RODO

mały kodeks postępowania
dla agencji zatrudnienia

RODO

mały kodeks postępowania
dla agencji zatrudnienia

Polskie Forum HR

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

SPIS TREŚCI

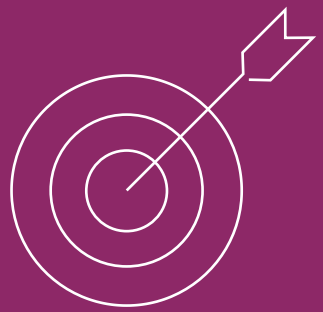
WSTĘP

Głównymi przyczynami powołania do życia RODO[1] była potrzeba wzmocnienia praw i ochrony osób, których dane dotyczą, skonkretyzowania i doprecyzowania obowiązków podmiotów przetwarzających dane osobowe, a także zaktualizowanie i unowocześnienie przepisów, które wraz z rozwojem techniki i powszechną cyfryzacją społeczeństw stały się nieefektywne. Przepisy formułowane na początku lat dwutysięcznych, jak na przykład ten o stosowaniu haseł składających się z 8 znaków, już od dawna nie zapewniały należytego bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

Wprowadzając RODO, europejski ustawodawca stworzył przepisy, które mają być neutralne technologicznie, aby nieustający postęp techniczny, technologiczny i informatyczny nie stwarzał konieczności ciągłego ich dostosowywania. Nie wskazuje się więc, ani nie rekomenduje w RODO żadnych środków technicznych czy organizacyjnych, które miałyby być obowiązkowo stosowane przez organizacje. RODO wskazuje jedynie kilka ogólnych zasad, którymi należy kierować się przy projektowaniu rozwiązań biznesowych i informatycznych.

---

1 Rozporządzenie 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.



Główne idee RODO

2

GŁÓWNE IDEE RODO

Podejście oparte na ryzyku

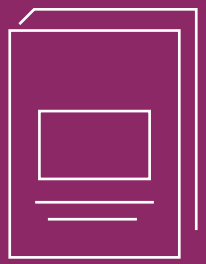
Ustawodawca europejski wyszedł z założenia, że przedsiębiorca, znając swoją branżę i będąc ekspertem w swojej dziedzinie, sam najtrafniej potrafi zidentyfikować ryzyka w prowadzonej działalności, dlatego też sam dokona optymalnego doboru środków ochrony danych osobowych. Metody te powinny być dopasowane do charakteru i sposobu przetwarzania oraz rodzaju przetwarzanych danych osobowych.

Privacy by design

Zasada ta oznacza, że każda organizacja zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, ma obowiązek uwzględnić ochronę prywatności w fazie projektowania swoich procesów, zwłaszcza, jeśli do przetwarzania danych osobowych wykorzystuje technologię informatyczną. Środki techniczne i organizacyjne powinny uwzględniać aktualny stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Privacy by default

Zasada ta oznacza, że każdy przedsiębiorca już na etapie projektowania systemu ochrony danych osobowych powinien wdrożyć takie środki techniczne i organizacyjne, by chronić przetwarzane dane oraz prywatność osób, których dane dotyczą. Ochrona prywatności, rozumiana jako minimalizowanie ilości i okresu przetwarzanych danych, a także ich dostępności, powinna zostać wbudowana w projekt.



Najważniejsze pojęcia

3

NAJWAŻNIEJSZE POJĘCIA

Przykład danych biometrycznych: wizerunek twarzy, kształt dłoni, zapis linii papilarnych palców, zapis obrazu tęczówki, zapis układu żył w palcu/nadgarstku, sposób chodzenia, sposób pisania na klawiaturze komputera.

Przykład danych dot. zdrowia: numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu zidentyfikowania tej osoby do celów zdrowotnych, informacje z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych oraz inne informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym, stanie fizjologicznym lub biomedycznym.

Agencja
Agencja zatrudnienia lub agencja pracy tymczasowej w rozumieniu Ustawy z dnia 20.04.2004 r. o promocji zatrudnienia i instytucjach rynku pracy (t.j. Dz. U. z 2017 r., poz. 1065, dalej „Ustawa o promocji zatrudnienia").

Dane osobowe
Dane identyfikujące lub pozwalające identyfikować daną osobę fizyczną.

Dane wrażliwe (inaczej: dane sensytywne)
Dane ujawniające w szczególności: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

Dane biometryczne
Informacje pozwalające zidentyfikować osobę na podstawie jej unikalnych cech biologicznych, dokonane poprzez porównanie zapisu tych cech z bazy danych z nową próbką i określenie, czy są identyczne. Wynikają z przetwarzania zautomatyzowanego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby.

Dane dotyczące zdrowia
Dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie zdrowia fizycznego lub psychicznego.

Osoba, której dane dotyczą
Osoba, do której odnoszą się dane osobowe, np. kandydat, pracownik agencji zatrudnienia, pracownik jej klienta.

Zgoda
Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby, której dane dotyczą, w formie oświadczenia lub wyraźnego działania

potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych.

Zbiór danych
Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie.

Przetwarzanie danych osobowych
Operacja lub zespół operacji na danych osobowych lub na zestawach danych, w szczególności: zbieranie, utrwalanie, udostępnianie, przechowywanie, modyfikowanie, pobieranie, wykorzystywanie, usuwanie, niszczenie, przeglądanie, ograniczanie.

Transgraniczne przetwarzanie danych
Przetwarzanie danych osobowych, które odbywa się na terenie UE w ramach działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w UE, posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim, jak również przetwarzanie danych, które odbywa się w UE w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim.

Administrator danych osobowych (inaczej: kontroler)
Podmiot, który samodzielnie lub wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający (inaczej: procesor)
Podmiot, który przetwarza dane osobowe w imieniu administratora.

Odbiorca
Podmiot, któremu ujawnia się dane osobowe.

Umowa powierzenia danych
Umowa, na podstawie której administrator danych osobowych powierza procesorowi przetwarzanie danych osobowych w imieniu administratora.

Profilowanie
Dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do

analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

RODO przewiduje dwie **kategorie** profilowania:

- polegające na ocenie prawdziwych informacji pozyskanych na temat danej osoby,
- polegające na wytworzeniu nowej (statystycznej) informacji o osobie, na podstawie danych pozyskanych od niej.

RODO przewiduje dwie **formy** profilowania:

- profilowanie zwykłe (z udziałem czynnika ludzkiego),
- zautomatyzowane (w pełni obsługiwane przez program komputerowy) – kończące się podjęciem zautomatyzowanej decyzji.

Automatyzacja podejmowania decyzji, jak wskazuje J. Mulawka[2] wiąże się z podziałem zautomatyzowanych systemów na: systemy doradcze (advisory systems), systemy podejmujące decyzję bez kontroli człowieka (dictatorial systems), systemy krytykujące (criticizing systems). Systemy mogą więc wspierać podjęcie decyzji przez człowieka (systemy, w których mamy do czynienia z profilowaniem zwykłym – z udziałem czynnika ludzkiego) lub systemy zautomatyzowane (w pełni obsługiwane przez program komputerowy, kończące się podjęciem decyzji bez kontroli człowieka).

Pseudonimizacja

Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Naruszenie ochrony danych osobowych

(inaczej: incydent)

Naruszenie bezpieczeństwa prowadzące do

2 J. Mulawka, „Systemy ekspertowe", 1996 Warszawa, patrz także Mrózek A., Proces stosowania prawa jako proces przetwarzania informacji, Państwo i Prawo, z. 7, 1970, J. Petzel, Informatyka prawnicza, Warszawa 1999, s. 311.

przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przesłanych, przechowywanych lub w innych sposób przetwarzanych danych osobowych.

Organ

Organ właściwy w zakresie ochrony danych osobowych. W Polsce organem takim jest Prezes Urzędu Ochrony Danych Osobowych (art. 34 ust. 1 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych).

Usługi świadczone przez agencje zatrudnienia

Rekrutacja

Usługa doradztwa personalnego i/lub pośrednictwa pracy, usługa zdefiniowana w Art. 18 ust. 1 Ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (t.j. Dz. U. 2017 poz. 1065 ze zm.), polegająca m.in. na inicjowaniu i organizowaniu kontaktów osób poszukujących odpowiedniego zatrudnienia lub innej pracy zarobkowej z pracodawcami, udzielaniu pomocy osobom w uzyskaniu odpowiedniego zatrudnienia oraz pracodawcom w pozyskaniu pracowników o poszukiwanych kwalifikacjach zawodowych, a także na udzielaniu pracodawcom informacji o kandydatach do pracy, w związku ze zgłoszoną ofertą pracy (pośrednictwo pracy), a także na określaniu kwalifikacji pracowników i ich predyspozycji, jak również weryfikacji kandydatów pod względem oczekiwanych kwalifikacji (doradztwo personalne).

Praca tymczasowa

Usługa zdefiniowana w Ustawie z dnia 10 maja 2018 r. o zatrudnianiu pracowników tymczasowych (t.j. Dz. U. z 2018 r., poz. 594, dalej „Ustawa o zatrudnianiu pracowników tymczasowych"), polegająca na zatrudnieniu pracowników tymczasowych i skierowaniu ich do wykonywania pracy tymczasowej na rzecz i pod kierownictwem pracodawcy użytkownika.

Delegowanie pracowników do pracy za granicę w ramach swobody świadczenia usług

Zdefiniowane w Dyrektywie 96/71/WE Parlamentu Europejskiego i Rady z dnia 16 grudnia 1996 roku dotyczącej delegowania pracowników w ramach świadczenia usług (dalej „Dyrektywa 96/71/WE"). Polega na wysyłaniu przez przedsiębiorcę pracowników w celu tymczasowego świadczenia usługi w przedsiębiorstwie, mającym siedzibę w innym państwie członkowskim (tzw. "państwo

przyjmujące"). 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.

Inne, niespecyficzne usługi, świadczone przez agencje zatrudnienia

Agencje zatrudnienia (podobnie jak inne podmioty prowadzące działalność gospodarczą i nie posiadające statusu agencji zatrudnienia), mogą świadczyć na rzecz swoich kontrahentów także inne, niespecyficzne usługi, do realizacji których wykorzystywany jest personel zatrudniany przez te agencje. Mogą być to poszczególne zadania, funkcje, jak również całe procesy, obsługiwane przez agencję na zlecenie kontrahenta. W takim wypadku mamy do czynienia z tzw. outsourcingiem usług, który nie jest regulowany w przepisach prawa, ale może być realizowany na zasadzie swobody zawierania i wykonywania umów i jest obecnie powszechną formą uzupełniania biznesowych potrzeb przedsiębiorców za pomocą dostawców zewnętrznych. Definicje outsourcingu są bardzo różne i niejednolite jest również podejście do tego tematu w praktyce. W pewnym uogólnieniu można powiedzieć, że outsourcing usług polega na powierzeniu przez jeden podmiot (kontrahenta agencji) drugiemu podmiotowi (agencji), stale lub okresowo, czynności, zadań, funkcji lub procesów związanych z obsługą działalności prowadzonej przez drugi podmiot, przy wykorzystaniu personelu podmiotu pierwszego.

Podstawowe zasady przetwarzania danych

4

PODSTAWOWE ZASADY PRZETWARZANIA DANYCH

Zasada zgodności z prawem – art. 6 RODO

Zgodnie z tą zasadą przetwarzanie danych osobowych może mieć miejsce wyłącznie wtedy, gdy występuje jedna z podstaw prawnych przetwarzania, wskazana w art. 6 RODO. Z punktu widzenia działalności agencji zatrudnienia szczególne znaczenie mają poniższe podstawy prawne:

Ważne:
na agencji zatrudnienia jako na administratorze danych spoczywa obowiązek udowodnienia, że dana osoba wyraziła zgodę.

- **zgoda** na przetwarzanie danych wyrażona przez osobę, której dane dotyczą;
- podjęcie działań niezbędnych dla **zawarcia umowy**;
- **konieczność wykonania umowy**, której stroną jest osoba, której dane dotyczą (tj. wykonywanie umowy, np. umowy o pracę lub umowy cywilnoprawnej, albo umowy z kontrahentem, które nie byłoby możliwe bez jednoczesnego przetwarzania danych);
- wypełnienie **obowiązku prawnego ciążącego na administratorze** (np. konieczność przechowywania dokumentów na potrzeby realizacji obowiązków pracodawcy w stosunku do Zakładu Ubezpieczeń Społecznych, Państwowej Inspekcji Pracy i innych instytucji publicznych);
- **prawnie uzasadniony interes** administratora danych.

Zasada rzetelności, przejrzystości – art. 5 ust. 1 pkt a RODO

Zasada ta obowiązuje wszystkie podmioty przetwarzające dane osobowe na każdym etapie przetwarzania. W kontekście rzetelności istotne znaczenie mają przede wszystkim odpowiednie środki techniczne i organizacyjne pozwalające na właściwe zabezpieczenie danych osobowych. Ponadto, agencja zatrudnienia powinna

dbać o to, aby osoby, których dane są przetwarzane były świadome stopnia, celu oraz zasad przetwarzania ich danych. Wszelkie informacje oraz komunikaty winny być łatwo dostępne oraz sformułowane zrozumiałym językiem. W tym kontekście szczególnego znaczenia nabiera obowiązek informacyjny (art. 13, 14 RODO), który nakazuje administratorowi informowanie m. in. o swoich danych, celu przetwarzania (rekrutacja, zatrudnienie), prawach przysługujących osobom, których dane są przetwarzane, odbiorcach lub kategoriach odbiorców danych osobowych (np. pracodawcy użytkownicy, którzy po udostępnieniu danych administrują danymi osobowymi pracowników tymczasowych). Ponadto bezwzględnie należy informować o uprawnieniu do przenoszenia i usuwania danych osobowych, jak również prawie do cofnięcia zgody na ich przetwarzanie.

Zasada ograniczoności celu – art. 5 ust. 1 pkt b RODO

Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Agencje zatrudnienia powinny unikać przetwarzania danych dla realizacji kilku celów jednocześnie, a także przetwarzania danych w niejasnych, trudnych do zdefiniowania celach, których nie można wskazać w sposób dokładny i precyzyjny (w szczególności celach nie związanych ze świadczonymi usługami, ale np. wyłącznie z działalnością kontrahenta).

Zasada minimalizacji danych – art. 5 ust. 1 pkt c RODO

Dopuszczalny zakres przetwarzanych danych musi być adekwatny i ograniczony wyłącznie do takiego katalogu danych, który jest niezbędny do osiągnięcia celów, dla których dane są przetwarzane. W kontekście powyższego, agencje zatrudnienia powinny mieć na uwadze, że nie powinno mieć miejsca zbieranie oraz przechowywanie kopii dokumentów tożsamości zatrudnianych osób, gdyż nie jest to konieczne, aby ustalić tożsamość zatrudnionej osoby i nie służy innym celom związanym z zatrudnieniem. Nie powinno również mieć miejsca zbieranie od osób ubiegających się o zatrudnienie danych innych niż przewidziane w Kodeksie pracy (np. stan cywilny, czy adres zameldowania), chyba, że osoba, której dane dotyczą wyraziła na to swoją dobrowolną zgodę lub sama udostępniła swoje dane (np. fotografię w CV).

Zasada prawidłowości – art. 5 ust. 1 pkt d RODO

Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Jest to szczególnie istotne z punktu widzenia przetwarzania danych osobowych na potrzeby instytucji publicznych (np. Zakład Ubezpieczeń Społecznych, właściwy urząd skarbowy), albowiem np. w toku postępowań kontrolnych, organy winny mieć dostęp do aktualnych, niewprowadzających w błąd danych.

Zasada ograniczenia przechowywania – art. 5 ust. 1 pkt e RODO

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą oraz przez okres **nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane**, przy czym:

- dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, pod warunkiem wdrożenia odpowiednich środków technicznych i organizacyjnych, czyli rozdzielenia baz danych ze względu na wymienione cele (na przykład wyodrębniona baza danych osobowych do celów statystycznych, do której dostęp mają wyłącznie pracownicy dedykowanego zespołu, która nie może być wykorzystywana do celu pierwotnego),

- aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania (tzw. okres retencji) lub okresowego przeglądu.

Ważne:
Nie jest rekomendowane długie przechowywanie danych, z których w ogóle nie korzystamy. **Rekomendujemy usuwanie danych kandydatów, z którymi brak jest kontaktu przez okres 2 lat, jak również skontaktowanie się z każdym kandydatem przynajmniej raz w roku w celu odświeżenia zgody.** Każda agencja, biorąc pod uwagę specyfikę swojej działalności i charakter realizowanych procesów rekrutacyjnych (w tym rodzaj lub poziom stanowisk, stopień trudności w ich pozyskaniu, długość trwania procesu rekrutacyjnego, czy wskaźnik rotacji w danym rodzaju/szczeblu stanowiska) może podjąć samodzielną decyzję o tym, aby ten okres skrócić lub wydłużyć; przy wydłużeniu musi jednak umieć wykazać, jakie kryteria, cele lub inne przesłanki o charakterze obiektywnym to uzasadniają.

W działalności agencji zatrudnienia niektóre dane osobowe musimy przechowywać obowiązkowo i przez czas określony przepisami obowiązującego prawa. Dotyczy to na przykład: pracowniczych akt osobowych, dokumentacji podatkowej lub ubezpieczeniowej pracowników. **W przypadku, gdy przepis prawa nie wskazuje obowiązkowego okresu przechowywania, każdy podmiot musi zdecydować samodzielnie przez jaki okres będzie przechowywał dane do określonego celu.** W szczególności dotyczy to danych, które zbieramy na potrzeby podstawowych celów naszej działalności – danych kandydatów i klientów. RODO nie wskazuje minimalnego lub maksymalnego okresu przechowywania takich danych. Dlatego każda agencja musi samodzielnie zdecydować przez jaki czas będzie przechowywała określone kategorie danych.

W przypadku przetwarzania danych osoby kontaktowej reprezentującej klienta, można je przetwarzać do celów realizacji umowy. Po okresie realizacji umowy również możliwe jest ich dalsze przetwarzanie, jeżeli ma to nadal związek z umową, np. dochodzenie roszczeń, regulowanie należności, obsługa reklamacji i gwarancji. Kontakt z taką osobą do celów handlowych lub marketingowych (np. złożenie oferty na nową usługę) możliwy jest, jeżeli osoba ta akceptuje tego rodzaju kontakt.

Zasada integralności danych i poufności – art. 5 ust. 1 pkt f RODO

Dane osobowe muszą być przetwarzane za pomocą odpowiednich środków technicznych lub organizacyjnych, w sposób zapewniający im odpowiednie bezpieczeństwo i poufność, w tym ochronę przed:

- niedozwolonym lub niezgodnym z prawem przetwarzaniem, czyli m.in. nieuprawnionym dostępem do nich oraz do sprzętu służącego ich przetwarzaniu, a także przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu,
- przypadkową utratą, zniszczeniem lub uszkodzeniem.

W powyższym kontekście szczególnie ważne jest, aby dane osobowe nie trafiały do osób nieupoważnionych, jak również nie przedostawały się do obrotu publicznego. Na podmiotach przetwarzających dane (zarówno administratorach, jak i procesorach) ciąży obowiązek stosowania odpowiednich środków i polityk gwarantujących bezpieczeństwo danych osobowych, przy czym przepisy nie przewidują zamkniętego katalogu tego rodzaju środków.

RODO zwraca uwagę między innymi na:

- **szyfrowanie danych osobowych**, które może być stosowane w szczególności w przypadku przesyłania drogą elektroniczną plików zawierających dane kadrowe (np. wysokość wynagrodzenia, liczba przepracowanych godzin, premie uzyskane przez pracowników); niezależnie od szyfrowania należy dbać o to, aby do tego rodzaju danych osobowych dostęp miały jedynie te osoby, dla których dostęp ten jest niezbędny (np. pracownicy działów kadr),
- **pseudonimizację**, która może przybrać kilka form, np. tokenizacja (dane zastępowane są przez ciągi liczb) lub skracanie, dzięki któremu odczytanie treści danych nie jest możliwe.

Niezależnie od zapisów RODO w działalności agencji zatrudnienia warto rozważyć stosowanie środków bezpieczeństwa, takich jak np.:

- stosowanie haseł zabezpieczających dostęp do komputerów, telefonów i innych nośników danych,
- stosowanie procedury odnawiania haseł dostępu,
- zabezpieczenie serwerów poprzez zlokalizowanie ich w zamkniętych pomieszczeniach z ograniczonym dostępem,
- stosowanie zabezpieczonych szafek kadrowych, w których przechowywane są dokumenty pracownicze,
- wprowadzenie rejestrów i monitoringu dostępu do danych osobowych,
- wprowadzenie upoważnień dla osób przetwarzających dane,
- prowadzenie cyklicznych szkoleń personelu w zakresie ochrony danych osobowych,
- wprowadzenie zasady czystego biurka,
- niepowielanie baz danych,
- skuteczne usuwanie danych.

Zasada rozliczalności – art. 5 ust. 2 RODO

Każdy administrator danych jest odpowiedzialny i musi wykazać przestrzeganie przepisów RODO. Po stronie administratora leży udowodnienie, że przestrzega RODO, np. w przypadku kandydatów do pracy administrator powinien wykazać, że **uzyskał** zgodę na przetwarzanie danych osobowych i **spełnił** obowiązek informacyjny. W przypadku osób kontaktowych po stronie klientów, administrator również powinien wykazać się spełnieniem powyższych obowiązków. Administrator musi być także w stanie udowodnić przestrzeganie, opisanego w art. 25 RODO, obowiązku uwzględniania ochrony danych w fazie projektowania oraz zapewnienia domyślnej ochrony danych. W tym celu zalecane jest prowadzenie dokumentacji, która pozwoli administratorowi wykazać, że przeprowadził ocenę skutków dla ochrony danych (np. kwestionariusz dotyczący środków technicznych i organizacyjnych stosowanych przez dostawcę usługi informatycznej, z którym administrator zamierza podpisać umowę).

Prawa osób, których dane dotyczą

5

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Osoba, której dane dotyczą może żądać od agencji realizacji wszystkich praw, które zostały wymienione w niniejszym rozdziale. Przed wykonaniem żądania oraz biorąc pod uwagę cel przetwarzania agencja ocenia, czy:

- tożsamość zgłaszającego może zostać potwierdzona na podstawie danych zawartych we wniosku, a jeżeli nie, wówczas agencja dokłada rozsądnych starań, aby te dane potwierdzić; brak możliwości potwierdzenia danych elektronicznie uzasadnia konieczność osobistego wezwania składającego żądanie; brak potwierdzenia tożsamości składającego żądanie stanowi podstawę odmowy realizacji żądania,
- przechowywanie określonych danych osobowych nie jest wymagane przez przepisy prawa,
- interes agencji nie jest nadrzędny względem interesu składającego żądanie (np. potencjalne roszczenia),
- składający żądanie nie wprowadza agencji w celowy błąd mogący narazić agencję na konsekwencje prawne lub stratę.

Prawo do informacji – art. 12 – 14 RODO

Przedsiębiorca, który jest administratorem jest zobowiązany 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. Informacje mogą być udzielone w sposób dowolny, bez zbędnej zwłoki, jednak nie później niż w terminie 30 dni od daty ich żądania.

Prawo dostępu do danych – art. 15 RODO

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarza on dane osobowe, które jej dotyczą. Jeżeli tak, osoba ta może żądać np. udzielenia jej informacji o celu przetwarzania, czy też okresie, w jakim dane będą przetwarzane. Administrator ma obowiązek wydać podmiotowi żądającemu kopię jego danych, przy czym domyślną formą wydania kopii jest kopia elektroniczna. Realizacja praw jest zasadniczo nieodpłatna dla osób, których dane dotyczą (art. 12 ust. 5 RODO). Oznacza to, że administrator nie pobiera opłat za spełnienie żądania lub udzielenie informacji. Wyjątkowo, administrator może pobrać z tego tytułu rozsądną opłatę uwzględniającą administracyjne koszty takich działań, jeśli żądania osoby, której dane dotyczą są nieuzasadnione lub nadmierne, w szczególności jeżeli są ustawiczne.

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.
Powyższe prawo jest realizowane w sposób elektroniczny lub osobiście poprzez wypełnienie dedykowanego formularza (oświadczenia). Agencja odpowiada na żądanie niezwłocznie, nie później niż w ciągu 30 dni. Termin realizacji żądania może ulec wydłużeniu, jeżeli wykonanie żądania napotkało na obiektywne przeszkody, o czym należy poinformować osobę zgłaszającą żądanie.

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 osobowych osoby, której dane dotyczą, włączając w to wszystkie bazy wewnętrzne agencji,

Ważne:
rekomenduje się podanie co najmniej dwóch alternatywnych form kontaktu.

która musi dołożyć wszelkich starań, aby podmioty przetwarzające dokonały takiego usunięcia w swoich bazach danych.
Agencja w sposób jasny i publicznie dostępny musi zapewnić możliwość kontaktu w celu realizacji powyższych praw, w formie formularza papierowego, na stronie internetowej lub dedykowanego adresu e-mail.
Prawa powyższe są realizowane w sposób elektroniczny lub osobiście poprzez bezpośrednie przesłanie żądania z danymi umożliwiającymi identyfikację składającego żądanie. Agencja odpowiada na żądanie podmiotu niezwłocznie, nie później niż w ciągu 30 dni, uwzględniając status realizacji żądania również u podmiotów przetwarzających.
Termin realizacji żądania może ulec wydłużeniu, jeżeli wykonanie żądania napotkało na obiektywne przeszkody, o czym należy poinformować osobę zgłaszającą żądanie.

Prawo do sprzeciwu – art. 21 RODO

Ważne:
prawo do sprzeciwu **nie przysługuje** osobie, której dane są przetwarzane na podstawie zgody (np. kandydatowi w procesie rekrutacyjnym) lub w związku z realizacją umowy (np. osobie kontaktowej klienta w związku z realizacją umowy). W stosunku to 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).

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 stanie się co do zasady niemożliwe.

Przykład ograniczenia przetwarzania danych:
kandydat bierze udział w procesie rekrutacji. Poza danymi określonymi w art. 221 § 1 Kodeksu pracy (których przetwarzanie może odbywać się na podstawie przepisów prawa), kandydat udostępnił podmiotowi rekrutującemu również szereg innych danych (np. zdjęcie, nr PESEL). Jednocześnie na etapie poprzedzającym rekrutację, jak również w jej trakcie, kandydat w ogóle nie wyraził zgody na przetwarzanie danych osobowych. W tej sytuacji, dopóki kandydat bierze udział w procesie rekrutacji (lub nie zażądał usunięcia swoich danych), podmiot rekrutujący może przetwarzać wyłącznie jego dane wskazane w Kodeksie pracy, natomiast kandydat w każdym czasie może zażądać, aby jego pozostałe dane (np. wspomniane zdjęcie, nr PESEL) nie były przetwarzane. W rezultacie dojdzie do ograniczenia przetwarzania danych osobowych, tj. administrator będzie je przetwarzał w dalszym ciągu, ale już w ograniczonym zakresie.

Prawo do ograniczenia przetwarzania danych – art. 18 RODO

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania, między innymi:

- jeżeli kwestionuje prawidłowość danych osobowych lub jeżeli przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
- gdy administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do przenoszenia danych – art. 20 RODO

Osoba, której dane dotyczą ma prawo żądania otrzymania w ustrukturyzowanym, powszechnie używanym formacie (np. PDF), nadającym się do odczytu maszynowego, danych osobowych jej dotyczących oraz przesłania ich innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Poza tym, ma prawo żądać przesłania danych bezpośrednio między administratorami, o ile jest to technicznie możliwe.

Aby 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

Osoba, której dane dotyczą ma prawo żądać od administratora uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.
Administrator ma obowiązek poinformowania o sprostowaniu, usunięciu lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe (wyjątek: chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku), a jeżeli zainteresowany tego zażąda, należy poinformować go o odbiorcach, którym ujawniono dane.
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 wniosek o nakazanie dopełnienia tego obowiązku.

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**. Zgodnie z art. 22 RODO w przypadku, kiedy zautomatyzowane podejmowanie decyzji **wywołuje skutki prawne wobec osoby, której dane dotyczą lub wpływa istotnie na osobę, której dane dotyczą, w podobny sposób do skutków prawnych konieczne jest uzyskanie zgody osoby, której dane dotyczą**.

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 zautomatyzowanym, wymagającym uzyskania zgody kandydata, ponieważ korzystanie z systemów baz danych

jest zawsze 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. Pracownik agencji zawsze analizuje profile kandydatów i z grupy kandydatów spełniających kryteria wybiera (sam, na podstawie własnej wiedzy i doświadczenia) tych, których rekomenduje klientowi.

Ważne:
jeżeli rekrutacja kandydatów odbywa się wyłącznie poprzez korzystanie z systemów informatycznych, w przypadku których system dokonuje ostatecznego wyboru (tj. wprowadzenie pożądanych kryteriów do systemu kończy się przedstawieniem przez system optymalnych kandydatów) mamy do czynienia z profilowaniem zautomatyzowanym **wymagającym zgody kandydata**.

Agencja, która zamierza poddawać profilowaniu dane osobowe kandydatów lub pracowników, powinna spełnić względem tych osób **obowiązek informacyjny**, obejmujący następujące informacje:

- że proces profilowania będzie wykonywany,
- w jakiej formie (zwykłej, zautomatyzowanej),
- jakie są konsekwencje i znaczenie profilowania dla tej osoby,
- że przysługuje każdej osobie prawo wniesienia sprzeciwu względem profilowania (zarówno w zwykłej, jak i zautomatyzowanej formie).

Przetwarzanie danych w agencjach zatrudnienia

6

PRZETWARZANIE DANYCH W AGENCJACH ZATRUDNIENIA

USŁUGI REKRUTACYJNE

Podstawowe role pełnione przez agencję i klientów usług rekrutacyjnych

W procesie świadczenia usług rekrutacyjnych agencja pełni rolę **administratora danych** w stosunku do danych osobowych kandydatów do pracy, rekomendowanych swoim klientom. Rola administratora danych wynika z istoty działalności prowadzonej przez agencję na podstawie Ustawy o promocji zatrudnienia. Zgodnie z art. 18 ust. 1 tej ustawy, prowadzenie działalności gospodarczej w zakresie **świadczenia usług pośrednictwa pracy**, polega m.in. na inicjowaniu i organizowaniu kontaktów osób poszukujących odpowiedniego zatrudnienia lub innej pracy zarobkowej z pracodawcami, udzielaniu pomocy osobom w uzyskaniu odpowiedniego zatrudnienia oraz pracodawcom w pozyskaniu pracowników o poszukiwanych kwalifikacjach zawodowych, a także na udzielaniu pracodawcom informacji o kandydatach do pracy, w związku ze zgłoszoną ofertą pracy. Z kolei domeną **usług doradztwa personalnego** jest m.in. określanie kwalifikacji pracowników i ich predyspozycji, jak również weryfikacja kandydatów pod względem oczekiwanych kwalifikacji. Powyższe usługi agencja wykonuje na potrzeby **wszystkich rekrutacji prowadzonych na rzecz swoich klientów, w tym obecnych i przyszłych**. Realizuje ona zatem **własne cele przetwarzania**, posługując się przy tym **własnymi środkami i metodami**, w tym środkami technologicznymi (bazy danych kandydatów, poszukiwania bezpośrednie i pośrednie, testy, formularze, analizy).

W celu świadczenia usług rekrutacyjnych, w szczególności zarekomendowania klientom kandydatów spełniających oczekiwane wymagania, agencja **udostępnia dane osobowe tych kandydatów klientowi, działającemu jako samodzielny administrator danych**. Klient agencji, po otrzymaniu od niej danych osobowych proponowanych kandydatów, zaczyna r**ealizować własny cel przetwarzania**, jakim jest weryfikacja i ocena danych,

a także samodzielne podjęcie decyzji o zatrudnieniu lub odrzuceniu danej kandydatury. **Jest zatem również w pełni odrębnym administratorem danych, decydującym o celach** (zatrudnienie pracownika o poszukiwanych cechach) i **środkach przetwarzania** (analiza dokumentów, spotkanie z kandydatem, wideokonferencja itd.).

Mając na uwadze powyższe, w procesie rekrutacji pomiędzy agencją a klientem zachodzi relacja administrator – administrator, a wymiana danych powinna następować na zasadzie udostępnienia danych. Każdy podmiot realizuje bowiem własny cel i posługuje się własnymi środkami przetwarzania danych.

Przetwarzanie danych osobowych w poszczególnych etapach świadczenia usług rekrutacyjnych

Rekrutacja – pozyskiwanie danych:

- z inicjatywy kandydata (przesłanie CV, wypełnienie aplikacji online itp.),
- z inicjatywy agencji (poszukiwania bezpośrednie, portale rekrutacyjne itp.).

Realizacja usługi po stronie agencji:

- analiza zamówienia klienta,
- weryfikacja źródeł pozyskania kandydatów,
- kontakt z kandydatem (rozmowa telefoniczna, spotkanie, wideokonferencja itp.),
- selekcja i wybór kandydatów najlepiej odpowiadających potrzebom klienta,
- rekomendacje kandydatów klientom.

Etap realizacji usługi po stronie klienta:

- analiza rekomendowanych kandydatów,
- kontakt z kandydatem (rozmowa telefoniczna, spotkanie, wideokonferencja itp.),
- wybór ostateczny i decyzja o zatrudnieniu wybranego kandydata.

Warunki konieczne przetwarzania danych kandydatów w procesie rekrutacji:

- zgoda kandydata (art. 6 pkt 1 lit. a RODO),
- dopełnienie obowiązku informacyjnego (art. 13 RODO).

Kandydat może udzielić zgody na **wszystkie procesy rekrutacyjne** prowadzone przez agencję, co daje możliwość udostępniania jego danych wielu potencjalnym pracodawcom. W takiej sytuacji dane kandydata najczęściej umieszczane są w bazie kandydatów, a ich przetwarzanie oparte jest na ogólnej zgodzie kandydata na korzystanie z jego danych do procesów rekrutacyjnych. **Dobrą praktyką jest potwierdzanie akceptacji kandydata na udostępnienie jego danych konkretnym klientom, których agencja chce zarekomendować do pracy.** Uzyskujemy wtedy pewność, że przedstawiamy potencjalnemu pracodawcy kandydata, który jest zainteresowany daną propozycją pracy.

Kandydat ma także prawo zgodzić się tylko na **niektóre procesy rekrutacyjne** (np. do konkretnej firmy albo branży). Wtedy proponowanie ofert i kontakt z kandydatem powinny być ograniczone do działania w tym zakresie, na który wyraził zgodę.

Prawem kandydata jest także wyrażenie zgody **wyłącznie na jeden proces rekrutacyjny**, w którym chce on wziąć udział (np. aplikując na ogłoszenie do konkretnej pracy lub firmy kandydat może zgodzić się, aby jego dane osobowe były przetwarzane wyłącznie w tym procesie). W takiej sytuacji agencja nie może przetwarzać danych tego kandydata w innych procesach rekrutacyjnych albo umieścić jego danych w bazie.

PRACA TYMCZASOWA

Podstawowe role pełnione przez agencję i pracodawcę użytkownika

Na etapie rekrutacji do pracy tymczasowej agencja pracy tymczasowej pełni rolę administratora danych osobowych kandydatów. Po zatrudnieniu pracownika tymczasowego w celu skierowania go do wykonywania pracy tymczasowej na rzecz pracodawcy użytkownika, agencja pracy tymczasowej jest administratorem jego danych osobowych jako pracodawca.

Analiza relacji pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem oraz roli pracodawcy użytkownika w świetle RODO musi być dokonywana z uwzględnieniem przepisów Ustawy o zatrudnianiu pracowników tymczasowych. W powołanym akcie prawnym przyjęto charakterystyczny dla zatrudnienia tymczasowego udział trzech podmiotów: pracownika tymczasowego, pracodawcy – agencji pracy tymczasowej i pracodawcy użytkownika, oraz specyficzną konstrukcję, wyodrębniającą ten rodzaj zatrudnienia o charakterze trójstronnym spośród innych nietypowych form zatrudnienia. Tę specyfikę tworzy w szczególności znajdująca swoje umocowanie w Ustawie o zatrudnianiu pracowników tymczasowych konstrukcja przejęcia części praw i obowiązków pracodawcy przez podmiot, który nie jest pracodawcą w sensie formalnym, ale w praktyce przysługuje mu szereg uprawnień pracodawcy, **na rzecz i pod kierownictwem którego świadczona jest praca tymczasowa (vide art. 1 ust. 2 Ustawy o zatrudnianiu pracowników tymczasowych)**. Wśród istotnych ustawowych obowiązków pracodawcy użytkownika **(które realizuje we własnym imieniu i dla osiągnięcia własnych celów)**, które tradycyjnie należą do obowiązków pracodawcy, a które mają istotne znaczenie dla oceny roli pełnionej przez ten podmiot wg RODO, należy wymienić między innymi następujące:

1. pracodawca użytkownik wyznacza pracownikowi tymczasowemu zadania i kontroluje ich wykonanie (art. 2 ust. 1 Ustawy o zatrudnianiu pracowników tymczasowych),
2. pracodawca użytkownik informuje agencję zatrudnienia o wynagrodzeniu, jakie ma być wypłacane pracownikom tymczasowym (art. 9 ust. 2 pkt 1 Ustawy o zatrudnianiu pracowników tymczasowych),

3. 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 o zatrudnianiu pracowników tymczasowych),
4. 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 o zatrudnianiu pracowników tymczasowych),
5. pracodawca użytkownik prowadzi ewidencję czasu pracownika tymczasowego w zakresie i na zasadach obowiązujących w stosunku do pracowników (art. 14 ust. 2 pkt 2 Ustawy o zatrudnianiu pracowników tymczasowych),
6. pracodawca użytkownik prowadzi ewidencję osób wykonujących pracę tymczasową (art. 14 a Ustawy o zatrudnianiu pracowników tymczasowych),
7. poprzez sprawowanie nadzoru nad przebiegiem pracy, pracodawca użytkownik może zdecydować np. o przyznaniu premii, nagrody, ale również zastosowaniu kary porządkowej, czy rozwiązaniu stosunku pracy z danym pracownikiem tymczasowym (art. 2 ust. 1 i art. 14 ust. 1 Ustawy o zatrudnianiu pracowników tymczasowych),
8. 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 o zatrudnianiu pracowników tymczasowych),
9. pracodawca użytkownik ma obowiązek stosować wobec pracowników tymczasowych tzw. zasadę równego traktowania (art. 15 Ustawy o zatrudnianiu pracowników tymczasowych).

Ustawowy zakres praw i obowiązków pracodawcy użytkownika jest znacznie szerszy, a dodatkowo może zostać poszerzony w umowie o świadczenie usług zawieranej z agencją. Ponadto, należy także przywołać przepis art. 5 Ustawy, zgodnie z którym w zakresie nieuregulowanym odmiennie przepisami Ustawy do pracodawcy użytkownika (a nie tylko do agencji pracy tymczasowej) stosuje się odpowiednio przepisy prawa pracy dotyczące pracodawcy.

Powyższe oznacza, że praktycznie od momentu przekazania pracodawcy użytkownikowi listy pracowników tymczasowych, którzy stawią się do pracy w jego zakładzie w związku z wykonaniem umowy o świadczenie usług pracy tymczasowej, pracodawca użytkownik zaczyna przetwarzać dane tych pracowników wyłącznie dla siebie (we własnym imieniu, a nie w imieniu agencji), przy pomocy własnych środków i wykonując w stosunku do tych osób obowiązki pracodawcy. Jest to samodzielna rola pracodawcy użytkownika, w której pracodawca użytkownik nie działa na zlecenie agencji, zaś obowiązki, które wykonuje nie są wykonaniem zobowiązań wobec agencji zawartych w umowie, ale realizowaniem samodzielnej roli pracodawcy użytkownika zapisanej w Ustawie o zatrudnianiu pracowników tymczasowych. W praktyce można by mnożyć przykłady działania pracodawcy użytkownika na własny rachunek z wykorzystaniem danych osobowych pracowników tymczasowych, np. prowadzenie szkoleń z zakresu BHP, prowadzenie ewidencji czasu pracy, sporządzanie protokołów powypadkowych, prowadzenie ewidencji okresów zatrudnienia, wydawanie kart dostępowych do zakładu pracy, identyfikatorów pracownika, ustalanie rozkładów i harmonogramów czasu pracy, 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 itd.

Zdaniem autorów niniejszego Kodeksu, w zakresie wykonania wszystkich powołanych wyżej czynności (a także innych, dotyczących samodzielnego organizowania pracy tymczasowej z udziałem pracownika tymczasowego i wykonywania obowiązków pracodawcy użytkownika na podstawie Ustawy o zatrudnianiu pracowników tymczasowych) pracodawca użytkownik **pełni samodzielną rolę administratora danych, działając we własnym celu** (pełnienia roli faktycznego pracodawcy, który jest odbiorcą pracy tymczasowej, sprawuje nadzór i kontrolę nad jej przebiegiem), i **posługując się własnymi środkami przetwarzania**.[3]

3 Odmiennie uważa M. Kawecki w: Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, str. 220-221, Wydawnictwo C.H. Beck Warszawa 2018. Autor ten prezentuje pogląd, że administratorem danych osobowych pracowników tymczasowych jest agencja pracy tymczasowej, które może i powinna powierzyć pracodawcy użytkownikowi niektóre czynności związane z przetwarzaniem danych. Zdaniem autora nie można wykluczyć, że w pewnych przypadkach pracodawca użytkownik będzie również administratorem danych pracownika tymczasowego, ale wyłącznie w zakresie dostępu do ewentualnych szkoleń na warunkach określonych w art. 15 ust. 2 Ustawy.

Z uwagi na pełnienie w procesie świadczenia usług pracy tymczasowych samodzielnych ról administratorów danych osobowych pracowników tymczasowych, uzasadnione jest, aby wymiana danych osobowych tych pracowników pomiędzy agencją pracy tymczasowej a pracodawcą użytkownikiem odbywała się w oparciu o udostępnianie danych, a nie w oparciu o umowę powierzenia przetwarzania.[4] Zdaniem autorów niniejszego kodeksu przyjęcie stanowiska, zgodnie z którym w powyższej relacji mamy do czynienia z powierzeniem danych osobowych, prowadziłoby do niedającego się zaakceptować rozwiązania, w ramach którego pracodawca użytkownik wykonując obowiązki pracodawcy i organizując pracę pracowników tymczasowych przetwarza dane osobowe w imieniu agencji zatrudnienia.

Przetwarzanie danych osobowych w poszczególnych etapach świadczenia usług pracy tymczasowej

Ważne:
pozyskiwanie danych kandydatów na pracowników tymczasowych jest oparte na przepisach prawa (art. 6 ust 1 pkt b RODO) i przesłance zgody (art. 6 ust. 1 pkt a RODO). W obu przypadkach konieczne jest dopełnienie obowiązku informacyjnego.

Rekrutacja – pozyskiwanie danych:

- z inicjatywy kandydata (osobiste dostarczanie i przesyłanie CV, wypełnianie aplikacji online, itp.),
- z z inicjatywy agencji (ogłoszenia rekrutacyjne, spotkania rekrutacyjne osobiste dostarczanie lub przesyłanie CV, wypełnianie aplikacji online, itp.).

Etap realizacji usługi pracy tymczasowej po stronie agencji:

- analiza zamówienia pracodawcy użytkownika,
- selekcja i wybór kandydatów najlepiej odpowiadających potrzebom pracodawcy użytkownika,
- zatrudnienie pracownika tymczasowego i udostępnienie jego danych pracodawcy użytkownikowi.

Etap realizacji usługi pracy tymczasowej po stronie pracodawcy użytkownika:

- organizowanie pracy z udziałem pracownika tymczasowego,
- wykonywanie praw i obowiązków pracodawcy użytkownika wynikających z Ustawy i umowy z agencją pracy tymczasowej.

---

4 Odmiennie M. Kawecki, op.cit., str. 221.

DELEGOWANIE PRACOWNIKÓW DO PRACY ZA GRANICĘ W RAMACH ŚWIADCZENIA USŁUG

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

Delegowanie pracowników w ramach świadczenia usług co do zasady najczęściej przybiera postać:

- wysyłania pracowników bezpośrednio przez pracodawcę, w przypadku którego dedykowani pracownicy czasowo świadczą pracę u zagranicznego kontrahenta pracodawcy (np. w ramach obsługi danego projektu),
- wysyłania pracowników tymczasowych świadczących pracę na rzecz i pod kierownictwem zagranicznego pracodawcy użytkownika.

W obu przypadkach, zarówno na etapie rekrutacji, jak i na etapie zatrudnienia, pracodawca (w przypadku zatrudnienia 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 w państwie członkowskim na rzecz podmiotu będącego odbiorcą usługi.

W obu wariantach odbiorca usługi (odpowiednio pracodawca użytkownik, kontrahent pracodawcy, do którego pracownik jest czasowo kierowany), również występuje w charakterze administratora danych osobowych 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 wydawanie poleceń i nadzorowanie procesu pracy. Z kolei w ramach wariantu czasowego kierowania pracownika do świadczenia pracy u zagranicznego kontrahenta, kontrahent ten administruje danymi np. na potrzeby weryfikacji jakości pracy, czasu w jakim jest ona świadczona, czy też wydajności procesu pracy.

W obu wariantach wymiana danych osobowych następuje w oparciu o ich udostępnienie. Należy w tym

wypadku wykluczyć instytucję powierzenia przetwarzania danych, albowiem każdy ze wskazanych powyżej podmiotów działa we własnym imieniu i realizuje odrębny cel. Każdy zatem zobowiązany jest spełnić względem delegowanego pracownika obowiązek informacyjny. W obu przypadkach rekomendowane jest pozyskanie zgody pracownika na udostępnienie jego danych osobowych, odpowiednio zagranicznemu pracodawcy użytkownikowi lub kontrahentowi pracodawcy delegującego.

Przetwarzanie danych osobowych w poszczególnych etapach świadczenia usług delegowania

Ważne:
Rekomenduje się uzyskanie zgody pracownika delegowanego na udostępnienie jego danych osobowych zagranicznemu pracodawcy użytkownikowi lub kontrahentowi pracodawcy delegującego.

Etap rekrutacji:
na etapie rekrutacji osoby, która zostaje delegowana, dane osobowe przetwarzane są na podstawie jej zgody oraz przepisów Kodeksu pracy (w przypadku zatrudnienia w ramach stosunku pracy), przy czym przetwarzanie następuje z inicjatywy kandydata (osobiste dostarczanie i przesyłanie CV, wypełnianie aplikacji online, itp.) lub z inicjatywy podmiotu zatrudniającego (ogłoszenia rekrutacyjne, spotkania rekrutacyjne, itp.).

Etap zatrudnienia:
na etapie zatrudnienia podstawą przetwarzania jest dany stosunek prawny (stosunek pracy, umowa cywilnoprawna) oraz usprawiedliwiony interes administratora danych.

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 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).

Zagraniczne systemy dot. delegowania, zgłaszania i ewidencjonowania pracowników delegowanych (np. francuski SIPSI) z reguły wymagają danych osobowych wykraczających poza standardowy katalog (np. obowiązkowe zdjęcie pracownika delegowanego).

OUTSOURCING

Usługi świadczone w ramach outsourcingu realizowane są przy wykorzystaniu personelu zaangażowanego na potrzeby realizacji danej usługi (personel agencji lub innego podmiotu świadczącego usługę). Z punktu widzenia przetwarzania danych osobowych podmiot świadczący usługę jest administratorem danych osobowych personelu (zarówno na etapie jego rekrutacji, jak i zatrudnienia).

Odbiorcę danej usługi należy również kwalifikować jako administratora danych osobowych. Wynika to z faktu, że po jego stronie występują własne cele, które mogą obejmować m. in.: potrzebę weryfikacji jakości usługi, czasu w jakim jest ona świadczona, czy też wydajności całego procesu, zapewnienia dostępu do budynku i pomieszczeń, zaopatrzenia w środki ochrony indywidualnej, ewentualne przekazania narzędzi niezbędnych do realizacji usługi i inne uzasadnione. Wymiana danych osobowych następuje w oparciu o ich udostępnienie. Należy w tym wypadku wykluczyć instytucję powierzenia przetwarzania danych, albowiem każdy ze wskazanych powyżej podmiotów działa we własnym imieniu i realizuje odrębny cel. Każdy zatem zobowiązany jest spełnić względem osoby świadczącej usługi obowiązek informacyjny.

Obowiązki administratora danych

7

OBOWIĄZKI ADMINISTRATORA DANYCH

Prowadzenie rejestru czynności – art.30 ust. 1 RODO

Administrator i jego przedstawiciel mają obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, za które ponoszą odpowiedzialność.

Rejestr prowadzony jest w formie pisemnej, w tym elektronicznej. Ma charakter dokumentu wewnętrznego, ale jest udostępniany na żądanie organu nadzorczego w celu monitorowania prowadzonego przetwarzania.

Obowiązek prowadzenia rejestru **nie ma zastosowania** wobec administratora/przetwarzającego zatrudniającego mniej niż 250 osób, chyba że czynności przetwarzania, które wykonuje:

- mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie mają charakteru sporadycznego lub obejmują szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub dotyczą wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Przykładowy szablon rejestru czynności przetwarzania:

Funkcja	Nazwa	Dane kontaktowe
Administrator		
Współadministrator[1]		
Przedstawiciela administratora[1]		
Inspektor Danych Osobowych[1]		
Cel przetwarzania	np. przeprowadzenie rekrutacji	np. spełnienie obowiązków wynikających z przepisów prawa
Kategorie osób, których dane dotyczą	np. kandydaci do pracy	np. pracownicy
Kategorie danych osobowych	np. imię i nazwisko, adres e-mail, numer telefonu	np. imię i nazwisko, adres zamieszkania, numer telefonu
Kategorie odbiorców, którym dane osobowe zostały bądź będą udostępnione	np. klient Agencji	np. dane nie są ujawniane odbiorcom
Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane[1]	np. Rosja	np. dane nie są przekazywane
Planowany termin usunięcia kategorii danych[2]	np. zakończenie rekrutacji	np. 50 lat od dnia rozwiązania/ wygaśnięcia umowy z pracownikiem
Ogólny opis techniczny i organizacyjny środków bezpieczeństwa[2]	np. zastosowano pseudonimizację i szyfrowanie danych osobowych	np. zastosowano szyfrowanie danych osobowych

[1] jeżeli ma zastosowanie
[2] jeżeli jest to możliwe

Powołanie inspektora danych osobowych – art. 37 RODO

Rozporządzenie o ochronie danych przewiduje obowiązek wyznaczenia Inspektora ochrony danych (zwanego dalej „DPO" od ang. „Data Protection Officer") dla administratorów i podmiotów przetwarzających wówczas, 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 oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Co może być wyznacznikiem dużej skali?

- liczba osób, których dane dotyczą,
- zakres przetwarzanych danych,
- okres przez jaki dane są przetwarzane,
- zakres geograficzny przetwarzania danych.

DPO może być zarówno osoba z wewnątrz, jak i spoza organizacji, a także podmiot świadczący usługę. Osoba/podmiot może być DPO dla grupy przedsiębiorstw np. grupy kapitałowej. Istotne jest, aby inspektor był „łatwo dostępny" dla osób wewnątrz organizacji, które podejmują decyzje oraz działania związane z przetwarzaniem danych osobowych. Wynika to z jego obowiązków, do których należą m.in.:

- informowanie administratora, podmiotu oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia,
- monitorowanie zgodności z RODO,
- współpraca z organem nadzorczym.

DPO powinien posiadać odpowiedni poziom wiedzy na temat prawa i praktyk w dziedzinie ochrony danych, w tym dogłębną znajomość przepisów RODO nt. operacji przetwarzania danych, jak i zabezpieczeń stosowanych u administratora.

W ramach wypełniania zadań DPO nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte czy celu jaki powinien zostać osiągnięty. Nie może zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu ochrony danych. Powinien mieć zapewnioną niezależność.

Obowiązkiem administratora lub podmiotu przetwarzającego jest opublikowanie danych kontaktowych DPO (adres e-mail, telefon kontaktowy) oraz zawiadomienie właściwego organu nadzorczego o danych kontaktowych DPO.

Agencja, która wyznaczyła inspektora, zawiadamia o tym Organ w terminie 14 dni od dnia wyznaczenia. Zasady dokonania tego zgłoszenia określa art. 10 ustawy z dnia 10 maja 2018 roku o ochronie danych danych osobowych.

Zgłaszanie incydentów

Zgodnie z art. 33 RODO przewidziane są dwa rodzaje incydentów (zgłoszenia naruszeń ochrony danych osobowych):

- zgłoszenie przez administratora organowi nadzorczemu zaistnienia incydentu (art. 33 ust. 1 RODO),
- zgłoszenie przez podmiot przetwarzający administratorowi zaistnienia incydentu (art. 33 ust. 2 RODO).

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** po stwierdzeniu naruszenia, ma obowiązek zgłosić je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie naruszenia ochrony danych osobowych do organu nadzoru powinno zawierać co najmniej:

- opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,

Ważne:
Administrator jest zobowiązany do dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

- opis możliwych konsekwencji naruszenia ochrony danych osobowych,
- opisy środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadamianie osoby, której dane dotyczą o naruszeniu

Jeżeli naruszenie ochrony danych osobowych spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi również zawiadomić osoby, których dane dotyczą. Wyjątki od tej zasady dotyczą tylko trzech przypadków:

Ważne:
Jeżeli administrator nie zawiadomi osób, których dane zostały naruszone, zawiadomi je zbyt późno lub w niewłaściwy sposób, może być na niego nałożona kara administracyjna.

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

Administracyjne kary pieniężne

8

ADMINISTRACYJNE KARY PIENIĘŻNE

W przypadku stwierdzenia naruszenia przepisów RODO, organ ma prawo nałożyć na administratora lub podmiot przetwarzający odpowiednie kary pieniężne – **art. 83 RODO**.

Naruszenie przepisów dotyczących m.in. obowiązków administratora i podmiotu przetwarzającego w zakresie stosowania zasady ochrony danych w fazie projektowania, domyślnej ochrony danych, notyfikacji naruszeń, prowadzenia rejestru czynności przetwarzania czy niewyznaczenia inspektora ochrony danych wbrew takiemu obowiązkowi – podlegają administracyjnej karze pieniężnej w wysokości do **10 000 000 EUR**, a w przypadku przedsiębiorstw **do 2% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Naruszenie przepisów dotyczących m.in. podstawowych zasad przetwarzania danych osobowych, warunków uzyskania zgody czy niezgodnym z przepisami przekazaniem danych do państwa trzeciego – podlegają administracyjnej karze pieniężnej w wysokości **do 20 000 000 EUR**, a w przypadku przedsiębiorstw **do 4% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Przy ustalaniu wysokości kary pieniężnej organ zwraca m. in. uwagę na:

- charakter, wagę i czas trwania naruszenia,
- umyślny lub nieumyślny charakter naruszenia,
- działania podjęte w celu zminimalizowania szkody,
- sposób w jaki dowiedział się o naruszeniu,
- stosowanie zatwierdzonych kodeksów postępowania.

Administracyjne kary pieniężne nakładane są oprócz lub zamiast innych środków (np. nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony jej danych bądź wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania danych osobowych), (art. 58 ust. 2 RODO).

Wykaz dokumentów w zakresie RODO występujących najczęściej w agencjach zatrudnienia

WRAZ Z NIEKTÓRYMI WZORAMI

9

WYKAZ DOKUMENTÓW W ZAKRESIE RODO WYSTĘPUJĄCYCH NAJCZĘŚCIEJ W AGENCJACH ZATRUDNIENIA (wraz z niektórymi wzorami)

Klauzule zgody na przetwarzanie danych osobowych:

ZGODA 1

Wyrażam zgodę na przetwarzanie podanych przeze mnie danych osobowych (włączając fotografię zamieszczoną w CV) przez administratora danych ..... (nazwa administratora) dla celów prowadzenia rekrutacji, w której biorę udział, w tym na udostępnienie podanych przeze mnie danych osobowych potencjalnemu pracodawcy.

Oświadczam, że administrator danych osobowych spełnił w stosunku do mnie obowiązek informacyjny wynikający z przepisów prawa.

ZGODA 2

Wyrażam zgodę na przetwarzanie podanych przeze mnie danych osobowych (włączając fotografię zamieszczoną w CV) przez administratora danych ..... (nazwa administratora) dla celów prowadzenia przyszłych rekrutacji, w tym na przesyłanie mi ofert pracy oraz udostępnienie podanych przeze mnie danych osobowych potencjalnym pracodawcom.

Oświadczam, że administrator danych osobowych spełnił w stosunku do mnie obowiązek informacyjny wynikający z przepisów prawa.

Klauzule informacyjne dotyczące przetwarzania danych osobowych:

Zaleca się, aby klauzula informacyjna dotycząca przetwarzania danych osobowych w relacji cyfrowej (w odróżnieniu od papierowej) była podana w sposób warstwowy. Treść pierwszej warstwy, zawierającej

podstawowe informacje o przetwarzaniu powinna być wyświetlana łącznie z treścią zgód (na tym samym ekranie). Te podstawowe informacje powinny wskazywać: tożsamość administratora danych, cel przetwarzania danych oraz opis praw osoby, której dane dotyczą. Ponadto z informacji podanej w pierwszej warstwie powinno jasno wynikać, jakie są konsekwencje przetwarzania danych (np. niewyrażenie zgody na przetwarzanie danych skutkuje brakiem możliwości wzięcia udziału w procesie rekrutacyjnym). Kolejna warstwa informacji powinna być możliwa do odnalezienia i wyświetlenia w prosty sposób – nie można zmuszać osoby udzielającej zgód do aktywnego poszukiwania informacji znajdujących się w kolejnych warstwach klauzuli. Kolejną warstwę informacji może stanowić link (kod QR) do polityki prywatności.

REKRUTACJA PRACOWNIKÓW

Informujemy, że administratorem Państwa danych osobowych jest _____ (nazwa spółki oraz dane kontaktowe: adres i telefon)

Dane kontaktowe inspektora ochrony danych osobowych: _____(adres email lub/ i telefon). Państwa dane osobowe przetwarzane są dla celów udziału w procesie rekrutacji na stanowisko, na które Państwo aplikują, a w przypadku wyrażenia przez Państwa odrębnej zgody, również dla celów przyszłych rekrutacji.

Podstawę prawną przetwarzania danych osobowych stanowi Państwa zgoda, jak również przepisy ustawy z dnia 26 czerwca 1974 roku Kodeksu pracy (art. 221). Zgoda może być w każdej chwili cofnięta, przy czym jej cofnięcie pozostaje bez wpływu na zgodność z prawem przetwarzania, którego dokonano na jej podstawie. Cofnięcie zgody powoduje, że Państwa udział w procesach rekrutacji nie będzie możliwy.

Odbiorcami Państwa danych osobowych są: upoważnieni pracownicy administratora; podmioty przetwarzające dane w jego imieniu; podmioty współpracujące (w tym potencjalni pracodawcy, na rzecz

których prowadzone jest lub będzie rekrutacja).

Dane osobowe przetwarzane są przez czas trwania procesu rekrutacji, w którym biorą Państwo udział, a w przypadku wyrażenia przez Państwa osobnej zgody również przez czas trwania przyszłych rekrutacji (nie dłużej niż przez 24 miesiące), w każdym razie nie dłużej niż do dnia wycofania zgody.

Przysługuje Państwu prawo żądania: dostępu do swoich danych osobowych, ich usunięcia, przenoszenia, sprostowania, ograniczenia przetwarzania, jak również prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Podanie danych osobowych jest dobrowolne, niemniej stanowi warunek Państwa udziału w procesie rekrutacji.

PRACA TYMCZASOWA

Informujemy, że administratorem danych osobowych osoby świadczącej pracę tymczasową _____. Dane kontaktowe inspektora ochrony danych osobowych: _____.

Przetwarzanie obejmuje udostępnione przez Państwa dane osobowe niezbędne do realizacji stosunku pracy/umowy cywilnoprawnej w zakresie określonym obowiązującymi przepisami, w tym przepisami ustawy z dnia 26 czerwca 1974 roku Kodeks pracy, ustawy z dnia 23 kwietnia 1964 roku Kodeks cywilny oraz ustawy z dnia 9 lipca 2003 roku o zatrudnianiu pracowników tymczasowych.

Podstawę prawną przetwarzania Państwa danych osobowych stanowi umowa o pracę tymczasową/umowa cywilnoprawna zawartą pomiędzy administratorem danych osobowych, a osobą świadczącą

pracę tymczasową, a w zakresie stosunku pracy również przepisy ustawy z dnia 26 czerwca 1974 Kodeks pracy (art. 221).

Administrator przetwarza dane osobowe dla celów realizacji stosunku pracy/umowy cywilnoprawnej oraz na potrzeby wykonywania obowiązków określonych obowiązującymi przepisami, w tym przepisami prawa pracy, ubezpieczeń społecznych, prawa podatkowego.

Odbiorcami Państwa danych osobowych są: upoważnieni pracownicy administratora; podmioty przetwarzające dane w jego imieniu; podmioty współpracujące (w tym pracodawcy użytkownicy, na rzecz których świadczycie Państwo pracę tymczasową); jak również organy administracji publicznej, przy zachowaniu wymogów określonych obowiązującymi przepisami, w tym wymogu poufności oraz w zakresie niezbędnym do dokonania danej czynności.

Państwa dane osobowe przetwarzane są przez czas trwania stosunku pracy/umowy cywilnoprawnej, a po ich zakończeniu przez okres określony obowiązującymi przepisami, w tym w zakresie przechowywania akt pracowniczych.

Przysługuje Państwu prawo dostępu do swoich danych osobowych, ich usunięcia, przenoszenia, sprostowania, ograniczenia przetwarzania, jak również prawo do wniesienia skargi do właściwego organu nadzorczego.

Podanie ww. danych osobowych jest wymogiem ustawowym określonym przez przepisy, w tym przepisy ustawy z ustawy z dnia 26 czerwca 1974 roku Kodeks pracy oraz przepisy ustawy z dnia 9 lipca 2003 roku o zatrudnianiu pracowników tymczasowych.

Potwierdzenie zapoznania się, podpis pracownika tymczasowego, data. .....

PRACOWNICY WEWNĘTRZNI

Informujemy, że administratorem danych osobowych pracownika jest _____.

Dane kontaktowe inspektora ochrony danych osobowych: _____.

Przetwarzanie obejmuje udostępnione przez Państwa dane osobowe niezbędne do realizacji stosunku pracy w zakresie określonym obowiązującymi przepisami, w tym przepisami ustawy z dnia 26 czerwca 1974 roku Kodeks pracy.

Podstawę prawną przetwarzania Państwa danych osobowych stanowi umowa o pracę zawartą pomiędzy administratorem danych osobowych, a pracownikiem, jak również przepisy ustawy z dnia 26 czerwca 1974 Kodeks pracy (art. 221).

Administrator przetwarza dane osobowe dla celów realizacji stosunku pracy oraz na potrzeby wykonywania obowiązków określonych obowiązującymi przepisami, w tym przepisami prawa pracy, ubezpieczeń społecznych, prawa podatkowego.

Odbiorcami Państwa danych osobowych są: upoważnieni pracownicy administratora; podmioty przetwarzające dane w jego imieniu; podmioty współpracujące; jak również organy administracji publicznej, przy zachowaniu wymogów określonych obowiązującymi przepisami, w tym wymogu poufności oraz w zakresie niezbędnym do dokonania danej czynności.

Państwa dane osobowe przetwarzane są przez czas trwania stosunku pracy, a po jego zakończeniu przez okres określony obowiązującymi przepisami, w tym w zakresie przechowywania akt pracowniczych.

Przysługuje Państwu prawo dostępu do swoich danych osobowych, ich usunięcia, przenoszenia, sprostowania, ograniczenia przetwarzania, jak również prawo do wniesienia skargi do właściwego organu nadzorczego.

Podanie ww. danych osobowych jest wymogiem ustawowym określonym przez przepisy, w tym przepisy ustawy z ustawy z dnia 26 czerwca 1974 roku Kodeks pracy.

potwierdzenie zapoznania się, podpis pracownika, data .....

Pozostałe dokumenty:

- umowa powierzenia danych osobowych (zawierana pomiędzy administratorem danych osobowych a podmiotem przetwarzającym),
- rejestr czynności przetwarzania (administrator danych osobowych),
- rejestr kategorii czynności przetwarzania (podmiot przetwarzający),
- rejestr incydentów,
- polityka bezpieczeństwa danych osobowych,
- instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Polskie Forum HR

www.polskieforumhr.pl

Polskie Forum HR jest najbardziej wpływową organizacją pracodawców reprezentującą rynek agencji zatrudnienia. Od 2002 roku działa na rzecz budowy efektywnego rynku pracy poprzez wpieranie zrównoważonego rozwoju usług w zakresie szeroko rozumianego doradztwa personalnego. Jest uznanym partnerem społecznym w Polsce i Europie.

Firmy członkowskie Polskiego Forum HR zatrudniają ponad **2,5 tys.** pracowników wewnętrznych w ponad 300 oddziałach na terenie całego kraju. W ubiegłym roku wsparły w zatrudnieniu blisko **300 tys.** osób zarówno w formie pracy tymczasowej, rekrutacji stałych, jak i delegowania za granicę.