dotyczące kwalifikacji zawodowych.

W zależności od rodzaju zastosowanego testu może dojść do przetwarzania danych zwykłej kategorii, na podstawie art. 6 ust. 1 RODO, lub danych szczególnych kategorii na podstawie art. 9 ust. 2 RODO. W sytuacji, gdy pracodawcy przeprowadzają testy językowe, manualne czy wiedzy, można przypuszczać, że wejdą oni w posiadanie danych osobowych zwykłej kategorii. Podstawą przetwarzania danych osobowych może być art. art. 6 ust. 1 lit. f RODO, który mówi o przetwarzaniu takich danych ze względu na niezbędność ce-

1 Dz.U. z 2025 r. poz. 214
2 Dz.U. z 2025 r. poz. 620

lów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Rozważając możliwość skorzystania z tej podstawy prawnej, należy przeprowadzić test proporcjonalności, czyli zestawić interesy realizowane przez pracodawcę (administratora danych) z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą.

Dla niektórych zawodów, takich jak służba w Policji czy Straży Pożarnej, udział w badaniach psychologicznych w postępowaniu kwalifikacyjnym lub w trakcie służby wynika wprost z przepisów prawa. W takich przypadkach badania te stanowią warunek dopuszczenia do wykonywania obowiązków służbowych. Z kolei w sytuacji, gdy obowiązek przeprowadzenia testów psychologicznych nie wynika z przepisów prawa a pracodawcy decydują się na przeprowadzenie testów psychologicznych lub osobowościowych z własnej inicjatywy, muszą oni ocenić, czy tego rodzaje dane osobowe są niezbędne do oceny predyspozycji kandydata do pracy, a także rozważyć, na jakiej podstawie prawnej przetwarzać dane osobowe pozyskane w wyniku testów. Jeżeli w ramach testów dochodzi do przetwarzania danych osobowych szczególnej kategorii, należy w szczególności przeanalizować możliwości oparcia przetwarzania na zgodzie osoby, której dane dotyczą. Pracodawcy powinni zwrócić także uwagę na dobrowolność udziału kandydata w testach, w wyniku których dojdzie do przetwarzania danych osobowych szczególnej kategorii. Zgoda pracownika powinna być uprzednia, świadoma i jednoznaczna, a jej udzielenie nie może wynikać z relacji podporządkowania. Odmowa udziału w badaniu nie powinna prowadzić do negatywnych konsekwencji dla pracownika, w szczególności w zakresie zatrudnienia lub warunków pracy.

Dotychczasowe stanowisko UODO wskazujące na zakaz przeprowadzania testów wobec kandydatów do pracy (o ile obowiązek ten nie wynika z przepisów ustawy), w obliczu współczesnych wyzwań i możliwości oferowanych przez rynkowe narzędzia wydaje się wymagać aktualizacji. Celem agencji pracy jest pomoc pracodawcom w wyborze odpowiednich kandydatów, a dostępne na rynku testy w znacznym stopniu odpowiadają potrzebom obu tych grup. Zbyt restrykcyjne podejście organów państwa do współczesnych wyzwań rynku pracy może nie spełniać funkcji ochronnej wobec kandydata.

Decydując się na stosowanie testów w procesach rekrutacyjnych, pracodawca powinien przeanalizować kilka kluczowych kwestii. Rodzaj testu determinuje bowiem to, z jakiego rodzaju danymi osobowymi będziemy mieli do czynienia (dane zwykłe czy dane szczególnej kategorii). Stosowanie testów wiedzy może pozwolić uniknąć przetwarzania danych szczególnej kategorii.

Kolejnym istotnym elementem jest właściwy dobór testów do konkretnego stanowiska oraz niestosowanie narzędzi, które nie są pracodawcy potrzebne do oceny kwalifikacji lub predyspozycji kandydata do pracy.

IV Główne obowiązki administratora danych

Główne obowiązki wobec osób, których dane dotyczą:

- spełnianie obowiązku informacyjnego wobec osoby, której dane są gromadzone;
- zapewnienie możliwość realizacji praw osób, których dane dotyczą;
- zawiadomienie o naruszeniu ochrony danych osoby, której dane dotyczą, jeżeli wiąże się to dla niej z wysokim ryzykiem naruszenia praw i wolności.

Jeżeli naruszenie ochrony danych osobowych spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi również zawiadomić osoby, których dane dotyczą. Odstąpić od tego obowiązku można wyłącznie w sytuacjach wskazanych w przepisach, tj.:

- gdy administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, np. poprzez zaszyfrowanie danych w sposób zapewniający ich bezpieczeństwo;
- gdy administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
- gdy takie zawiadomienie wymagałoby niewspółmiernie dużego wysiłku (co należy ustalać przy uwzględnieniu kosztu zawiadomienia oraz potencjalnych strat związanych z jego brakiem), przy czym w takim przypadku administrator musi wydać publiczny komunikat lub zastosować podobny środek tak, aby osoby, których dane zostały ujawnione, zostały poinformowane o naruszeniu w równie skuteczny sposób.

Główne obowiązki wobec Prezesa Urzędu Ochrony Danych:

- zgłoszenie inspektora ochrony danych, jeżeli był powołany;
- zgłoszenie wystąpienia naruszenia ochrony danych osobowych.

Zgodnie z art. 4 pkt 12 RODO, poprzez naruszenie ochrony danych osobowych rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, jednak nie później niż w terminie 72 godzin od stwierdzenia naruszenia, ma obowiązek zgłosić je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W tym miejscu warto zwrócić uwagę, że zgłoszenie może być sukcesywnie uzupełniane w toku podjętych działań, jeżeli administrator uzyskał dodatkowe in-

formacje. Kluczowe wydaje się, by we wskazanym powyżej terminie poinformować organ o zaistniałym zdarzeniu, nawet jeżeli nie posiadamy pełnego obrazu sytuacji i kompletu informacji.

Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Obowiązek zapewnienia bezpieczeństwa przetwarzanym danym osobowym poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, które pozwolą przetwarzać dane osobowe zgodnie z przepisami prawa

Obejmuje on m.in.:

- przyjęcie odpowiednich polityk ochrony danych osobowych;
- zawieranie stosownych umów związanych z przetwarzaniem danych osobowych, w szczególności umów powierzenia przetwarzania danych osobowych;
- nadawanie upoważnień do przetwarzania danych osobowych;
- szkolenie personelu z zakresie zagadnień związanych z przetwarzaniem danych osobowych;
- stosowanie odpowiednich zabezpieczeń technicznych, takich jak pseudonimizacja czy szyfrowanie.

Pozostałe obowiązki administratora danych osobowych

1. Powołanie inspektora ochrony danych, jeżeli taki obowiązek wynika z przepisu (art. 37 RODO).

Inspektor ochrony danych (IOD) to osoba wyznaczona przez administratora, której głównym zadaniem jest dbanie o zgodność przetwarzania danych osobowych z przepisami dotyczącymi ochrony danych, w tym RODO. Inspektor pełni funkcję doradczą i nadzorczą w zakresie ochrony danych osobowych, wspierając agencję w przestrzeganiu odpowiednich przepisów oraz zapewniając, że prawa osób, których dane dotyczą, są chronione. IOD zobowiązany jest do zachowania tajemnicy lub poufności co do wykonywanych przez siebie zadań. Inspektorem ochrony danych nie może być osoba prawna, np. spółka. Zawsze musi to być konkretna osoba fizyczna.

Obowiązek powołania IOD powstaje, gdy:

- przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę,
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

2. Dokonywanie oceny ryzyka związanego z przetwarzaniem danych osobowych i jego monitorowanie, a także przeprowadzenie oceny skutków dla ochrony danych, jeżeli zachodzi duże prawdopodobieństwo naruszenia praw i wolności osób, których dane są przetwarzane.

3. Kierowanie się podstawowymi zasadami dotyczącymi przetwarzania danych osobowych, w tym m.in. zasadą minimalizacji, zasadą adekwatności lub zasadą ograniczonego przechowywania, a także możliwość wykazania, że przetwarzanie ma miejsce.

4. Zapewnienie, aby przetwarzanie danych osobowych odbywało się w oparciu przesłanki legalizujące takie działanie.

5. Prowadzenie rejestru czynności przetwarzania danych osobowych.

Rejestry czynności przetwarzania oraz kategorii czynności muszą być prowadzone przez agencje, które spełniają przynajmniej jedno z poniższych kryteriów:

- zatrudniają ponad 250 osób;
- w ich przypadku przetwarzanie danych wiąże się z ryzykiem naruszenia praw i wolności osób, których dane dotyczą;
- przetwarzanie danych nie jest sporadyczne;
- przetwarzane są szczególne kategorie danych osobowych lub dane dotyczące wyroków skazujących i czynów zabronionych.

Rejestr czynności powinien zawierać m.in. następujące informacje:

- dane administratora lub podmiotu przetwarzającego (określenie, kto przetwarza dane osobowe);
- cel przetwarzania;
- wskazanie, czyje dane są przetwarzane oraz jaki jest ich zakres;
- określenie, komu dane są ujawniane oraz czy są przekazywane do państwa trzeciego lub organizacji międzynarodowych (wraz ze wskazaniem ich zabezpieczeń przy określonej podstawie prawnej transferu);
- okres przetwarzania danych oraz opis środków ich zabezpieczenia.

Zakres obligatoryjnych informacji w przypadku **rejestru kategorii czynności** jest nieco węższy niż w rejestrze czynności i obejmuje wskazanie:

- administratora danych;
- procesów, które są podejmowane w ramach przetwarzania danych;
- czy dane są przekazywane do państwa trzeciego lub organizacji międzynarodowych oraz jak są zabezpieczone (w przypadku określonej podstawy prawnej transferu).

Rejestry są prowadzone najczęściej w formie elektronicznej, co umożliwia bieżące aktualizowanie dokumentu zgodnie ze stanem faktycznym. Aktualizacja rejestrów jest konieczna w przypadku pojawienia się nowych procesów przetwarzania danych lub w sytuacji, gdy zachodzą zmiany w informacjach już umieszczonych w rejestrze.

6. Zapewnienie zgodności z przepisami przy przekazywaniu danych osobowych do państw spoza Europejskiego Obszaru Gospodarczego (EOG).

7. Zadbanie o stosowanie zasad privacy by design i privacy by default.

8. Przeprowadzenie i udokumentowanie tzw. testu równowagi.

Test równowagi jest obligatoryjny w przypadku przetwarzania danych osobowych w oparciu o uzasadniony interes administratora tj. na podstawie art. 6 ust 1 lit. f RODO. Przetwarzanie na tej podstawie jest zgodne z prawem, jeżeli jest ono niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych.

Elementy testu równowagi:

- ocena celu przetwarzania oraz identyfikacja uzasadnionego interesu lub interesów administratora, który ma stanowić przesłankę przetwarzania danych. Interesy, na które powołuje się administrator, muszą być zgodne z prawem, realne, aktualne oraz istotne na tyle, aby uzasadniać przetwarzanie danych osobowych (np. marketing bezpośredni, zapobieganie oszustwom oraz bezpieczeństwo sieci i informacji);

- ocena konieczności przetwarzania danych: administrator powinien określić czy przetwarzanie jest niezbędne do realizacji celu oraz czy celu nie można osiągnąć innymi środkami;

- ocena wpływu przetwarzania na osoby, których dane dotyczą – czyli w jakim stopniu przetwarzanie danych wpływa na te osoby;

- ocena środków ochrony i minimalizacji ryzyka – aby zapewnić równowagę, należy wdrożyć środki ochrony minimalizujące ryzyko dla prywatności osoby, której dane dotyczą.

Kryteria testu mogą być uzupełniane o dodatkowe czynniki. Przeprowadzenie testu powinno być udokumentowane.

V AI w działalności agencji zatrudnienia i podmiotów HR

Czym jest sztuczna inteligencja (AI)

W rozumieniu art. 3 AI Act[1] system AI „oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne".

Oznacza to, że system AI analizuje dane, uczy się na ich podstawie i generuje rekomendacje lub decyzje mogące wpływać na sytuację osób, których dotyczą wyniki jego działania.

Systemy AI różnią się od klasycznych systemów informatycznych w szczególności tym, że:

- posiadają zdolność do wnioskowania, rozumianą jako zdolność systemu do przetwarzania danych wejściowych i generowania wyników w postaci prognoz, rekomendacji, treści lub rozstrzygnięć, które wywierają wpływ na decyzje lub działania podejmowane poza systemem;
- cechuje je autonomia działania, polegająca na zdolności do realizowania określonych zadań bez każdorazowej, bezpośredniej ingerencji człowieka, w granicach wyznaczonych celem systemu i przyjętymi parametrami;
- wykazują zdolność do adaptacji, ponieważ model może zmieniać swoje zachowanie w czasie na podstawie danych historycznych lub bieżących, co może prowadzić do modyfikacji sposobu generowania wyników.

Za systemy AI nie uznaje się systemów informatycznych działających wyłącznie w oparciu o z góry zdefiniowane reguły i scenariusze, przeznaczonych do automatycznego wykonywania ściśle określonych czynności. Przykładem takich systemów mogą być w szczególności: systemy workflow automatyzujące obieg zadań według ustalonych statusów, systemy RPA (robotic process automation) odtwarzające powtarzalne czynności użytkownika oraz systemy formularzowe i walidacyjne sprawdzające kompletność lub poprawność danych.

Przykładowe zastosowania AI w HR

Systemy AI mogą przynosić korzyści organizacyjne agencjom zatrudnienia oraz innym podmiotom świadczącym usługi HR, w szczególności w obszarze:

- automatycznej analizy CV i dokumentów aplikacyjnych;
- dopasowywania kandydatów do ofert pracy na podstawie profilu kompetencyjnego;
- wspierania podejmowania decyzji o zatrudnieniu lub awansie;

1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji, Dz.U. UE L 2024/1689 z 12.07.2024 r.)

- obsługi wstępnego kontaktu z kandydatami, w tym z wykorzystaniem chatbotów i voicebotów;
- przewidywania rotacji pracowników tymczasowych i ryzyka wcześniejszego zakończenia kontraktu;
- planowania obsady projektów oraz prognozowania zapotrzebowania kadrowego u klientów.

Kwalifikacja systemów AI w HR na gruncie AI Act

Zgodnie z AI Act systemy wykorzystywane w rekrutacji, selekcji, ocenie pracowników, przydzielaniu zadań oraz monitorowaniu pracy są co do zasady uznawane za systemy wysokiego ryzyka. Skutkuje to objęciem dostawców i podmiotów stosujących takie systemy podwyższonym reżimem obowiązków, w szczególności w zakresie zarządzania ryzykiem, nadzoru człowieka, dokumentacji, przejrzystości, monitorowania działania systemu oraz raportowania incydentów.

W praktyce każda agencja zatrudnienia powinna przed wdrożeniem narzędzia AI zweryfikować, czy stanowi ono system wysokiego ryzyka oraz czy spełnia wymagania wynikające z AI Act. AI Act przewiduje również kategorię systemów zakazanych, do których należą m.in. systemy manipulujące zachowaniem osób lub wykorzystywane do tzw. social scoring. W obszarze HR szczególnej ostrożności wymaga stosowanie narzędzi analizujących emocje, cechy osobowości czy mikroekspresję twarzy, ponieważ ich użycie może prowadzić do naruszeń prawa oraz dyskryminacji.

Główne role na gruncie AI Act i wynikające z nich obowiązki

Dostawca systemu AI

Na gruncie AI Act dostawcą systemu AI jest podmiot, który opracowuje system AI lub zleca jego opracowanie oraz – odpłatnie lub nieodpłatnie – wprowadza go do obrotu lub oddaje do użytku pod własną nazwą lub znakiem towarowym.

Podstawowe obowiązki dostawcy systemu AI obejmują w szczególności:

1. zapewnienie zgodności systemu z ogólnymi wymogami AI Act;
2. dokonanie klasyfikacji systemu pod kątem ryzyka;
3. zapewnienie przejrzystości, w tym przekazanie informacji o interakcji z systemem AI oraz odpowiednie oznakowanie jego wyników.

Dodatkowo, w zależności od rodzaju systemu, dostawca może być zobowiązany do podjęcia dalszych działań:

4. w przypadku **systemów ogólnego przeznaczenia** obowiązki te obejmują w szczególności:

- sporządzenie dokumentacji technicznej modelu oraz informacji potrzebnych do integracji modelu;
- wprowadzenie polityki zapewniającej zgodność z prawem autorskim;
- sporządzenie i podanie do publicznej wiadomości informacji dotyczących treści wykorzystanych do trenowania modelu.

5. z kolei, w **przypadku systemów wysokiego ryzyka** dostawca powinien w szczególności:

- wdrożyć i obsługiwać system zarządzania ryzykiem;
- sporządzić dokumentację techniczną dla systemu AI;
- zapewnić mechanizm rejestrowania zdarzeń;
- zapewnić przejrzystość oraz przekazać podmiotom stosującym instrukcję obsługi;
- zapewnić mechanizmy nadzoru człowieka;
- przeprowadzić ocenę zgodności przed wprowadzeniem systemu na rynek;
- prowadzić rejestry działania systemu;
- monitorować system po wdrożeniu;
- zgłaszać poważne incydenty organom nadzorczym.

Podmiot stosujący system AI

Podmiotem stosującym system AI jest podmiot wykorzystujący system AI w ramach działalności niebędącej osobistą działalnością pozazawodową, a zarazem sprawujący nad nim kontrolę.

Do kluczowych obowiązków podmiotu stosującego należą:

1. poinformowanie osób, wobec których stosowane są systemy rozpoznawania emocji lub kategoryzacji biometrycznej, o fakcie ich stosowania i przetwarzania ich danych. Niezależnie od realizacji obowiązku informacyjnego należy przy tym uwzględnić okoliczność, że możliwość stosowania systemów rozpoznawania emocji i kategoryzacji biometrycznej jest istotnie ograniczona w związku z treścią art. 5 AI Act. Zgodnie z tym przepisem zakazane jest w szczególności stosowanie systemów AI służących do wnioskowania o emocjach osób fizycznych w obszarze miejsca pracy, z wyjątkiem zastosowań medycznych lub związanych z bezpieczeństwem. Zakazana jest również kategoryzacja biometryczna osób fizycznych na podstawie ich danych biometrycznych, jeżeli służy dedukowaniu lub wnioskowaniu o cechach szczególnie chronionych, takich jak rasa, poglądy polityczne, przynależność związkowa, przekonania religijne lub światopoglądowe, życie seksualne lub orientacja seksualna, przy czym zakaz ten nie obejmuje w szczególności etykietowania lub filtrowania zgodnie z prawem pozyskanych zbiorów danych biometrycznych, takich jak obrazy, jak również kategoryzowania danych biometrycznych w obszarze ścigania przestępstw;

2. ujawnienie, że obrazy, treści audio lub wideo stanowiące deepfake zostały sztucznie wygenerowane lub zmanipulowane, a także – w odpowiednich przypadkach – ujawnienie tego samego w odniesieniu do tekstu publikowanego w celu informowania społeczeństwa o sprawach leżących w interesie publicznym;

3. w przypadku systemów wysokiego ryzyka – stosowanie środków technicznych i organizacyjnych w celu zapewnienia wykorzystywania systemu zgodnie z instrukcją;

4. zapewnienie nadzoru ludzkiego przez osoby o właściwych kompetencjach;

5. zapewnienie adekwatności i reprezentatywności danych wejściowych, w zakresie, w jakim podmiot sprawuje nad nimi kontrolę;

6. monitorowanie sposobu działania systemu AI, w tym zgłaszanie ryzyka działania systemu i – w razie potrzeby – zawieszenie jego działania;

7. poinformowanie przedstawicieli pracowników i samych pracowników, przed oddaniem do użytku lub wykorzystaniem systemu AI wysokiego ryzyka w miejscu pracy, że taki system będzie wobec nich stosowany.

Podstawowe wyzwania dla dostawców i podmiotów stosujących AI z perspektywy RODO

Wykorzystanie AI w działalności agencji zatrudnienia wiąże się z podwyższonym poziomem ryzyka naruszenia zasad ochrony danych osobowych. W świetle wymogów stawianych przez RODO kluczowe wyzwania obejmują w szczególności:

- legalność przetwarzania danych (art. 5 ust. 1 lit. a RODO) – dostawca lub podmiot stosujący system AI powinien zapewnić zgodność procesu przetwarzania danych osobowych z RODO oraz z innymi mającymi zastosowanie przepisami prawa, od etapu gromadzenia danych po ich wykorzystanie w ramach modelu AI;

- rzetelność przetwarzania danych (art. 5 ust. 1 lit. a RODO) – systemy AI powinny być projektowane i wykorzystywane w sposób gwarantujący poprawność, wiarygodność oraz niedyskryminujący charakter procesów przetwarzania i ich wyników;

- przejrzystość przetwarzania danych (art. 5 ust. 1 lit. a RODO) – osobom, których dane dotyczą, należy zapewnić zrozumiałe, sformułowane prostym językiem i łatwo dostępne informacje o wykorzystywaniu systemów AI w procesach przetwarzania danych osobowych, w tym o charakterze zautomatyzowanego przetwarzania oraz jego potencjalnych skutkach;

- ograniczenie celu i minimalizacja danych (art. 5 ust. 1 lit. b i c RODO) – systemy AI powinny przetwarzać dane osobowe wyłącznie w zakresie niezbędnym do realizacji jednoznacznie określonych i prawnie uzasadnionych celów, przy czym rodzaj oraz ilość danych powinny pozostawać adekwatne i niezbędne do osiągnięcia tych celów;

- w przypadku zautomatyzowanego przetwarzania danych, w tym profilowania, w rozumieniu art. 22 RODO – osobie, której dane dotyczą, należy przekazać jasne informacje dotyczące stosowania zautomatyzowanego przetwarzania, zasad i ogólnych mechanizmów działania systemu oraz znaczenia i przewidywanych skutków przetwarzania; konieczne jest również wdrożenie skutecznych mechanizmów nadzoru człowieka, umożliwiających wyrażenie stanowiska i zakwestionowanie decyzji;

- realizacja praw podmiotów danych – dostawca lub podmiot stosujący systemy AI powinien zapewnić skuteczne i terminowe wykonywanie praw osób, których dane dotyczą, określonych w art. 12–22 RODO, ze szczególnym uwzględnieniem prawa do informacji o przetwarzaniu danych osobowych, prawa do sprostowania lub usunięcia danych oraz prawa sprzeciwu wobec ich przetwarzania, w tym także gdy dane zostały wykorzystane do trenowania, testowania lub doskonalenia modeli AI. Korzystanie z systemów AI może w tym zakresie powodować szczególne trudności, w szczególności związane z identyfikacją zakresu wykorzystania konkretnych danych w modelu, wykazaniem ich skutecz-

nego usunięcia, koniecznością zastosowania mechanizmów „oduczania" lub ponownego trenowania modelu, a także ryzykiem wpływu takich działań na dokładność, integralność lub bezstronność systemu. Wymaga to wdrożenia procedur i środków techniczno-organizacyjnych umożliwiających realizację tych praw w sposób rzeczywisty, weryfikowalny i rozliczalny, a nie wyłącznie formalny.

Praktyczne aspekty związane z wdrożeniem systemu AI na gruncie AI Act i RODO

Dostosowanie sposobu wykorzystywania systemów AI do wymogów AI Act oraz RODO nie ogranicza się do formalnej oceny narzędzia. W praktyce wymaga ono podjęcia przez organizację szeregu działań o charakterze organizacyjnym, technicznym i dokumentacyjnym.

Rekomendowane działania przed wdrożeniem i w toku korzystania z systemu AI

Aby zapewnić zgodność z przepisami, agencja zatrudnienia oraz inne podmioty świadczące usługi HR powinny w szczególności:

- sprawdzić, czy używany system AI kwalifikuje się jako system wysokiego ryzyka;
- zweryfikować dostawcę, w tym ustalić, czy system posiada oznakowanie CE oraz dokumentację zgodności;
- przeprowadzić analizę ryzyka przed wdrożeniem systemu i wdrożyć środki ograniczające te ryzyka;
- zapewnić, aby decyzje podejmowane przy wsparciu AI podlegały realnemu nadzorowi człowieka;
- poinformować kandydatów i pracowników o stosowaniu systemów AI, jeżeli jest to wymagane;
- regularnie monitorować działanie systemu oraz testować go pod kątem ryzyka dyskryminacji;
- wdrożyć procedurę reagowania na błędne decyzje systemu oraz inne incydenty związane z jego działaniem.

Ocena skutków dla ochrony danych (DPIA) jako element wdrożenia systemu AI

W przypadku systemów wysokiego ryzyka stosowanych w HR co do zasady konieczne jest przeprowadzenie DPIA, czyli oceny skutków dla ochrony danych.

W praktyce oznacza to, że przed wdrożeniem systemu organizacja powinna:

- opisać sposób działania systemu;
- określić, jakie dane są przetwarzane;
- ocenić ryzyka dla kandydatów i pracowników;
- wskazać środki ograniczające zidentyfikowane ryzyka;
- udokumentować cały proces.

Jeżeli pomimo zastosowania odpowiednich środków ryzyko nadal pozostaje wysokie, przed wdrożeniem systemu może być konieczne przeprowadzenie konsultacji z organem nadzorczym.

Transfer danych poza EOG oraz ryzyko utraty kontroli nad danymi

Korzystanie z systemów AI, w szczególności z narzędzi chmurowych, modeli generatywnych lub rozwiązań oferowanych w formule SaaS, może wią-

zać się z przetwarzaniem danych osobowych poza Europejskim Obszarem Gospodarczym (EOG). W praktyce oznacza to, że dane kandydatów lub pracowników, takie jak CV, dane kontaktowe czy informacje o zatrudnieniu, mogą być przekazywane na serwery zlokalizowane w państwach trzecich. W takiej sytuacji zastosowanie znajdują przepisy rozdziału V RODO dotyczące transferu danych do państw trzecich, a organizacja powinna w tej sytuacji podjąć w szczególności następujące działania:

- sprawdzić, gdzie fizycznie przetwarzane są dane;
- ustalić, czy dostawca korzysta z podprocesorów spoza EOG;
- zapewnić odpowiednią podstawę transferu, np. decyzję stwierdzającą odpowiedni stopień ochrony lub standardowe klauzule umowne (SCC);
- przeprowadzić ocenę wpływu transferu na ochronę danych (Transfer Impact Assessment – TIA), jeżeli jest to wymagane.

Utrata kontroli nad danymi jako ryzyko związane ze stosowaniem systemów AI

Szczególne ryzyko związane ze stosowaniem systemów AI przez agencje zatrudnienia oraz inne podmioty świadczące usługi HR stanowi możliwość utraty kontroli nad danymi wprowadzanymi do tych systemów. Ryzyko to może wystąpić w szczególności w sytuacji, gdy:

- dane wprowadzane do systemu są wykorzystywane do dalszego trenowania modeli;
- brak jest jasnej informacji o okresie przechowywania danych;
- nie ma możliwości trwałego usunięcia danych z systemu;
- organizacja nie posiada wiedzy, kto faktycznie ma dostęp do danych.

W celu ograniczenia powyższego ryzyka organizacja powinna w szczególności:

- zweryfikować warunki korzystania z systemu, w tym postanowienia dotyczące dalszego wykorzystywania danych przez dostawcę;
- ustalić zasady przechowywania, usuwania oraz zwrotu danych po zakończeniu korzystania z usługi;
- potwierdzić, jakie podmioty i osoby mogą uzyskiwać dostęp do danych oraz na jakiej podstawie;
- ocenić, czy zakres danych wprowadzanych do systemu jest adekwatny i niezbędny z perspektywy celu ich przetwarzania;
- wprowadzić wewnętrzne zasady ograniczające wprowadzanie do systemów AI danych szczególnie wrażliwych lub nadmiarowych;
- zapewnić odpowiednie postanowienia umowne oraz środki organizacyjne i techniczne służące ochronie danych.

Wewnętrzne ramy organizacyjne zapewnienia zgodności w zakresie stosowania systemów AI

Zapewnienie zgodności z AI Act nie ogranicza się wyłącznie do wyboru narzędzia spełniającego wymagania regulacyjne, lecz obejmuje również konieczność wdrożenia odpowiednich rozwiązań wewnętrznych regulujących zasady korzystania z systemów AI, zakres odpowiedzialności

poszczególnych osób oraz sposób sprawowania nadzoru nad ich stosowaniem, a także zapewnienia odpowiednich szkoleń dla osób uczestniczących w procesie ich wykorzystywania.

Procedura AI (wewnętrzna polityka AI)

Organizacja powinna przyjąć wewnętrzną procedurę regulującą zasady korzystania z systemów AI. Taka procedura powinna określać w szczególności:

- kto może korzystać z narzędzi AI i w jakim zakresie;
- jakie dane mogą być wprowadzane do systemów, a jakie są wyłączone z takiego wykorzystania;
- zasady nadzoru człowieka nad decyzjami podejmowanymi przy wsparciu AI;
- sposób dokumentowania analizy ryzyka oraz DPIA;
- procedurę zgłaszania incydentów i błędnych decyzji systemu;
- zasady weryfikacji dostawców i ich zgodności z AI Act.

W praktyce procedura AI pozwala wykazać, że organizacja realizuje obowiązek zarządzania ryzykiem oraz zasadę rozliczalności.

Regulaminy wewnętrzne

Jeżeli system AI jest wykorzystywany w miejscu pracy, np. do monitorowania wydajności, przydzielania zadań lub oceny pracowników, zasady jego stosowania powinny znaleźć odzwierciedlenie w odpowiednich regulacjach wewnętrznych, w szczególności w:

- regulaminie pracy;
- polityce monitoringu;
- klauzulach informacyjnych kierowanych do pracowników.

Pracownicy powinni zostać jasno poinformowani:

- o fakcie stosowania systemu AI wysokiego ryzyka;
- o celu, w jakim system jest wykorzystywany;
- o kategoriach danych, które dane są przetwarzane;
- o tym, jakie prawa im przysługują, w tym o prawie do zakwestionowania decyzji.

Szkolenia

AI Act wskazuje na konieczność zapewnienia odpowiedniego poziomu kompetencji osób obsługujących systemy AI. Organizacja powinna zapewnić szkolenia dla swojego personelu. Szkolenia te powinny obejmować w szczególności następujące zagadnienia:

- podstawowe obowiązki wynikające z AI Act;
- ryzyko dyskryminacji algorytmicznej;
- zasady nadzoru człowieka;
- odpowiedzialność organizacji za decyzje podejmowane przy wsparciu AI;
- zasady bezpiecznego korzystania z narzędzi generatywnych.

Brak odpowiedniego przeszkolenia personelu może zostać uznany za naruszenie obowiązków organizacyjnych.

Pozostałe wyzwania:

Brak weryfikacji i rozliczalności

Administrator musi być w stanie udowodnić, że dane zostały usunięte. W przypadku AI, nie ma prostego technicznego sposobu na gwarancję, że wszystkie „ścieżki" i cząstki informacji o osobie zostały usunięte z modelu. Audyt „oduczenia" jest jednym z największych wyzwań.

Koszty i czasochłonność pełnego przetrenowania

Jeżeli „unlearning" zawiedzie, jedynym sposobem na zagwarantowanie usunięcia danych jest całkowite usunięcie i ponowne trenowanie modelu. Jest to operacja bardzo kosztowna (wymaga dużej mocy obliczeniowej) i czasochłonna, co stoi w sprzeczności z miesięcznym terminem na realizację żądania RODO.

Wpływ na integralność i dokładność modelu

Selektywne usunięcie danych (nawet jeżeli technicznie możliwe) może negatywnie wpłynąć na dokładność, spójność i niezawodność działania modelu, potencjalnie wprowadzając nowe błędy (bias) lub degradując jego wyniki.

VI Sankcje

W przypadku stwierdzenia naruszenia przepisów RODO Prezes UODO, jako organ nadzorczy, może zastosować wobec administratora lub podmiotu przetwarzającego **administracyjną karę pieniężną** (art. 83 RODO), a także **inne środki naprawcze** (art. 58 ust. 2 RODO).

Administracyjna kara pieniężna

RODO przewiduje dwa podstawowe progi administracyjnych kar pieniężnych. W przypadku naruszeń dotyczących obowiązków administratora i podmiotu przetwarzającego kara może wynieść do **10 000 000 euro**, a w przypadku przedsiębiorstwa – do **2% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym stosuje się kwotę wyższą. W przypadku naruszeń dotyczących podstawowych zasad przetwarzania danych, warunków zgody, praw osób, których dane dotyczą, przekazywania danych do państwa trzeciego, a także niewykonania nakazu organu nadzorczego, kara może wynieść do **20 000 000 euro**, a w przypadku przedsiębiorstwa do **4% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, również z zastosowaniem kwoty wyższej.

Wysokość kary nie jest ustalana automatycznie. Organ nadzorczy bierze pod uwagę okoliczności konkretnej sprawy, w szczególności: **charakter, wagę i czas trwania naruszenia**, jego **umyślny lub nieumyślny charakter**, działania podjęte w celu ograniczenia szkody, stopień współpracy z organem nadzorczym, wcześniejsze naruszenia, rodzaj danych, których sprawa dotyczy, a także stosowanie zatwierdzonych kodeksów postępowania lub mechanizmów certyfikacji.

Inne środki, które może zastosować organ nadzorczy

Kara pieniężna nie jest jedyną możliwą sankcją. Na podstawie **art. 58 ust. 2 RODO** Prezes UODO może także wydać **ostrzeżenie** lub **upomnienie**, nakazać dostosowanie przetwarzania do przepisów, nakazać spełnienie żądania osoby, której dane dotyczą, czasowo lub całkowicie ograniczyć przetwarzanie albo go zakazać, a także nakazać zawiadomienie osoby o naruszeniu ochrony danych. Środki te mogą zostać zastosowane samodzielnie albo łącznie z karą pieniężną.

Odpowiedzialność może być szersza

Naruszenie przepisów o ochronie danych osobowych może prowadzić nie tylko do odpowiedzialności administracyjnej. Osoba, której dane dotyczą, może **dochodzić odszkodowania** na podstawie art. 82 RODO. Ponadto za nieuprawnione przetwarzanie danych osobowych można ponieść **odpowiedzialność karną** na podstawie art. 107 ustawy z 10 maja 2018 r. o ochronie danych osobowych[1].

Ryzyka sankcji w HR

W obszarze HR ryzyko sankcji nie ogranicza się wyłącznie do wycieku danych, ale obejmuje także nieprawidłowości pojawiające się w codziennej praktyce przetwarzania danych osobowych. Dotyczy to w szczególności: pozyskiwania zbyt szerokiego zakresu danych kandydatów lub pracowników, braku właściwej podstawy prawnej przetwarzania, przechowywania danych dłużej, niż jest to potrzebne, zbyt szerokiego dostępu do dokumentacji, niewłaściwego zabezpieczenia danych lub braku jasnej informacji o zasadach przetwarzania.

1 Dz.U. z 2019 r. poz. 1781

VII Suplement
Wybrane techniczne i organizacyjne środki zabezpieczeń danych osobowych

Wdrożenie odpowiednich środków technicznych i organizacyjnych jest kluczowe dla zapewnienia zgodności z RODO. Przepisy te nakładają na administratora danych oraz podmiot przetwarzający obowiązek stosowania zabezpieczeń adekwatnych do ryzyka naruszenia praw i wolności osób fizycznych. Poniżej przedstawiono wybrane środki, ze szczególnym uwzględnieniem dobrych praktyk i nowoczesnych rozwiązań.

Środki organizacyjne

Są to zasady, procedury i mechanizmy zarządcze określające sposób postępowania z danymi osobowymi oraz zarządzania ryzykiem. Należą do nich:

- **aktualne, zatwierdzone przez najwyższe kierownictwo polityki i procedury** (np. Polityka Ochrony Danych, Polityka Bezpieczeństwa Informacji) określające zasady przetwarzania danych, w tym:
  - zasady czystego biurka i czystego ekranu – dbanie o porządek w dokumentacji papierowej i blokowanie ekranów komputerów po odejściu od stanowiska;
  - procedury zarządzania uprawnieniami – przyznawanie dostępu do danych osobowych na zasadzie minimalizacji (zasada „need to know");
  - procedury obsługi incydentów oraz naruszeń ochrony danych;
  - procedury obsługi wniosków osób fizycznych;
  - procedury zarządzania ryzykiem stron trzecich w zakresie np. podpisywania umów powierzenia z dostawcami w roli podmiotów przetwarzających;
  - obowiązkowe, cykliczne szkolenia z zasad ochrony danych osobowych i bezpieczeństwa informacji dla wszystkich pracowników oraz szkolenia z zastosowania rozwiązań AI;
- **umowy powierzenia przetwarzania danych osobowych** – zawieranie i bieżąca weryfikacja umów z podmiotami przetwarzającymi, które gwarantują wdrożenie adekwatnych zabezpieczeń (np. aktualizacja dalszych podmiotów przetwarzających czy zakresu powierzenia);
- **role i odpowiedzialność** – wyznaczenie Inspektora Ochrony Danych lub osoby, która będzie punktem kontaktowym w firmie w zakresie tematów związanych z przetwarzaniem danych osobowych oraz jasne określenie odpowiedzialności za bezpieczeństwo danych na poszczególnych stanowiskach;
- **ocena skutków dla ochrony danych (DPIA)** – przeprowadzanie DPIA w przypadku nowych procesów lub systemów niosących wysokie ryzyko dla praw i wolności osób, których dane dotyczą[1].

Środki techniczne

Są to rozwiązania technologiczne i narzędzia informatyczne mające na celu ochronę systemów i danych. Należą do nich m.in.:

1 Szczegóły: Monitor Polski 2019, poz. 666.

- **ochrona danych w fazie projektowania i domyślna ochrona danych** – zasady, które powinny być uwzględniane we wczesnych fazach projektowania systemów i procesów, w których przetwarzane są dane osobowe;

- **kontrola dostępu fizycznego** – zabezpieczenie pomieszczeń, w których przetwarzane są dane (alarmy, zamki, monitoring);

- **kontrola dostępu logicznego** – złożone hasła, uwierzytelnianie wieloskładnikowe (MFA), stosowanie YubiKey, automatyczne wylogowywanie/blokowanie sesji;

- **szyfrowanie** – stosowanie szyfrowania (np. AES-256) dla danych przesyłanych (np. maile, połączenia VPN) oraz dla danych przechowywanych (np. szyfrowanie dysków twardych, w tym w laptopach i nośnikach przenośnych);

- **kopie zapasowe i odtwarzanie** – regularne wykonywanie kopii zapasowych, ich testowanie oraz fizyczne zabezpieczenie (np. przechowywanie poza siedzibą firmy, kopie offline);

- **ochrona przed złośliwym oprogramowaniem** – aktualne oprogramowanie antywirusowe i antyspywar;

- **firewall**;

- **zarządzanie poprawkami** – bieżące aktualizowanie systemów operacyjnych i aplikacji w celu eliminacji luk w zabezpieczeniach.

Normy z zakresu zarządzania bezpieczeństwem informacji i ochrony danych osobowych pomagają administratorom i podmiotom przetwarzającym w usystematyzowaniu i weryfikacji wdrożonych środków. Należą do nich:

- **Norma ISO/IEC 27001** – to międzynarodowy standard określający wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Certyfikacja na zgodność z tą normą jest uznawanym dowodem na to, że agencja podjęła systemowe działania w celu ochrony danych;

- **Norma ISO/IEC 27701** – to rozszerzenie normy ISO/IEC 27001, które określa wymagania dotyczące Systemu Zarządzania Informacjami o Prywatności (PIMS) i jest bezpośrednio związane z wymogami RODO. Wdrożenie PIMS jest uważane za najlepszą praktykę w zakresie wykazania spełnienia zasady rozliczalności;

- **Krajowe i sektorowe schematy certyfikacji RODO** – w Polsce Prezes Urzędu Ochrony Danych Osobowych może zatwierdzać krajowe mechanizmy certyfikacji. Uzyskanie takiej certyfikacji stanowi formalny dowód zgodności z RODO.

Najlepsze praktyki w sposobach zabezpieczeń danych

W dobie dynamicznego rozwoju technologii i metod ataków zaleca się stosowanie zaawansowanych, następujących środków, zwłaszcza w kontekście przetwarzania dużych zbiorów danych kandydatów:

- **wierzytelnianie wieloskładnikowe (MFA/2FA) i logowanie bezhasłowe:**

    - wymaganie stosowania MFA (np. tokeny sprzętowe, aplikacje uwierzytelniające) przy logowaniu do wszystkich systemów przetwarzających dane osobowe;

    - rozważenie wdrożenia technologii passkey lub logowania biometrycznego jako alternatywy dla tradycyjnych haseł;

- **pseudonimizacja i anonimizacja na wczesnym etapie:**
  - stosowanie pseudonimizacji (np. haszowanie danych, tokenizacja) przy testowaniu systemów lub tworzeniu raportów analitycznych. Dane osobowe powinny być anonimizowane lub pseudonimizowane w możliwie najwcześniejszym etapie ich przetwarzania;
- **regularne testy penetracyjne i audyty bezpieczeństwa:**
  - cykliczne przeprowadzenie testów w celu zidentyfikowania luk w zabezpieczeniach systemów informatycznych;
- **systemy detekcji i reagowania (SIEM/SOAR):**
  - wdrożenie narzędzi do monitorowania i analizy zdarzeń bezpieczeństwa w czasie rzeczywistym oraz automatyzacji reagowania na incydenty;
- **segmentacja sieci:**
  - podział sieci wewnętrznej na strefy (np. oddzielna sieć dla systemów HR, oddzielna dla gości), co ogranicza zasięg potencjalnego ataku w przypadku kompromitacji jednej strefy;
- **zabezpieczenia w chmurze:**
  - w przypadku korzystania z usług chmurowych, stosowanie najwyższych standardów zabezpieczeń dostawcy (np. szyfrowanie na poziomie bazy danych, zarządzanie kluczami szyfrującymi przez administratora);
- **zabezpieczenia w systemach Sztucznej Inteligencji (AI):**
  - minimalizacja danych wejściowych – zasada minimalizacji musi być ściśle przestrzegana: do szkolenia i działania modeli AI należy wykorzystywać wyłącznie dane niezbędne do realizacji celu;
  - ograniczenie dostępu do modeli i zbiorów treningowych poprzez zastosowanie ścisłej kontroli dostępu (ang. „role-based access control" – RBAC) do środowisk, w których trenowane są modele oraz gdzie są przechowywane dane treningowe i operacyjne;
  - usuwanie wrażliwych danych z modeli (ang. „unlearning") można osiągnąć poprzez opracowanie i wdrożenie procedur umożliwiających usunięcie wpływu danych konkretnej osoby na model (np. w realizacji prawa do bycia zapomnianym), bez konieczności całkowitego usuwania i przetrenowywania modelu, o ile jest to technicznie wykonalne;
  - testowanie odporności (ang. „adversarial testing") to regularne testowanie modeli AI pod kątem podatności na ataki mające na celu wydobycie danych treningowych lub manipulację wynikami (np. ataki inwazyjne);
  - przejrzystość i wyjaśnialność (ang. „explainability") to dokumentowanie procesów decyzyjnych modelu AI, zwłaszcza w kontekście art. 22 RODO (zautomatyzowane podejmowanie decyzji), aby móc wyjaśnić osobie, której dane dotyczą, logiczne podstawy wydanej decyzji;
  - ocena ryzyka AI, czyli przeprowadzanie dedykowanej oceny ryzyka dla każdego systemu AI, która uwzględnia specyficzne ryzyka, takie jak uprzedzenia modelu (bias) i potencjalne skutki prawne zautomatyzowanych decyzji.

Polskie
Forum HR

Głos branży usług HR. Najbardziej wpływowa organizacja reprezentująca sektor usług HR w Polsce. Od 2002 roku kształtujemy efektywny rynek pracy. Wspieramy naszych członków w rozwoju zgodnym z najwyższymi standardami, łącząc edukację, badania i praktykę.

www.polskieforumhr.pl

RODO

mały kodeks postępowania dla agencji zatrudnienia

EDYCJA III 2026