Ochrona danych osobowych w miejscu pracy Poradnik dla pracodawców

Poradnik RODO

październik 2018

Spis treści

01

1. WPROWADZENIE

Poradnik jest zaktualizowaną i rozszerzoną wersją materiałów opublikowanych przez Generalnego Inspektora Ochrony Danych Osobowych[1], która uwzględnia zmiany wynikające z postanowień ogólnego rozporządzenia o ochronie danych[2] oraz nowelizacji Kodeksu pracy wprowadzonej ustawą z 10 maja 2018 r. o ochronie danych osobowych[3].

Starając się wyjść naprzeciw trendom, jakie panują na rynku pracy poradnik obejmie kwestie związane z zatrudnieniem na podstawie stosunku pracy oraz w oparciu o tzw. cywilnoprawne lub niepracownicze formy zatrudnienia, na które pracodawcy decydują się coraz częściej, np. gdy wymaga tego charakter wykonywanej pracy lub chcą elastyczniejszej formy kształtowania relacji pomiędzy stronami umowy. Stosunkiem pracy nazywamy zaś sytuację, w której pracownik w zamian za wynagrodzenie zobowiązuje się do wykonywania na rzecz pracodawcy pracy określonego rodzaju, pod jego kierownictwem oraz w miejscu i czasie przez niego wyznaczonym. Charakteryzuje się on zatem, co najmniej podporządkowaniem służbowym oraz odpłatnym charakterem pracy, która dodatkowo wykonywana jest na ryzyko pracodawcy. Z zatrudnianiem na podstawie stosunku pracy wiążą się liczne uprawnienia i obowiązki zarówno po stronie pracownika, jak i pracodawcy. Jego główną ideą jest tzw. zasada uprzywilejowania pracownika. Ustawodawca wyszedł bowiem z założenia, że ze względu na nierówność stron takiej umowy, pewne określone (minimalne) prawa pracownika powinny być wyraźnie wskazane w przepisach prawa, a postanowienia kształtujące stosunek pracy nie mogą być od nich mniej korzystne.

Publikację poradnika poprzedziły szerokie konsultacje publiczne, które spotkały się z bardzo dużym odzewem. Prezes Urzędu Ochrony Danych Osobowych serdecznie dziękuje wszystkim interesariuszom za przesłane uwagi i propozycje. Nie wszystkie z podnoszonych w trakcie konsultacji kwestii znalazły odzwierciedlenie w treści poradnika, lecz będzie on systematycznie uzupełniany, bądź kwestie te zostaną poruszone w innych materiałach UODO.

Poradnik w swoim założeniu ma służyć pomocą pracodawcom w ich codziennej pracy. Dlatego zrezygnowano w nim z prezentowania rozbudowanych analiz prawnych, koncentrując się na praktycznych wskazówkach.

Informacje zawarte w poradniku nie uwzględniają proponowanych zmian w Kodeksie pracy, które nadal mają status projektu.

---

1 Por. Dekalog rekrutera, który został opublikowany na: https://giodo.gov.pl/pl/259/10318 oraz dokument pt. Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników, który został opublikowany na: https://giodo.gov.pl/pl/1520155/7917.

2 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm. ,) zwane dalej: RODO.

3 Ustawa z dnia 10 maja 2018 r. r. o ochronie danych osobowych (Dz. U. z 2018 r. poz.1000).

02

2. POSZUKIWANIE PRACY

Bez względu na to, w jaki sposób pracodawca będzie poszukiwał kandydatów do pracy, proces ten zawsze będzie wiązał się z pozyskiwaniem przez niego danych osobowych zawartych w dokumentach rekrutacyjnych (CV, listach motywacyjnych, świadectwach pracy, listach referencyjnych, zaświadczeniach itd.). Pracodawca powinien przetwarzać tylko takie dane, które są niezbędne ze względu na cel ich zbierania, jakim jest podjęcie przez niego decyzji o zatrudnieniu nowego pracownika. Innymi słowy, pracodawca nie może żądać od kandydata danych nadmiarowych, które nie są niezbędne do przeprowadzenia rekrutacji. Dane osobowe nie mogą być zbierane na zapas, „na wszelki wypadek", tj. bez wykazania zgodnego z prawem celu ich pozyskania i wykazania ich niezbędności dla realizacji tego celu przez administratora. Ponadto, żądanie przez pracodawcę od kandydatów do pracy informacji wykraczających poza to, co przede wszystkim przewidują przepisy prawa pracy może naruszać zarówno postanowienia RODO, jak i przepisy prawa pracy rodząc np. zarzut dyskryminacji.

2.1 Dane wymagane od kandydata w toku rekrutacji

Pracodawca może oczekiwać od kandydata do pracy podania mu danych, które ogólnie możemy określić, jako dane:

- identyfikacyjne (imię, nazwisko, imiona rodziców, data urodzenia);
- kontaktowe (adres zamieszkania) oraz
- o wykształceniu, umiejętnościach, doświadczeniu zawodowym (ukończonych szkołach oraz studiach, przebytych szkoleniach i kursach, poprzednich pracodawcach, zajmowanych stanowiskach oraz obowiązkach zawodowych)[4].

Jest to katalog danych, których pracodawca może żądać od kandydata do pracy, w celu podjęcia działań zmierzających do zawarcia z nim umowy[5]. Co istotne, z uwagi na specyfikę procesu rekrutacji, do zawarcia tej umowy wcale nie musi ostatecznie dojść.

---

4 Zakres danych, których pracodawca może żądać od osoby ubiegającej się o zatrudnienie wskazany został w art. 22^1 Kodeksu pracy oraz rozporządzeniu Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika.

5 Art. 6 ust. 1 lit. b RODO

Ważne!

Uwzględniając cel, jaki przyświeca gromadzeniu tych danych, tj. podjęcie przez pracodawcę decyzji o zatrudnieniu pracownika, która będzie się opierała na ocenie jego przydatności do pracy na określonym stanowisku, informacje przekazywanie przez pracownika muszą być konkretne, tj. nie mogą ograniczać się jedynie do zdawkowej informacji, że odbył jakieś kursy czy ukończył studia, bez wskazywania, jakie dokładnie.

Jakich danych pracodawca nie może żądać od kandydata do pracy?

Pracodawca nie może żądać od kandydata danych wykraczających poza zakres, który został wskazany w przepisach prawa, danych nadmiarowych, w szczególności takich, które nie mają związku z celem, jakim jest zatrudnienie pracownika (np. danych o stanie cywilnym, wyznaniu, poglądach religijnych czy orientacji seksualnej). Może się oczywiście zdarzyć, że osoba kandydująca na konkretne stanowisko będzie musiała spełnić pewne określone prawem wymogi, np. wymóg niekaralności i wówczas pracodawca będzie uprawniony do pozyskania informacji o nim w tym zakresie.

Czy pracodawca może zbierać informacje o karalności kandydata do pracy?

Zaświadczenie o niekaralności jest dokumentem zawierającym dane o wyrokach skazujących, czynach zabronionych lub powiązanych środkach bezpieczeństwa zawartych w Krajowym Rejestrze Karnym, którego funkcjonowanie jest uregulowane przepisami ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (ustawa o KRK). Zgodnie z art. 6 ust. 1 pkt 10 ustawy o KRK, prawo do uzyskania informacji o osobach, których dane osobowe zgromadzone zostały w rejestrze, przysługuje pracodawcom, w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej.

Pracodawca może żądać od przyszłego i obecnego pracownika dokumentów wynikających również z przepisów szczególnych, odnoszących się do konkretnych uregulowań wykonywania określonych zawodów. Jednakże pracodawca musi pamiętać, że w odniesieniu do danych dotyczących niekaralności, musi wynikać to wprost z przepisów prawa. Oznacza to, że pracodawca nie może żądać każdego dokumentu na wszelki wypadek, np. zaświadczenia o niekaralności, chyba że jest do tego uprawniony z mocy ustawy

Przykład:

Istnieją zawody, do których dostęp ograniczony jest ze względu na wymóg niekaralności:

- nauczyciele (art. 10 ust. 8a ustawy – Karta Nauczyciela),
- straż graniczna (art. 31 ust. 1 ustawy o Straży Granicznej),
- detektywi (art. 29 ust. 2 ustawy o usługach detektywistycznych),
- osoby ubiegającej się o zatrudnienie w podmiotach sektora finansowego (art. 3 ustawy z dnia z dnia 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego) – w zakresie dotyczącym skazania prawomocnym wyrokiem za przestępstwa wskazane w tej ustawie.

Czy pracodawca, który poszukuje pracowników cieszących się nieposzlakowaną opinią, może żądać od nich informacji o karalności?

Nie. Przepisy szczególne regulujące wykonywanie niektórych zawodów wskazują często na przesłankę nieposzlakowanej opinii, która jest terminem nieostrym i stanowi zwrot niedookreślony odwołujący się do przesłanek uznaniowych, o charakterze ocennym. Nie stanowi ona jednak podstawy do tego, aby pracodawca miał prawo przetwarzać dane pracownika o jego niekaralności, ponieważ nie wynika to bezpośrednio z przepisów prawa. Pracodawca nie może przetwarzać danych, o których mowa w art. 10 RODO nawet za zgodą pracownika. Podkreślić również należy, że przesłanka zgody, rozpatrywana na gruncie prawa pracy, wskazuje na nierówność podmiotów, w związku z tym w przedmiotowej sprawie nie miałaby podstawy zastosowania. Należy także podkreślić, że informacja, iż dana osoba nie widnieje w Krajowym Rejestrze Karnym jest również informacją zawierającą dane określone w art. 10 RODO. Zatem, każde zaświadczenie o niekaralności, które będzie zawierało informacje o wyrokach skazujących, czy też informację o tym, że dana osoba nie była skazana, będzie informacją dotyczącą wyroków skazujących i czynów zabronionych w rozumieniu RODO.

2.2 Czy pracodawca musi poinformować kandydatów do pracy o przetwarzaniu ich danych osobowych?

Tak. Każdy potencjalny pracodawca, który zbiera dane od kandydatów do pracy, jest zobowiązany poinformować te osoby o[6]:

- pełnej nazwie i adresie swojej siedziby,
- danych kontaktowych inspektora ochrony danych (o ile go wyznaczył),
- celu przetwarzania danych oraz podstawie prawnej przetwarzania,
- znanych mu w chwili gromadzenia danych odbiorcach danych (rozumianych szeroko) lub ich kategoriach,
- zamiarze transgranicznego przetwarzania danych (o ile taki istnieje),
- okresie, przez który dane będą przetwarzane bądź kryteriach ustalania tego okresu,
- przysługujących jej prawach do żądania dostępu do danych, w tym otrzymania ich kopii, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania,
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli dane są zbierane na podstawie zgody),
- prawie wniesienia skargi do Prezesa UODO,
- dobrowolności lub obowiązku podania danych i konsekwencjach ich nie podania.

6 Art. 13 RODO

Pracodawca ma obowiązek poinformować kandydata do pracy o tych okolicznościach w chwili pozyskiwania tych danych w sposób jasny, czytelny i łatwo dostępny dla kandydata. Może to zrobić np. w treści ogłoszenia o pracę lub w informacji zwrotnej bezpośrednio po otrzymaniu od kandydata aplikacji do pracy.

Przykład klauzuli informacyjnej

Administrator

Administratorem Państwa danych przetwarzanych w ramach procesu rekrutacji jest X, jako pracodawca.

Inspektor ochrony danych

Mogą się Państwo kontaktować z inspektorem ochrony danych osobowych pod adresem: …

Cel i podstawy przetwarzania

Państwa dane osobowe w zakresie wskazanym w przepisach prawa pracy *będą* przetwarzane w celu przeprowadzenia obecnego postępowania rekrutacyjnego *(art. 6 ust. 1 lit. b RODO)*, natomiast inne dane, w tym dane do kontaktu, na podstawie zgody *(art. 6 ust. 1 lit. a RODO)*, która może zostać odwołana w dowolnym czasie.

X będzie przetwarzał Państwa dane osobowe, także w kolejnych naborach pracowników, jeżeli wyrażą Państwo na to zgodę *(art. 6 ust. 1 lit. a RODO)*, która może zostać odwołana w dowolnym czasie.

Jeżeli w dokumentach zawarte są dane, o których mowa w art. 9 ust. 1 RODO konieczna będzie Państwa zgoda na ich przetwarzanie *(art. 9 ust. 2 lit. a RODO)*, która może zostać odwołana w dowolnym czasie.

Przepisy prawa pracy: *art. 22 Kodeksu pracy oraz §1 rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika.*

Odbiorcy danych osobowych

Odbiorcą Państwa danych osobowych będzie …..

Okres przechowywania danych

Państwa dane zgromadzone w obecnym procesie rekrutacyjnym będą przechowywane do zakończenia procesu rekrutacji.

W przypadku wyrażonej przez Państwa zgody na wykorzystywane danych osobowych dla celów przyszłych rekrutacji, Państwa dane będą wykorzystywane przez 9 miesięcy.

Prawa osób, których dane dotyczą

Mają Państwo prawo do:

1) prawo dostępu do swoich danych oraz otrzymania ich kopii
2) prawo do sprostowania (poprawiania) swoich danych osobowych;
3) prawo do ograniczenia przetwarzania danych osobowych;
4) prawo do usunięcia danych osobowych;
5) prawo do wniesienia skargi do Prezes UODO (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych

Podanie przez Państwa danych osobowych w zakresie wynikającym z art. 22^1 Kodeksu pracy jest niezbędne, aby uczestniczyć w postępowaniu rekrutacyjnym. Podanie przez Państwa innych danych jest dobrowolne.

2.3 Znaczenie zgody na przetwarzanie danych osobowych

Zgoda jest jedną z podstaw prawnych uprawniających do przetwarzania danych. Dotychczasowa praktyka zamieszczenia w liście motywacyjnym CV zgody na przetwarzanie danych w celach rekrutacyjnych nie jest właściwa. Zgoda, a w szczególności wyraźna zgoda na przetwarzanie wybranych danych może być niezbędna jedynie w określonych sytuacjach.

Ważne!

„Zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Czy pracodawca może przetwarzać dane zamieszczone przez kandydata w CV, które wykraczają poza to, co przewidują przepisy prawa pracy?

Zdarza się, że osoby kandydujące do pracy przekazują z własnej inicjatywy więcej danych, niż wskazane w Kodeksie pracy. W takiej sytuacji dane osobowe kandydata, o ile nie należą do szczególnej kategorii danych, są przetwarzane przez potencjalnego pracodawcę na podstawie zgody, która może polegać na oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Aplikacja kandydata stanowi zazwyczaj odpowiedź na ogłoszenie o pracę pracodawcy, kandydat jest świadomy, do jakiego podmiotu składa aplikację oraz w jakim celu jego dane mają być przetwarzane. Kandydat zna jednocześnie zakres danych, jaki przekazuje pracodawcy. Oznacza to, że zwykłe dane osobowe, które wykraczają poza zakres uregulowany przepisami prawa pracy, są przetwarzane przez pracodawcę na podstawie zgody kandydata, która przejawia się przez działanie, polegające np. na przesłaniu pracodawcy życiorysu i listu motywacyjnego.

Dane osobowe dzielą się na trzy kategorie:

a) **dane tzw. zwykłe**, takie jak imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek, adres e-mail itp.,

b) szczególne kategorie danych osobowych (uprzednio zwane **danymi wrażliwymi**), wymienione w art. 9 RODO ujawniające:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby,

c) dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa wymienione w art. 10 rozporządzenia (uprzednio również zaliczane do **danych wrażliwych**).

Osoba ubiegająca się o pracę umieściła w CV szczególne kategorie danych (tzw. dane wrażliwe). Czy pracodawca może je przetwarzać?

W toku prowadzonej rekrutacji może zdarzyć się, że kandydat z własnej inicjatywy przekaże administratorowi dane osobowe np. o swoim stanie zdrowia. Jeżeli kandydat do pracy nie wyrazi odrębnej zgody na przetwarzanie tego rodzaju danych osobowych, a pracodawca nie legitymuje się przepisem prawa, który zobowiązuje go do ich przetwarzania, pracodawca powinien usunąć te dane ze swoich zasobów. Ewentualna zgoda na przetwarzanie szczególnych kategorii danych, powinna być wyraźna, np. w formie odrębnego oświadczenia. Są jednak pewne sytuacje, w których potencjalny pracodawca będzie uprawniony do przetwarzania szczególnych kategorii danych na podstawie odrębnych przepisów prawa. Przykładem takich regulacji są np. przepisy dotyczące wymogów dotyczących stanu zdrowia, jakie musi spełniać kandydat na policjanta.

Przykład

Art. 25 ust. 2 ustawy z dnia 6 kwietnia 1990 r. o policji (t.j. Dz.U. z 2017 r. ,poz. 2067) stanowi, że przyjęcie kandydata do służby w policji następuje po przeprowadzeniu postępowania kwalifikacyjnego mającego na celu ustalenie, czy kandydat spełnia warunki przyjęcia do służby w policji oraz określenie jego predyspozycji do pełnienia tej służby. Postępowanie kwalifikacyjne, składa się m.in. z testu sprawności fizycznej, test psychologicznego oraz ustalenia zdolności fizycznej i psychicznej do służby w policji.

Czy pracodawca może wykorzystać dane kandydatów do pracy pozyskane w konkretnym procesie rekrutacyjnych do celów przyszłych rekrutacji?

Nie, jeżeli kandydat nie wyraził na to zgody. Pracodawca po zakończeniu procesu rekrutacji powinien usunąć dane osobowe kandydata, jeżeli jednak kandydat do pracy, w składanych potencjalnemu pracodawcy dokumentach, wyraził zgodę na przetwarzanie jego danych w celu wzięcia udziału w przyszłych rekrutacjach prowadzonych przez pracodawcę, dane te mogą być w tym celu przetwarzane.

Przykład 1:

„Wyrażam zgodę na przetwarzanie danych w celu wykorzystania ich w kolejnych naborach prowadzonych przez X przez okres najbliższych 6 miesięcy."

Przykład 2:

„Wyrażam zgodę na przetwarzanie szczególnych kategorii danych, o których mowa w art. 9 ust. 1 RODO, które zamieściłem w liście motywacyjnym oraz załączonych do niego dokumentach."

Ważne!

Kandydat musi być poinformowany o możliwości i sposobie wycofania zgody. Sposób wycofania zgody powinien być równie łatwy, jak było jej wyrażenie.

Czy pracownik może wycofać swoją zgodę?

Tak. Zgoda na przetwarzanie danych w celach rekrutacyjnych może być wycofana w dowolnym momencie. W takiej sytuacji pracodawca traci uprawnienie do dalszego przetwarzania tych danych i powinien niezwłocznie je usunąć. O prawie do wycofania zgody pracodawca powinien poinformować pracownika w momencie pozyskania jego danych.

2.4 Prowadzenie rekrutacji on-line

Gromadzenie danych przez Internet jest obecnie jednym z najbardziej popularnych sposobów tworzenia baz danych, często wykorzystywanym także w procesie rekrutacji pracowników. Jeżeli potencjalny pracodawca zdecyduje się pozyskiwać dane kandydatów przez Internet, powinien wdrażać odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności tych osób związanym ze specyfiką cyberprzestrzeni. Obowiązek ten ma zastosowanie także do administratorów innych niż pracodawcy, np. agencji zatrudnienia. Każdy bowiem administrator, bez względu na sposób gromadzenia danych, musi działać zgodnie z przepisami o ochronie danych osobowych.

Na co pracodawca powinien zwrócić uwagę decydując się na poszukiwanie pracowników za pośrednictwem stron internetowych?

W zależności od tego czy zadaniem podmiotu zajmującego się publikacją ogłoszeń o pracę jest tylko i wyłącznie udostępnienie narzędzi do ich publikacji, czy również przetwarzanie danych kandydatów, pracodawca powinien rozważyć, czy zawrzeć z takim podmiotem umowę powierzenia przetwarzania danych osobowych. Umowę powierzenia należy zawrzeć, jeżeli podmiot zajmujący się publikacją ogłoszeń o pracę będzie przetwarzał dane kandydatów wyłącznie w imieniu i na rzecz pracodawcy. Należy w niej określić m.in. charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób (w tym przypadku dane kandydatów do pracy), których dane dotyczą, a także obowiązki i prawa administratora. Przypomnieć należy, że pracodawca może korzystać wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi prawa i chroniło prawa osób, których dane dotyczą, czyli osób fizycznych (kandydatów do pracy). Przed powierzeniem danych pracodawca musi, więc ocenić czy poziom zabezpieczeń danych osobowych, stosowanych przez podmiot przetwarzający, jest odpowiedni.

2.5 Czy można poszukiwać pracowników w ramach tzw. rekrutacji „ślepych”, „ukrytych”?

Prowadzenie procesów rekrutacyjnych, w których pracodawca zlecający firmie rekrutacyjnej przeprowadzenie postępowania rekrutacyjnego, zastrzega sobie anonimowość, jest coraz powszechniejszym zjawiskiem na rynku pracy. Motywy pracodawców decydujących się na ich przeprowadzenie są różne – od chęci utajnienia rekrutacji przed pracownikiem, którego mają zamiar zwolnić (najczęściej, gdy zatrudniony jest na samodzielnym stanowisku, np. głównego księgowego), po chęć gromadzenia bazy kandydatów niejako „na zapas”. Do przeprowadzenia rekrutacji „ukrytej” wykorzystywane są zazwyczaj portale internetowe, które pośredniczą w rekrutacji udostępniając narzędzie wykorzystywane do publikowania ogłoszeń. Takiego typu rekrutacji, nie można uznać za zgodną z przepisami o ochronie danych osobowych, ponieważ kandydat do pracy nie posiada wiedzy, jaki podmiot zbiera jego dane osobowe i wobec jakiego podmiotu może realizować swoje prawa. O prawidłowym wykonaniu obowiązku informacyjnego, nie możemy mówić również w sytuacji, gdy klauzula informacyjna zostanie wysłana przez potencjalnego pracodawcę w odpowiedzi na otrzymaną aplikację, ponieważ obowiązek poinformowania m.in. o tożsamości pracodawcy powinien być realizowany przez niego na etapie zbierania danych osobowych, a nie na etapie ich utrwalania. Osoba przekazująca dane osobowe powinna posiadać wiedzę odnośnie tego, komu je udostępnia. Ma to szczególne znaczenie w związku z sytuacjami, w których ogłoszenia o prace są sposobem na wyłudzanie danych osobowych przez nieuczciwe podmioty do własnych celów niezwiązanych z zatrudnianiem pracowników.

2.6 Agencje zatrudnienia

Rozwiązaniem umożliwiającym pracodawcy utrzymanie anonimowości na wstępnym etapie rekrutacji może być zlecenie jej przeprowadzenia innym podmiotom, np. agencjom zatrudnienia, których działalność uregulowana jest prawnie i które zobowiązane są do przetwarzania posiadanych danych osobowych zgodnie z przepisami o ochronie danych osobowych.

Jaka będzie rola agencji zatrudnienia w procesie przetwarzania danych kandydatów do pracy? Jakie są obowiązki przyszłego pracodawcy, a jakie agencji?

Gdy pracodawca zleca rekrutację agencji zatrudnienia kandydaci mogą kierować swoje zgłoszenia do agencji, która w takiej sytuacji będzie pełniła rolę administratora ich danych. Będzie ona przetwarzać dane osobowe kandydatów na podstawie ich zgody wyrażonej w zgłoszeniu w celu przeprowadzenia pierwszego etapu rekrutacji – pozyskania CV oraz selekcji pracowników. W tej sytuacji obowiązek informacyjny podczas pozyskiwania danych powinna spełnić agencja. Obowiązek informacyjny po stronie pracodawcy, który wcześniej nie ujawnił swojej tożsamości powstaje w momencie, kiedy dane wybranych przez agencję kandydatów mają być mu przekazane. Wówczas wybrani kandydaci przed przekazaniem danych powinni zostać poinformowani przez agencję o danych potencjalnego pracodawcy oraz wyrazić zgodę na przekazanie ich kandydatur. Pracodawca otrzymuje dane osobowe tylko tych kandydatów, którzy wyrażą stosowną zgodę.

03

3. PROCES REKRUTACYJNY

W toku rekrutacji pracodawca zwykle może zechcieć spotkać się z kandydatem osobiście, aby sprawdzić jego doświadczenie i umiejętność oraz upewnić się czy jest właściwą osobą, na stanowisko, na które aplikuje (np. podczas rozmowy kwalifikacyjnej lub testu wiedzy i umiejętności). W trakcie tego procesu także dochodzi do gromadzenia danych osobowych.

3.1 Jakie dane kandydata pracodawca może gromadzić w trakcie rozmowy kwalifikacyjnej?

Podczas rozmowy kwalifikacyjnej pracodawca może zadawać szereg szczegółowych pytań odnoszących się do informacji, jakie kandydat na pracownika zawarł w swoim CV. Musi jednak pamiętać, że powinny się one odnosić wyłącznie do kwestii związanych ze stanowiskiem, na które on aplikuje. Należy unikać zadawania pytań, które kandydata na pracownika mogą zawstydzić, lub naruszyć jego prawo do prywatności bądź dobra osobiste (np. dotyczących wyznania, orientacji seksualnej, przekonań politycznych, życia prywatnego, rodzicielstwa czy planowanego potomstwa). W pewnych sytuacjach jednak, o ile wynika to bezpośrednio z przepisów prawa, pracodawca może być uprawniony do zadania pytań niedyskretnych (np. pytanie starającego się o posadę nauczyciela w szkole publicznej czy był karany za przestępstwo popełnione umyślnie).

„Dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („**osobie, której dane dotyczą**”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

3.2 Czy można skontaktować się z poprzednim pracodawcą kandydata w celu uzyskania informacji na jego temat?

Niedopuszczalne jest pozyskiwanie przez potencjalnego pracodawcę informacji o kandydacie na pracownika od jego poprzedniego pracodawcy, jeśli nie posiada on zgody kandydata na powyższe. Należy też pamiętać, że złożenie przez kandydata do pracy tzw. referencji nie uprawnia pracodawcy do kontaktu z podmiotem je wystawiającym w celu pozyskania dodatkowych informacji o kandydacie. Pamiętać należy, że udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Potencjalny pracodawca nie może tym samym zwrócić się do poprzedniego pracodawcy o informację, jakie zadania realizował kandydat u tego podmiotu oraz jaką ma opinię o kandydacie do pracy. Podczas procesu rekrutacyjnego źródłem informacji, które dotyczą przebiegu pracy zawodowej, powinien być sam kandydat.

3.3 Czy potencjalny pracodawca może zwrócić się do uczelni wyższej z prośbą o potwierdzenie, czy kandydat do pracy uzyskał w niej dyplom?

Nie. Potwierdzanie prawdziwości dyplomu ukończenia studiów wyższych, jak i innych danych zawartych w dokumentach przedkładanych przez kandydata w toku rekrutacji, poprzez kierowanie zapytań do podmiotów, które wydały te dokumenty jest niedopuszczalne. Polski prawodawca co zasady nie przewiduje w przepisach krajowych uprawnienia pracodawcy do występowania do innych podmiotów w celu potwierdzenia lub sprawdzenia prawdziwości dokumentów i danych w nich zawartych przedłożonych przez kandydatów w toku rekrutacji.

Takie działanie nie ma również oparcia w przesłance określonej w art. 6 ust. 1 lit. f RODO. Przypomnieć należy, że zgodnie z art. 22^{1} § 3 Kodeksu pracy udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą, zatem należy uznać, że praktyka polegająca na dodatkowej weryfikacji informacji uzyskanych od kandydata, naruszałaby prawa i wolności osoby. Polski ustawodawca zdecydował, w jakiej formie pracodawca powinien pozyskiwać informacje o kandydacie do pracy.

Wskazać należy, że praktyka polegająca na pozyskiwaniu zgód od kandydata na weryfikowanie prawdziwości złożonych oświadczeń i danych zawartych w dokumentach również nie znajduje oparcia w przepisach RODO. Podkreślenia wymaga, że jednym z warunków skuteczności zgody jest jej dobrowolność, co oznacza, że osoba, której dane dotyczą nie powinna ponosić żadnych negatywnych konsekwencji, jeżeli odmówi jej wyrażenia. Niewyrażenie zgody przez kandydata na kontakt z uczelnią przez pracodawcę (choćby z powodów subiektywnych np. konfliktu z uczelnią), może spowodować, że potencjalny pracodawca odrzuci jego kandydaturę.

Jeżeli pracodawca ma podejrzenia, że przedkładany dokument został sfałszowany powinien złożyć zawiadomienie o możliwości popełnienia przestępstwa określonego w art. 270 § 1 Kodeksu karnego.

3.4 Jak długo można przetwarzać dane kandydatów do pracy?

Okres przechowywania danych kandydata do pracy powinien być dostosowany do zasad przetwarzania danych i z góry określony przez administratora. Co do zasady pracodawca powinien trwale usunąć dane osobowe kandydata (np. poprzez zniszczenie bądź odesłanie), z którym nie zdecydował się zawrzeć umowy o pracę, niezwłocznie po zakończeniu procesu rekrutacji, tj. podpisaniu umowy o pracę z nowozatrudnionym pracownikiem, chyba że ziściły się inne przesłanki uprawniające administratora do ich przetwarzania. Konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. Wydłużenie okresu przechowywania danych zawartych w aplikacji, powinno być zatem wyjątkiem od reguły niezwłocznego ich usuwania oraz powinno być szczególnie uzasadnione.

3.5 Czy pracodawca może przetwarzać dane kandydatów do pracy po zakończeniu rekrutacji w celu zabezpieczenia się przed ich ewentualnymi roszczeniami?

Niedopuszczalne jest przetwarzanie danych tylko w celu zabezpieczenia się przed ewentualnym przyszłym i niepewnym roszczeniem osoby, której dotyczą. W przeciwnym razie może pojawić się wątpliwość jak długo należy przetwarzać dane osobowe, jeżeli ta osoba nie zdecyduje się na wytoczenia powództwa przeciwko pracodawcy. W toku rekrutacji nie powstaje żaden stosunek zobowiązaniowy pomiędzy kandydatem do pracy, a pracodawcą. Brak jest dokonania wzajemnych rozliczeń lub możliwości zarzucenia drugiej stronie niewykonania umowy lub nieprawidłowego jej wykonania. Nie ma więc podstaw do uznania, że pracodawca jest uprawniony do przetwarzania danych z uwagi na konieczność ustalenia bądź nie, istnienia roszczenia. Działanie pracodawcy stanowiłoby przetwarzanie danych kandydata „na wszelki wypadek".

3.6 Czy możliwość wystąpienia roszczeniem z tytułu dyskryminacji uzasadnia dłuższe przechowywanie danych?

W przypadku roszczeń wynikających z dyskryminacji kandydata do pracy, to na kandydacie spoczywa obowiązek przedstawienia faktów, z których wynika domniemanie nierównego traktowania, a następnie na pracodawcę zostaje przerzucony ciężar udowodnienia, że nie traktował kandydata gorzej od innych albo, że, traktując go odmiennie od innych, kierował się obiektywnymi i usprawiedliwionymi przyczynami. Pracodawca może np. wykazać przed sądem, z jakiego powodu zatrudnił inną osobę na stanowisko, na które aplikował kandydat. Pracodawca w procesie rekrutacji podejmuje czynności zmierzające do zatrudnienia pracownika.

Powszechną praktyką jest zapraszanie na rozmowę kwalifikacyjną kandydatów do pracy. To głównie w jej wyniku kandydat może odnieść wrażenie, że jest dyskryminowany.

Należy jednocześnie pamiętać, że osobiste przekonanie kandydata o tym, że jest dyskryminowany nie jest równoznaczne z uprawdopodobnieniem przez niego wystąpienia dyskryminacji.

Może zatem dojść do sytuacji, w której kandydat zgodnie z jego CV legitymuje się dużym doświadczeniem, w porównaniu do innych kandydatów ma wysokie kwalifikacje, jednak nie otrzymuje propozycji pracy, z uwagi na to, że rozmowa kwalifikacyjna nie poszła mu dobrze (np. był nieuprzejmy lub nie znał odpowiedzi na merytoryczne pytania, zadawane przez rekrutera), w efekcie czego pracodawca nie zatrudnia takiego kandydata. Kandydat natomiast uważa, że nie dostał pracy z uwagi na dyskryminację ze względu na płeć. Zarówno w tej, jak i w innych przypadkach przechowywanie danych osobowych takiego kandydata do pracy po zakończeniu rekrutacji nie można uznać za niezbędne dla pracodawcy.

Istotą roszczenia z tytułu dyskryminacji ze względu na jakąś cechę lub przekonania jest uprawdopodobnienie, że to właśnie z tej przyczyny kandydat został potraktowany w sposób gorszy niż reszta kandydatów, natomiast dopiero wtedy pracodawca musi wykazać, że ta cecha nie miała wpływu na dokonanie przez niego oceny negatywnej, do czego, nie jest konieczne przetwarzanie danych zawartych w życiorysie kandydata do pracy.

3.7 Jak powinien się zachować pracodawcą z sektora służby cywilnej, gdy wpływa do niego CV (lub inne dokumenty rekrutacyjne), choć nie jest przeprowadzany nabór?

Z art. 28 ust. 1 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2018 r. poz. 1559 tj.) wynika obowiązek dyrektora generalnego urzędu do upowszechniania informacji o wolnych stanowiskach pracy przez umieszczanie ogłoszeń o naborach w miejscu powszechnie dostępnym w siedzibie urzędu, w Biuletynie Informacji Publicznej urzędu, oraz w Biuletynie Informacji Publicznej Kancelarii Prezesa Rady Ministrów. W sytuacji, kiedy do urzędu wpłyną dokumenty potencjalnego kandydata do pracy, a nieprzeprowadzany jest nabór na wolne stanowisko pracy dyrektor generalny nie ma prawa zatrudnić takiej osoby. Zatem albo musi niezwłocznie usunąć dane dotyczące takiego kandydata ze swoich zasobów albo skontaktować się z kandydatem, aby otrzymać ewentualną zgodę kandydata na przetwarzanie jego danych osobowych zawartych w takiej dokumentacji dla celów przyszłych naborów na wolne stanowiska pracy w urzędzie.

3.8 Jakimi zasadami powinienem się kierować pracodawca z sektora służby cywilnej publikując informacje związane z prowadzonym naborem?

Istnieją przepisy prawa, które w sposób szczególny regulują kwestie dotyczące naboru pracowników, np. w służbie cywilnej. I tak, art. 31 ustawy o służbie cywilnej stanowi, że dyrektor generalny urzędu niezwłocznie

po przeprowadzonym naborze upowszechnia informację o wyniku naboru przez umieszczenie jej w miejscu powszechnie dostępnym w siedzibie urzędu, w Biuletynie urzędu oraz w Biuletynie Kancelarii.

Przepisy ustawy nie wskazują okresu, przez jaki taka informacja ma być dostępna publicznie. W takim przypadku administrator danych osobowych powinien kierować się zasadą ograniczenia przechowywania (retencji) danych osobowych określoną w art. 5 ust. 1 lit. e RODO. Zgodnie z tą zasadą dane osobowe muszą być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Celem publikacji danych wybranego kandydata jest realizacja zasady jawności, która umożliwia dokonanie społecznej kontroli prawidłowości przebiegu postępowania rekrutacyjnego. Zatem czas publikacji takich danych powinien być wystarczający do umożliwienia przeprowadzenia takiej kontroli w czasie niezbyt odległym od dokonanego wyboru, tzn. w czasie, kiedy kandydaci lub osoby trzecie mogą być zainteresowane danym naborem i będą chciały skorzystać z prawa do takiej informacji, jakie mają na podstawie art. 31 tej ustawy.

Wydaje się, że optymalnym okresem czasu, przez jaki takie informacje mogą być ujawniane na podstawie art. 31 ustawy jest okres trzech miesięcy liczony od dnia ich publikacji. Na taki okres czasu może wskazywać art. 33 ustawy stanowiący przepis dotyczący wyjątku od zasady obowiązku przeprowadzenia naboru[7]. Na Jednocześnie trzeba pamiętać, że przepis art. 29 ustawy o służbie cywilnej uznaje wyniki naboru za informację publiczną, a zatem każda osoba zainteresowana wynikiem naboru może złożyć wniosek o udostępnienie takich informacji w sytuacji, kiedy zostaną one usunięte z Biuletynu urzędu, Biuletynu Kancelarii czy przestaną być dostępne w siedzibie urzędu, do którego przeprowadzany był nabór.

3.9 Czy można tworzyć tzw. „czarne listy" osób ubiegających się o zatrudnienie?

Nie. Za niedopuszczalne należy uznać tworzenie tzw. „czarnych list" osób ubiegających się o zatrudnienie. Podstawy prawnej nie znajduje ponadto wymienianie się informacjami pomiędzy pracodawcami o kandydatach do pracy, których zatrudniać nie chcą. Ponadto należy pamiętać, że tworzenie zbiorów danych o charakterze negatywnym może prowadzić do dyskryminacji i podejmowania niekorzystnych dla danej osoby decyzji w oparciu o często nierzetelne, bezpodstawnie pozyskane informacje.

3.10 Wpływa do pracodawcy CV potencjalnego kandydata do pracy, jednak nie prowadzi on rekrutacji. Czy zachować przesłane dane w nim na potrzeby przyszłych rekrutacji?

[7] Jeżeli w ciągu 3 miesięcy od dnia nawiązania stosunku pracy z osobą wyłonioną w drodze naboru istnieje konieczność ponownego obsadzenia tego samego stanowiska pracy, dyrektor generalny urzędu może zatrudnić na tym samym stanowisku inną osobę spośród kandydatów, o których mowa w art. 29a ust. 1

Zdarzają się sytuacje, w których osoby poszukujące pracy z własnej inicjatywy, niezależnie od tego, czy potencjalny pracodawca prowadzi proces rekrutacji czy też nie, wysyłają do różnych podmiotów swoje aplikacje. Pracodawca po otrzymaniu takiej kandydatury powinien rozważyć, czy chce rozpocząć rekrutację, czy też nie jest zainteresowany zatrudnianiem nowych pracowników. W przypadku, gdy zdecyduje, że jest zainteresowany zatrudnieniem nowej osoby, powinien niezwłocznie wykonać w stosunku do niej obowiązek informacyjny oraz rozpocząć podejmowanie działań zmierzających do zawarcia umowy (np. przeprowadzenie rozmowy kwalifikacyjnej, gromadzenie koniecznej dokumentacji). Jeżeli jednak pracodawca stwierdzi, że nie jest zainteresowany poszerzeniem swojej kadry, powinien niezwłocznie usunąć dane dotyczące kandydata ze swoich zasobów.

3.11 Czy potencjalny pracodawca może pozyskiwać dane kandydata z portali społecznościowych?

Co do zasady niedopuszczalne jest gromadzenie przez pracodawców i agencje rekrutacyjne informacji zamieszczanych przez kandydatów do pracy na swój temat w mediach społecznościowych i innych ogólnodostępnych źródłach. Co prawda rozwój społeczeństwa informacyjnego pozwala na „budowanie" przez potencjalnych kandydatów do pracy swojego wizerunku w sieci, również w oczach przyszłego pracodawcy, poprzez zamieszczane w Internecie różnych informacji na swój temat, ale nie oznacza to, że informacje te mogą zostać wykorzystane w procesie rekrutacyjnym. Należy również pamiętać, że takie działanie potencjalnie może mieć negatywny wpływ na ocenę kandydata do pracy i prowadzić do profilowania go na podstawie dostępnych w Internecie danych.

3.12 Czy potencjalny pracodawca może zweryfikować kandydata lub komunikować się z nim za pośrednictwem branżowych portali społecznościowych np. LinkedIn?

Jako że żyjemy w dobie społeczeństwa informacyjnego, coraz częściej przyszli pracodawcy korzystają z możliwości weryfikacji kandydatów do pracy lub komunikacji z nimi, korzystając z portali internetowych dedykowanych takim celom. Portale takie, umożliwiając kandydatom do pracy, czy pracodawcom wzajemny kontakt, umożliwiają efektywne znalezienie pracy lub pracownika. Użytkownicy takich portali (poszukujący pracy) najczęściej zanim zaczną korzystać z usług oferowanych przez portale, muszą zapoznać się z regulaminami, politykami prywatności i je zaakceptować.

Jeżeli możliwość korzystania z takiego portalu będzie wiązała się z obowiązkiem podania danych, a może tak być, bo żeby założyć konto i aby dane z tego konta mogły być udostępniane potencjalnym pracodawcom,

to portal musi mieć do tego podstawy prawne. Przepisem umożliwiającym pozyskiwanie, gromadzenie, udostępnianie danych użytkowników (kandydatów) do pracy, będzie zgoda osoby, której dane dotyczą[8] czy też/lub potrzeba wykonania umowy (ewentualnie podjęcie działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy)[9]. Inną kwestią natomiast będzie możliwość kontaktowania się (przetwarzania danych w związku z tym) przez pracodawcę z kandydatem w innej formie np. mailowej (poza portalem, na którym doszło do kontaktu).

[8] art. 6 ust. 1 lit. a RODO

[9] art. 6 ust. 1 lit.b RODO

4. OKRES ZATRUDNIENIA

04

W ramach stosunku pracy istnieje nieustanna potrzeba wymiany informacji, w tym o pracowniku. Jej konieczność może wynikać z obowiązków pracodawcy wynikających z przepisów prawa, z charakteru wykonywanej przez pracownika pracy bądź też z uwagi na interes pracodawcy lub samego pracownika. Należy pamiętać, że ochrona danych osobowych pracownika nie jest absolutna i nie zawsze zależy od jego zgody. Jednocześnie fakt, czy to przetwarzanie jest zgodne z prawem, należy oceniać w każdym konkretnym przypadku.

4.1 Konkretne kwestie związane z przetwarzaniem danych w okresie zatrudnienia.

Wraz z powstaniem stosunku pracy powstają określone prawa i obowiązki pracodawcy i pracownika, których realizacja w sposób oczywisty wiąże się z koniecznością przetwarzania danych pracownika.

Zgodnie z art. 22^1 § 2 i 4 Kodeksu pracy pracodawca ma prawo żądać od pracownika, którego zdecydował się zatrudnić, podania, niezależnie od danych osobowych, które mógł od niego pozyskać w toku rekrutacji, także:

- innych jego danych osobowych, a także imion i nazwisk oraz dat urodzenia jego dzieci, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez niego ze szczególnych uprawnień przewidzianych w prawie pracy;
- jego numeru PESEL,
- innych danych osobowych niż pozyskane w procesie rekrutacji i wskazane wyżej, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

4.1.1 Zawarcie umowy o pracę i akta osobowe pracownika

Powstanie stosunku pracy generuje po stronie pracodawcy szereg obowiązków związanych z dokumentowaniem przebiegu pracy pracownika, w tym przede wszystkim prowadzenie akt osobowych[10].

Czy pracodawca może wykonać kserokopię dokumentu tożsamości pracownika, którego zatrudnia?

Zazwyczaj nie istnieje prawnie uzasadniona potrzeba wykonywania kopii tego typu dokumentu. Co więcej posiadanie jej będzie prowadziło do gromadzenia nadmiarowych danych niezwiązanych z wykonywaną przez pracownika pracą.

Czy pracodawca może przechowywać informacje związane z życiem osobistym pracowników w ich aktach osobowych?

Nie zawsze będzie tak, że w aktach osobowych pracownika znajdować się będą wyłącznie informacje związane z jego stosunkiem pracy. Zazwyczaj, aby pracownik mógł skorzystać z określonych uprawnień będzie musiał udostępnić pracodawcy informacje dotyczące jego życia osobistego. Przykładem może być urlop związany z realizacją jego zobowiązań cywilnych, publicznych itp. (zawarcie małżeństwa, śmierć krewnego, oddanie krwi, wezwanie do sądu itd.).

Czy w przypadku zatrudnienia pracownika pracodawca musi ponownie spełnić wobec niego obowiązek informacyjny?

Ponieważ dane pracownika już zatrudnionego pracodawca będzie przetwarzał w innym celu aniżeli kandydata oraz zmieni się krąg odbiorców tych danych, pracownik powinien pozyskać informacje w tym zakresie. Cel ten można osiągną umieszczając powyższe informacje w ramach klauzuli informacyjnej przekazywanej kandydatom w toku rekrutacji (poprzez uzupełnienie jej o informacje dotyczące celu przetwarzania danych i wskazanie odbiorców danych w razie zatrudnienia kandydata) lub też poprzez uzupełnienie tych informacji już po zatrudnieniu pracownika.

10 Zgodnie z art. 94 pkt 9a Kodeksu pracy pracodawca jest obowiązany prowadzić dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników, a zakres prowadzenia przez pracodawców tej dokumentacji oraz sposób prowadzenia akt osobowych regulują przepisy rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (t.j. Dz. U. z 2017 r., poz. 894).

4.1.2 Ujawnianie i dostęp do danych osobowych w kontekście zatrudnienia

Dane pracownika są poufne i nie mogą być ujawniane bez jego zgody bądź innej podstawy prawnej.

Jakie informacje o pracowniku można umieścić na liście obecności pracowników?

Przepisy prawa nie precyzują sposobu potwierdzania obecności pracownika w pracy. Często spotykanym sposobem jest złożenie podpisu na liście obecności. W wielu sytuacjach na owych listach, dostępnych dla wszystkich pracowników można było znaleźć informację o tym, że dany pracownik jest chory bądź korzysta z urlopu „na żądanie". Taka praktyka jest niewłaściwa, a informacje m.in. o zwolnieniach lekarskich czy urlopie „na żądanie", więc o szczególnych rodzajach nieobecności powinny znaleźć się w ewidencji czasu pracy, do którego dostęp oprócz samego pracownika, którego karta dotyczy mogą mieć jeszcze osoby odpowiedzialne za sprawy kadrowe i osoba reprezentująca pracodawcę (bezpośredni przełożony, osoby zarządzające zakładem pracy). Reasumując symbol absencji nie powinien być zamieszczony na liście obecności. Wystarczy wskazanie czy dany pracownik jest obecny czy też nie. W przeciwnym razie może to naruszać zasady minimalizacji oraz poufności danych osobowych. Czas pracy jest jednym z kluczowych elementów pracy zarówno dla pracownika jak i pracodawcy. To jak kwestia potwierdzania obecności w pracy przez pracownika będzie zorganizowana określać powinien regulamin lub inny wewnętrzny dokument, niezależnie czy będzie to lista obecności czy system kart zbliżeniowych - to już wewnętrzna sprawa samego pracodawcy - ważne jest by przy tych czynnościach nie naruszać praw i wolności swoich pracowników.

Czy pracodawca może umieścić zdjęcia pracowników na identyfikatorach?

Ze względu na to, że wizerunku pracownika nie ma wśród danych wskazanych w Kodeksie pracy, aby pracodawca mógł je pozyskać i umieścić np. na identyfikatorze musi legitymować się zgodą pracownika. Należy jednak zaznaczyć, że zgoda musi być udzielona dobrowolnie, a zatem pozyskiwanie przez pracodawcę zgody pracownika będzie możliwe, jeżeli pracownik będzie miał możliwość odmowy jej udzielenia i nie spotkają go z tego powodu żadne negatywne konsekwencje. Warto dodać, że zgoda może być odwołana w każdym czasie.

Istnieją jednak sytuacje wyjątkowe, gdy wizerunek pracownika jest ściśle związany z wykonywanym przez niego zawodem czy charakterem pracy i wskazywanie wizerunku pracownika przewidują wprost przepisy prawa. Jako przykład podać można choćby pracowników ochrony, co do których – ze względów bezpieczeństwa – powinna być możliwość ich identyfikacji. Wówczas pracodawca nie jest zobowiązany do pozyskiwania zgody w tym właśnie celu.

Przykład:

Art. 9 a ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (t.j. Dz. U. z 2017 r., poz. 2213) stanowi, iż legitymacja kwalifikowanego pracownika ochrony fizycznej lub kwalifikowanego pracownika zabezpieczenia technicznego zawiera m.in. jego aktualne zdjęcie.

Czy pracodawca może umieścić na swojej stronie internetowej takie dane osobowe pracowników, jak ich imiona i nazwiska, stanowiska, numery telefonów, czy adresy e-mail?

Informacje o pracowniku takie jak np. jego imię i nazwisko, czy właśnie służbowy adres e-mail są ściśle związane z życiem zawodowym pracownika i z wykonywaniem przez niego obowiązków służbowych. Dane te mogą być wykorzystywane (np. udostępniane) przez pracodawcę nawet bez zgody pracownika, którego one dotyczą. Pracodawca nie może być pozbawiony możliwości ujawniania nazwisk pracowników, zajmujących określone stanowiska w ramach instytucji i pozostających w kontakcie z podmiotami zewnętrznymi – kontrahentami, klientami. Przeciwne stanowisko prowadziłoby do sparaliżowania lub poważnego ograniczenia możliwości działania pracodawcy, bez żadnego rozsądnego uzasadnienia w ochronie interesów i praw pracownika. Z tego też względu za dopuszczalne uznać także należy umieszczanie imion i nazwisk pracowników na drzwiach w zakładach pracy, na pieczątkach imiennych, pismach sporządzanych w związku z pracą oraz prezentowanie w informatorach o instytucjach i przedsiębiorstwach. Kwestie tego typu uregulowane powinny zostać w regulaminach pracy, a pracownik powinien być świadomy tego przed nawiązaniem stosunku pracy.

Czy pracodawca może umieścić na swojej stronie internetowej wraz z danymi kontaktowymi wizerunek pracownika?

Nie. Publikacja wizerunku pracownika na stronie internetowej będzie wymagała uzyskania jego dobrowolnej zgody.

Czy pracodawca może umieszczać zdjęcia pracowników w Intranecie?

Sytuacja umieszczania zdjęć pracownika w Intranecie jest sytuacją szczególną, gdyż dostęp do tego wewnętrznego systemu ma ściśle określony krąg osób, tj. pracownicy, którzy znają się nawzajem, oraz z uwagi na cel, jaki przyświeca tego typu działaniom pracodawcy, jakim jest usprawnienie procesu zarządzania i wewnętrznej komunikacji w firmie. Jeśli pracodawca jest podmiotem z sektora prywatnego, można więc się zastanowić czy takie działanie nie będzie się mieściło w granicach jego usprawiedliwionego celu zgodnie z art. 6 ust. 1 lit. f RODO. Należy pamiętać, że w niektórych sytuacjach może wystąpić nawet konieczność umożliwienia wizualnej identyfikacji pracownika wynikająca np. z zakresu jego obowiązków, charakteru wykonywanej pracy czy potrzeb pracodawcy związanych z konkretnym stanowiskiem pracy. O ile więc umieszczenie zdjęć w Intranecie służy jedynie polepszeniu i usprawnieniu zarządzania firmą, a dostępu do nich nie mają osoby z zewnątrz, to można przyjąć to za dopuszczalne.

Gdyby jednak w ocenie pracownika wspomniana praktyka godziła w jego dobro, może on skorzystać z unormowań art. 21 ust. 1 RODO regulującego prawo do sprzeciwu z przyczyn związanych ze szczególną sytuacją takiej osoby.

Czy, a jeśli tak, to w jakim zakresie pracodawca może wykorzystać służbowy adresu e-mail po byłym pracowniku?

W związku z dynamicznym rozwojem nowych technologii, jednym z podstawowych sposobów komunikacji w relacjach pomiędzy firmami i instytucjami jest poczta elektroniczna. Powszechną praktyką jest nadawanie pracownikom adresów e-mailowych, składających się z imienia i nazwiska, pierwszej litery imienia i nazwiska lub w niektórych przypadkach z pseudonimu. Zarówno taki adres mailowy, jak też pozbawiony imienia i nazwiska, ale powiązany z konkretną osobą, uznawany jest za dane osobowe związane z zatrudnieniem. Problem pojawia się w sytuacji ustania stosunku pracy. Jeśli adres e-mail byłego pracownika stanowi dane osobowe, wówczas taki adres powinien zostać usunięty z chwilą zakończenia stosunku pracy, a przed usunięciem

konta wszystkie dane związane z wykonywaną pracą powinny zostać przekazane pracodawcy. Pracodawca może zobowiązać pracownika do skontaktowania się z osobami, z którymi pracownik pozostawał w służbowych relacjach, celem poinformowania ich o usunięciu adresu e-mail. Natomiast po zakończeniu współpracy pracodawca może tak skonfigurować serwer poczty, aby korespondencja była przekierowana na inny adres, a także żeby nadawca otrzymywał zwrotną wiadomość informującą, że nie ma takiego użytkownika.

4.1.3 Przetwarzanie danych na potrzeby przyznawania świadczeń z Zakładowego Funduszu Świadczeń Socjalnych (ZFŚS)

Pomimo tego, że funkcjonowanie Zakładowego Funduszu Świadczeń Socjalnych (ZFŚS) określają przepisy prawa[11], a zasady i warunki korzystania z usług i świadczeń z niego finansowanych oraz zasady przeznaczania środków ZFŚS określa pracodawca w regulaminie, to kwestią nieuregulowaną pozostaje kwestia gromadzenia danych, które mają świadczyć o sytuacji materialnej pracownika uprawniającej go do skorzystania z finansowanych z Funduszu świadczeń.

Czy i jakie dane pracownika można pozyskać, aby zweryfikować czy przysługuje mu prawo do pozyskania świadczenia z Funduszu?

Prawo uzależnia przyznawanie ulgowych usług i świadczeń oraz wysokość dopłat z Funduszu od określonych kryteriów, tj. sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej. Przyznanie świadczeń, a także ich wysokość, uzależniona jest od spełnienia przez osobę ubiegającą się o to świadczenie określonych kryteriów socjalnych. Kryterium dotyczące sytuacji rodzinnej i materialnej pracownika oznacza, że przy ustalaniu wysokości świadczenia znaczenie ma sytuacja życiowa i materialna wszystkich członków jego rodziny, z którymi prowadzi wspólne gospodarstwo domowe. Jeżeli zatem przyznawanie świadczeń jest uzależnione od kryterium socjalnego, to oznacza, że sytuacja pracownika lub innej osoby uprawnionej do korzystania z Funduszu wymaga każdorazowo jej określenia, czyli przetwarzania danych osobowych pracownika i członków jego rodziny. Przetwarzanie tych danych nie może jednak prowadzić do gromadzenia ich w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są pozyskiwane, bowiem adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana, jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych (pracodawcy).

Czy można żądać od pracownika przedłożenia rocznego zeznania podatkowego (PIT) w celu wykazania wysokości dochodu, na potrzeby Zakładowego Funduszu Świadczeń Socjalnych?

Uprawnienie pracodawcy do żądania podania stosownych informacji oraz przedłożenia odpowiednich dokumentów uzasadniających przyznanie świadczenia z Funduszu powinno zatem znajdować uzasadnienie w regulaminie, o którym mowa powyżej, który powinien precyzować zasady i warunki korzystania z usług i świadczeń finansowanych z Funduszu oraz tryb rozpatrywania wniosków o ich przyznanie. Należy jednak mieć na względzie, że zakazane jest zbieranie danych niemających znaczenia, jak i danych o większym, niż konieczny

11 Kwestie związane z funkcjonowaniem ZFŚS uregulowane zostały w ustawie z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (Dz. U. z 2017 r. poz. 2191 ze zm.).

stopniu szczegółowości, jak również danych zbieranych „na przyszłość". Zatem konieczność weryfikacji sytuacji materialnej osoby ubiegającej się o środki z Zakładowego Funduszu Świadczeń Socjalnych może być dokona w inny sposób, niż pozyskiwanie przez pracodawcę np. kopii zeznania podatkowego (PIT) osoby będącej członkiem rodziny pracownika. **Przedstawienie takiego dokumentu jedynie do wglądu pracodawcy będzie w celu dokonania takiej weryfikacji w pełni wystarczające. Warto również rozważyć przyjęcie rozwiązań polegających na respektowaniu oświadczeń o wysokości dochodu przypadającego na jednego członka rodziny ze wskazaniem ile osób i w jakim wieku składa się na rodzinę pracownika.** Należy również wskazać, że forma oświadczenia wskazuje na dobrowolność jego złożenia. Pracownik, który będzie chciał skorzystać z przysługującego mu uprawnienia, np. dofinansowania do wypoczynku, będzie obowiązany wypełnić oświadczenie. W sytuacji, kiedy nie będzie on chciał złożyć stosownego oświadczenia, pracodawca nie będzie zaś miał podstaw do wypłacenia danego świadczenia, ponieważ przyznawanie ulgowych usług i świadczeń oraz wysokość dopłat z Funduszu jest uzależniona od określonych w ustawie kryteriów.

Przez jaki czas można przetwarzać dane pracownika udostępnione na potrzeby rozpatrzenia jego wniosku przez ZFSŚ?

Dane osobowe powinny być przechowywane przez pracodawcę przez okres nie dłuższy niż jest to niezbędne do przyznania ulgowej usługi i świadczenia oraz dopłaty z Funduszu oraz ustalenia ich wysokości, a także przez okres dochodzenia do nich praw lub roszczeń. Pracodawca powinien także dokonywać systematycznego, np. raz w roku, przeglądu danych osobowych w celu ustalenia, które dane osobowe są niezbędne do ich dalszego przechowywania oraz usuwać te dane, których dalsze przechowywanie jest zbędne. Przykładowo, jeżeli pracodawca w ramach ZFŚS wspiera pracownika poprzez dofinansowanie wypoczynku, tzw. wczasy pod gruszą, powinien on usunąć dane z ubiegłych lat. Pracodawca nie ma podstaw do tego, aby zbierać dane osobowe „na przyszłość" oraz dane niepotrzebne do wypłacenia należnego świadczenia, mając na uwadze zasadę minimalizacji danych. W związku z tym oświadczenie pracownika o wysokości dochodu przypadającego na jednego członka rodziny ze wskazaniem ile osób i w jakim wieku składa się na rodzinę pracownika wydaje się być w pełni wystarczające i zgodne z zasadami celowości, minimalizacji danych, przejrzystości i rozliczalności. Dane te pracodawca może przetwarzać w zakresie niezbędnym do czasu wykonania koniecznych rozliczeń i sprawozdawczości (w przypadku np. jednostek publicznych).

4.2 Udostępnianie danych pracowników podmiotom zewnętrznym.

W czasie trwania stosunku pracy pracodawca niejednokrotnie zmuszony jest udostępnić dane pracowników innym podmiotom w celu realizacji przez nie ich uprawnień bądź w związku z oferowaniem przez nie na rzecz pracodawcy jak i jego pracowników pewnych usług. W każdej takiej sytuacji pracodawca musi mieć podstawę prawną zarówno do udostępnienia danych pracownika jak i żądania ich od innego podmiotu

4.2.1 Przetwarzanie danych osobowych pracowników w ramach relacji pracodawcy z organizacją związkową.

Kwestie dotyczące uprawnień związków zawodowych oraz wzajemnych relacji między nimi a pracodawcą, które w sposób oczywisty wiążą się z przetwarzaniem danych pracowników, określają przepisy prawa[12]. Wydaje się jednak, że nie regulują w sposób wyczerpujący sposobu udostępnienia i zakresu danych, które te podmioty mogą między sobą wymieniać.

Czy pracodawca ma prawo zażądać od organizacji związkowej przedstawienia pełnej listy osób pozostających pod jej ochroną, gdy nie ma zamiaru zwolnić ich z pracy?

Przepisy prawa pracy przewidują współdziałanie pracodawcy z zakładową organizacją związkową w indywidualnych sprawach ze stosunku pracy. Pracodawca ma obowiązek współdziałać w takich sprawach z zakładową organizacją związkową reprezentującą pracownika z tytułu jego członkostwa w związku zawodowym albo wyrażenia zgody na obronę praw pracownika niezrzeszonego w związku - zgodnie z ustawą o związkach zawodowych. Jednak przepisy te nie mogą stanowić podstawy do pozyskiwania przez pracodawcę od związku zawodowego, wszystkich danych osobowych pracowników korzystających z ochrony tego związku. Odnoszą się one bowiem do ochrony stosunku pracy indywidualnego pracownika, w stosunku, do którego pracodawca chce np. wypowiedzieć umowę o pracę. **Oznacza to, że pozyskiwanie informacji o przynależności związkowej pracownika w toku konsultacji ze związkami zawodowymi jest uzasadnione w razie zamiaru rozwiązania umowy o pracę z konkretnym pracownikiem. Jednak brak jest podstaw do pozyskiwania przez pracodawcę od związku zawodowego danych osobowych w odniesieniu do wszystkich pracowników korzystających z ochrony danego związku zawodowego, w sytuacji, gdy pracodawca nie ma zamiaru ich zwolnić z pracy.**

4.2.2 Przetwarzanie danych pracowników w ramach realizacji zadań z zakresu medycyny pracy

Kodeks pracy zobowiązuje pracodawcę do kierowania pracowników na wstępne, okresowe i kontrolne badania lekarskie (zwane łącznie badaniami profilaktycznymi) i przechowywania orzeczeń wydanych na ich podstawie. Z kolei kwestię sposobu kierowania pracownika na te badania regulują przepisy ustawy o służbie medycyny pracy[13], które stanowią, że badania wstępne, okresowe i kontrolne pracowników oraz inne świadczenia zdrowotne są wykonywane na podstawie pisemnej umowy zawartej przez podmiot obowiązany do ich

[12] Kwestie związane z funkcjonowaniem związków zawodowych uregulowane zostały w ustawie z dnia 23 maja 1991 r. o związkach zawodowych (t.tj. Dz. U. z 2015 r., poz. 1881).

[13] Ustawa z dnia 27 czerwca 1997 r. o służbie medycyny pracy (t.j. Dz.U .z 2018 r., poz. 1155).

zapewnienia (pracodawcę) z podstawową jednostką służby medycyny pracy (podmioty wykonujące działalność leczniczą w celu sprawowania profilaktycznej opieki zdrowotnej nad pracującymi).

Czy kierując pracowników na badania profilaktyczne pracodawca musi zawrzeć z jednostką służby medycyny pracy umowę powierzenia?

Nie. Pracodawca i podstawowa jednostka służby medycyny pracy zawierając umowę, o której mowa powyżej, działają niezależnie od siebie (każdy z nich samodzielnie ustala cele i środki przetwarzania danych osobowych). A zatem są jak oddzielnymi administratorami danych.

Czy, a jeśli tak, to w jakim zakresie pracodawca może przetwarzać dane pracowników związane z przeprowadzonymi wobec nich badaniami profilaktycznymi?

Po przeprowadzonym badaniu profilaktycznym lekarz przeprowadzający badanie profilaktyczne dokonuje w dokumentacji medycznej pracownika opisu badania oraz wpisu treści orzeczenia, a następnie wydaje orzeczenie lekarskie osobie badanej oraz pracodawcy. Do przechowywania dokumentacji badań profilaktycznych stosuje się odpowiednio ogólnie obowiązujące przepisy o dokumentacji medycznej. Należy pamiętać przy tym, że dane zawarte w dokumentacji medycznej oraz dane zawarte w dokumentacji (dokumentacji badań i orzeczeń psychologicznych), są objęte tajemnicą zawodową i służbową. Dane te mogą być udostępniane wyłącznie podmiotom określonym w odrębnych przepisach i na zasadach określonych w tych przepisach.

4.2.3 Przetwarzanie danych pracowników w ramach organizowanych przez pracodawców szkoleń

Każdy pracodawca dąży do podnoszenia kwalifikacji swoich pracowników poprzez kierowanie ich na różnego rodzaju szkolenia. Oprócz szkoleń, do których przeprowadzenia pracodawca zobowiązany jest na podstawie przepisów prawa, np. z zakresu bhp, pracodawcy mogą zaoferować pracownikom szkolenia podnoszące ich kwalifikacje zawodowe (np. regulowane postanowieniami układów zbiorowych pracy, porozumień zbiorowych, regulaminów pracy, statutów pracy, umów o pracę). Ze względu na podmiot, który szkolenie organizuje, wyróżnić możemy szkolenia wewnętrzne – organizowane u pracodawcy i przez pracodawcę przy pomocy własnych pracowników lub osób najętych (z zewnątrz) lub zewnętrzne - organizowane przez firmy szkoleniowe lub inne instytucje. Skierowanie pracownika na szkolenie wiąże się zaś w sposób oczywisty z przetwarzaniem jego danych.

Czy osoby szkolące z zakresu bhp mogą przetwarzać dane pracowników szkolonych?

Szkolenia z zakresu bhp mogą być przeprowadzone przez pracownika pracodawcy wyznaczonego np. ds. bhp lub podmiot zewnętrzny (osobę fizyczną lub firmę). Pracownik ds. bhp lub podmiot zewnętrzny będący osobą

fizyczną powinni posiadać upoważnienie do przetwarzania danych osób biorących udział w szkoleniu. Z kolei firma zewnętrzna będzie musiała zawrzeć z pracodawcą umowę powierzenia przetwarzania danych osobowych.

Pracodawca chce zaoferować pracownikom szkolenia podnoszące ich kwalifikacje zawodowe. Jak się to ma do przetwarzania ich danych osobowych przez podmioty szkolące?

Podobnie jak w przypadku szkoleń z zakresu bhp, jeśli szkolenie prowadzi pracownik pracodawcy wyznaczony do przeprowadzania takich szkoleń, może szkolić pracowników. Jeżeli zewnętrzna firma szkoleniowa prześle do pracodawcy ofertę szkoleń i pracownicy pracodawcy zdecydują się na skorzystanie z tych szkoleń i następnie firma ta przekaże za pośrednictwem pracodawcy formularze (zgłoszenia) do wypełnienia przez pracowników (poprzez wpisanie ich danych osobowych), wówczas firma taka będzie administratorem ich danych osobowych. W tym przypadku firma szkoleniowa może przetwarzać dane osobowe pracownika na podstawie jego zgody. Natomiast, jeżeli pracodawca zajmie się rozdysponowaniem ww. formularzy do pracowników i następnie uzupełnione formularze odbierze od nich (by je przekazać firmie szkoleniowej) wówczas firma szkoleniowa będzie musiała zawrzeć z tym pracodawcą umowę powierzenia przetwarzania danych osobowych pracowników.

Jakie obowiązki wobec pracowników będzie miał pracodawca w przypadku zlecenia ich przeszkolenia firmie zewnętrznej?

Jeżeli szkolenie odbywa się w taki sposób, że pracownik bierze udział w szkoleniu, na które sam się zapisał w firmie zewnętrznej, natomiast pracodawca jedynie finansuje udział tego pracownika w szkoleniu, to firma zewnętrzna, jako odrębny administrator, przetwarza dane osobowe pracownika i będzie musiała wykonywać w stosunku do niego obowiązki informacyjne oraz pozostałe zadania określone w RODO.

Jeżeli firma szkoleniowa zewnętrzna będzie podmiotem, któremu pracodawca powierzy przetwarzanie danych osobowych, wówczas będzie musiała spełnić obowiązki spoczywające na takim podmiocie oraz zawarte w umowie powierzenia.

Jakie dane pracowników może przetwarzać podmiot zewnętrzny prowadzący szkolenie?

Adekwatne do celu pozyskania, czyli np.: imię, nazwisko, stanowisko służbowe, miejsce pracy. Dane takie mogą być niezbędne np. do sporządzenia listy obecności, jej sprawdzenia lub wydania zaświadczenia ze szkolenia. Należy pamiętać, że tzw. dane służbowe pracownika to też dane osobowe.

Ważne!

Zlecenie przeszkolenia pracowników nie zawsze będzie wiązało się z koniecznością przetwarzania ich danych. Jeśli to niego nie dojdzie, np. firma zewnętrzna jedynie przeszkoli pracowników bez uzyskiwania jakichkolwiek informacji o nich (np. w postaci list obecności, innych dokumentów), pracodawca nie musi zawierać z nią umowy powierzenia ani w inny sposób regulować kwestii przetwarzania danych.

W jaki sposób można przekazać dane pracowników zewnętrznemu podmiotowi w celu ich przeszkolenia?

Dane pracowników mogą być przekazane w formie listy pracowników. Przekazanie może nastąpić również w formularzach firmy zewnętrznej, wypełnionych przez pracowników.

Czy pracodawca może zgłosić pracownika na szkolenie bez jego zgody i w związku z tym również bez jego zgody przekazać jego dane osobowe?

Tak, ale pod pewnymi warunkami. Jeżeli pracodawca prowadzi szkolenie wewnętrzne lub zawiera umowę powierzenia przetwarzania danych z firmą zewnętrzną, to jest on uprawniony do udostępnienia danych osobowych pracownika w tym celu, również do firmy zewnętrznej. Powierzenie przetwarzania danych osobowych nie zmienia podstawy przetwarzania danych osobowych, skutkując jedynie tym, że przetwarza je podmiot trzeci na polecenie pracodawcy.

4.2.4 Przekazywanie danych w związku z oferowanymi przez pracodawcę dodatkowymi świadczeniami pracowniczymi

Coraz częściej pracodawcy, aby zachęcić pracowników do podjęcia pracy w ich firmach oferują różnego rodzaju udogodnienia np. karnety na siłownię, prywatną opiekę zdrowotną czy też dodatkowe ubezpieczenia pracownicze. W związku z faktem, iż korzystanie z tych udogodnień jest w pełni dobrowolne, pracodawca nie może udostępnić danych osobowych pracowników bez ich wiedzy i zgody na rzecz podmiotów świadczących te usługi. Udostępnienie danych osobowych przez pracodawcę odbywa się na podstawie zgody wyrażonej przez pracownika. Przetwarzanie przez podmioty świadczące tego typu usługi danych osobowych pracowników lub innych osób zgłoszonych do programu odbywa się zatem na podstawie uprzednio wyrażonej przez nich zgody, tj. na podstawie art. 6 ust. 1 lit. a RODO. Podmioty te stają się administratorami danych osobowych osób korzystających z ich usług, niemniej jednak wszelkie roszczenia z tytułu zawartych umów przysługują im względem pracodawców, a nie pracowników będących beneficjentami usług. Konsekwencją uznania takiego podmiotu za administratora danych osobowych jest konieczność stwierdzenia, że takie podmioty są

zobowiązane do informowania osób, których dane dotyczą o okolicznościach wskazanych w art. 13 RODO np. w deklaracji przystąpienia. Jednocześnie nie ma tu zastosowania instytucja powierzenia przetwarzania danych osobowych. Podkreślić należy, że istota powierzenia przetwarzania danych osobowych polega m.in. na tym, że nie jest wymagane uzyskanie zgody osoby, której dane dotyczą, na powierzenie jej danych.

Czy należy zawrzeć umowę powierzenia z podmiotem oferującym benefity?

Zasadniczą kwestią decydującą o uznaniu, czy podmiot przetwarzający dane osobowe jest ich administratorem jest stwierdzenie czy decyduje on o celach i środkach przetwarzania. Zaznaczyć należy, że pracodawca przetwarza dane osobowe pracowników w zakresie i celu niezbędnym dla wykonania ciążących na nim obowiązków wynikających ze stosunku pracy. Natomiast usługodawcy przetwarzają dane osobowe pracowników w celu i zakresie świadczonych przez nich usług. Mamy więc tutaj do czynienia z dwoma odrębnymi zbiorami danych osobowych prowadzonymi przez odrębnych administratorów danych. Pracodawca nie może więc zażądać od podmiotów medycznych czy ubezpieczycieli, z którymi ma podpisaną umowę na świadczenie usług wobec swoich pracowników, przekazania danych osobowych np. na temat ich zdrowia.

Jakie dane pracowników pracodawca może udostępnić?

Zakres danych osobowych udostępnianych przez pracodawcę jest ograniczony i ściśle związany z przedmiotem działalności podmiotu świadczącego usługę. Musi on być zatem niezbędny do realizacji danej usługi. Podkreślić należy, że jeśli przekazane dane obejmują szczególne kategorie danych, o których mowa w art. 9 ust. 1 RODO niezbędne jest uzyskanie odrębnej zgody pracownika (art. 9 ust. 2 pkt a RODO).

4.2.5 Przekazywanie informacji o pracownikach pomiędzy spółkami grupy przedsiębiorstw (np. do jakiegoś projektu, zadań albo pracy).

Zgodnie z **art. 4 pkt 19 RODO**, grupę przedsiębiorstw tworzą przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez niekontrolowane. Zgodnie natomiast z **motywem 37 RODO,** przedsiębiorstwo sprawujące kontrolę to przedsiębiorstwo, które może wywierać dominujący wpływ na pozostałe przedsiębiorstwa ze względu na przykład na strukturę właścicielską, udział finansowy lub przepisy regulujące jego działalność, lub też uprawnienia do nakazywania wdrożenia przepisów o ochronie danych osobowych. Za grupę przedsiębiorstw należy uznać przedsiębiorstwo kontrolujące przetwarzanie danych osobowych w przedsiębiorstwach powiązanych z nim, wraz z tymi przedsiębiorstwami.

Pojęcie kontroli zawarte w przepisach RODO nie jest tym samym, co kontrola właścicielska, lecz należy ją rozumieć, jako kontrolę definiowaną przez przetwarzanie danych osobowych. Warto zauważyć, że nie tylko spółka dominująca (w rozumieniu przepisów Kodeksu spółek handlowych) może sprawować kontrolę, ale także odpowiadać za to może inna dowolna spółka należąca do grupy przedsiębiorstw.

Czy można przekazywać dane pracowników w ramach grupy przedsiębiorstw, do której należy pracodawca?

Administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji powiązanych z podmiotem centralnym, mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników[14]. Oznacza to, że przekazywanie w ramach grupy przedsiębiorstw danych osobowych pracowników poszczególnych podmiotów z grupy (np. w związku z centralizacją określonych procesów w zakresie kadr i płac) może znajdować oparcie w prawnie uzasadnionym interesie pracodawcy[15].

Na czym polegają cele administracyjne, w których można przetwarzać dane pracowników w ramach grupy przedsiębiorstw?

Poprzez cele administracyjne należy rozumieć wszelkie czynności bezpośrednio związane ze stosunkiem pracy, np. przekazanie pracownika do innego miejsca, w tym delegowanie go na jakiś czas do pracy w innej spółce w ramach grupy, działania związane z rozwojem pracownika - organizacja szkoleń, zatwierdzania wysokości wynagrodzenia, czy też prowadzenia statystyk dotyczących zatrudnienia w grupie, jak również rekrutację pracowników (spółka córka utworzona na potrzeby rekrutacji). Jedynym ograniczeniem są sytuacje, w których nadrzędny charakter wobec prawnie uzasadnionego interesu pracodawcy mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych.

Jakie będą obowiązki administratora danych pracowników przetwarzanych w ramach grupy przedsiębiorstw?

Administratorzy będący częścią grupy przedsiębiorstw powinni rozważyć współpracę w zakresie administrowania danymi osobowymi. Specyfika relacji współadministrowania polega przede wszystkim na tym, że administratorzy wspólnie ustalają cele i sposoby przetwarzania, a także wspólnie realizują obowiązki wynikające z przepisów i podejmują procesy przetwarzania. Tym samym nie dochodzi między tymi podmiotami do powierzenia ani udostępnienia danych, ponieważ przetwarzają dane wspólnie, w ramach ustalonych celów. Należy przy tym pamiętać, że:

- Współadministratorzy w drodze wspólnych uzgodnień w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków informacyjnych, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają.
- Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą – wymóg transparentnego i przejrzystego komunikowania osobie, której dane dotyczą, kluczowych informacji dotyczących przetwarzania jej danych.
- W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. Może to odbywać się poprzez powierzenie tej funkcji inspektorowi ochrony danych. Osoby te mogą kontaktować

14 Motyw 48 RODO.

15 Art. 6 ust. 1 lit. f RODO

się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem ich praw. Tym samym nie ma przeszkód, by inspektor udzielał także informacji w zakresie uzgodnień między współadministratorami.

- Osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego z administratorów, niezależnie od uzgodnień pomiędzy współadministratorami.

4.3 Wykorzystanie wewnętrznych zasobów telekomunikacyjnych

W ciągu ostatnich lat postęp techniki sprawił, że zamieniliśmy maszyny do pisania na klawiatury komputerów, a druczki papierowe coraz częściej zastępujemy dokumentami elektronicznymi. Świat w zakresie nowych technologii nie biegnie tylko pędzi, a my musimy temu wyzwaniu sprostać czy tego chcemy czy nie. Nowe technologie pozwalają również pracodawcy na wykorzystywanie wewnętrznych zasobów telekomunikacyjnych do monitorowania pracowników. Mimo to, musi on pamiętać, że nie ma prawa do naruszania prywatności pracownika w miejscu pracy (na przykład poprzez monitorowanie rozmów telefonicznych, śledzenie korespondencji e-mail czy sprawdzanie przesyłek adresowanych do pracownika) bez poważnego powodu związanego z charakterem jego pracy[16].

4.3.1 Monitoring poczty elektronicznej pracownika

Na jakiej podstawie pracodawca może prowadzić monitoring poczty elektronicznej pracownika?

Pracodawca może monitorować pocztę elektroniczną swoich pracowników, ale musi pamiętać, że uprawnienie to dotyczy tylko służbowej poczty elektronicznej. Ma takie prawo, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Takie uprawnienie pracodawcy zostało przewidziane w art. 22^3 Kodeksu pracy.

Czy pracodawca może kontrolować służbową pocztę elektroniczną pracownika?

Tak. Pracodawca może kontrolować aktywność swoich pracowników w trakcie pozostawania ich do jego dyspozycji w miejscu pracy, tzn. może sprawdzać czy pracownicy nie korzystają ze stron zabronionych czy też z innych witryn, które nie służą wykonywaniu przez nich obowiązków służbowych. Pracodawcy zależy przecież na tym, aby pracownicy jak najpełniej wykorzystali czas pracy na wykonywanie swoich obowiązków, a także, aby prawidłowo korzystali z udostępnionych im w tym celu narzędzi. Co istotne, kontrola nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Kontrola taka ma służyć zapewnieniu, by pracownik nie był zbytnio obciążony pracą oraz wykorzystywał powierzone mu narzędzia do celów zawodowych.

16 O prowadzeniu monitoringu wizyjnego w miejscu pracy szerzej we Wskazówkach Prezesa UODO dotyczących wykorzystywania monitoringu wizyjnego, które są dostępne na: https://uodo.gov.pl

Czy pracodawca może kontrolować prywatną skrzynkę pocztową swojego pracownika?

Pracodawca nie może kontrolować prywatnej korespondencji swoich pracowników, jest to wręcz zabronione. Takie zachowanie naruszałoby konstytucyjne prawo do prywatności. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

Jakie obowiązki spoczywają na pracodawcy względem pracowników w zakresie monitoringu ich poczty elektronicznej?

- Przede wszystkim pracodawca musi ustalić cel, zakres oraz sposób zastosowania monitoringu poczty elektronicznej w układzie zbiorowym pracy lub regulaminie pracy, bądź w obwieszczeniu - jeżeli nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy. O celu, zakresie oraz sposobie zastosowania monitoringu musi powiadomić pracowników.
- Pracodawca musi poinformować pracowników o planowanym uruchomieniu monitoringu, najpóźniej na 2 tygodnie przed jego uruchomieniem (poza sytuacjami, kiedy monitoring taki jest już stosowany). W przypadku nowych pracowników realizacja tego obowiązku powinna nastąpić przed dopuszczeniem ich do pracy[17]. Ponadto w przypadku pracowników, który zostali już dopuszczeni do pracy, pracodawca powinien poinformować ich o zamiarze prowadzenia monitoringu. Nieprawidłowym jest jednocześnie prowadzenie monitoringu aktywności obejmującej okres sprzed poinformowania pracownika zamiarze jego prowadzenia. Dla celów dowodowych dobrze będzie udokumentować taką czynność na piśmie.
- Dodatkowo pracodawca musi pamiętać o wykonywaniu w stosunku do monitorowanych pracowników obowiązków informacyjnych określonych w RODO[18].

4.3.2 Ewidencjonowanie czasu pracy przy użyciu nowoczesnych technologii

Ewidencjonując czas pracy pracodawca może sprawdzać, czy pracownicy jego firmy pozostają do jego dyspozycji tak długo jak wynika to z przepisów prawa czy z umowy, jaką ukształtował relacje z pracownikiem. Właściwe ewidencjonowanie czasu pracy pracowników jest także obowiązkiem pracodawcy. Trzeba jednak pamiętać, że Kodeks pracy nie narzuca sposobu potwierdzania obecności w pracy przez pracodawcę. Pracodawca ma zatem dużą swobodę w zakresie potwierdzania obecności pracownika w pracy. Musi jednak pamiętać, że o ile ewidencjonowanie czasu pracy jest wymogiem prawa, o tyle czynności odnotowywania obecności pracowników czy to w postaci listy obecności, czy przy użyciu innych urządzeń kontrolujących proces pracy nie stanowią ewidencji czasu pracy. Czynności te są jedynie elementem pomocniczo-technicznym, za

[17] Art. 22^2 §6 Kodeksu pracy

[18] Art. 13, art. 15 RODO

pomocą, których pracodawca może w drodze regulaminu pracy czy też w drodze informacji o warunkach zatrudnienia ukształtować proces odnotowywania obecności swoich pracowników w pracy.

Czy pracodawca może wybrać każdy rodzaj odnotowywania obecności swoich pracowników?

Niezupełnie. Wspomniano powyżej, że odnotowywanie obecności pracowników to tylko element wewnętrznej organizacji, wewnętrznego postępowania dotyczącego obecności w pracy, procedury wejść i wyjść i tym podobnych operacji. Prawo w tym elemencie daje dużą swobodę, ale wprowadza też wymogi. Jednym z nich jest kategoryczny zakaz wykorzystywania danych biometrycznych dla celów ewidencji czasu pracy. Postęp technologiczny sprawia, że coraz większą popularność zyskują metody oparte na wykorzystywaniu danych biometrycznych pracowników jak odcisk palca, zdjęcie tęczówki, siatkówki oka, układu żył na ręce czy też biometria kształtu ucha. Elementy te są charakterystyczne dla każdej osoby i umożliwiają ich identyfikację.

Czy pracodawca może skanować indywidualne cechy ludzkiego organizmu (np. linie papilarne) należące do swoich pracowników w ramach sprawdzenia obecności?

Nie. Pracodawca nie może skanować czy pobierać danych biometrycznych pracowników w celu rejestracji godzin przyjścia i wyjścia z zakładu, nawet za zgodą takiego pracownika. Pobieranie danych biometrycznych od pracowników nie służy celowi, jakim jest ewidencja czasu pracy, a jedynie ograniczeniu dostępu do miejsc, w stosunku, do których pracodawca może wymagać specjalnych uprawnień ze względu na tajemnice przedsiębiorstwa bądź ograniczony zakres osób o fachowych umiejętnościach mogących dostać się na pewien chroniony obszar. Pracodawca zgodnie z zasadą rozliczalności nie byłby w stanie wykazać, dlaczego stosuje monitoring danych biometrycznych dla celów związanych z obecnością w pracy. Trzeba także pamiętać, że dane biometryczne to dane szczególnej kategorii i mogą być przetwarzane tylko w enumeratywnie wymienionych sytuacjach, wśród których nie ma kwestii odnotowywania obecności pracownika w pracy.

Ważne!

Jak stwierdził Naczelny Sąd Administracyjny w wyroku z dnia 1 grudnia 2009 r. (sygn. I OSK 249/09):

- Brak równowagi w relacji pracodawca pracownik stawia pod znakiem zapytania dobrowolność wyrażeniu zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 22 Kodeksu Pracy katalog danych, których pracodawca może żądać od pracownika. Uznanie faktu wyrażenia zgody, jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 22 Kodeksu pracy, stanowiłoby obejście tego przepisu.

- Ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności, jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych , to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania. Pracodawca może monitorować pocztę elektroniczną swoich pracowników, ale musi pamiętać, że uprawnienie to dotyczy tylko służbowej poczty elektronicznej. Ma takie prawo jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie

4.3.3 Monitorowanie przy użyciu urządzeń lokalizujących GPS

Obok monitorowania poczty elektronicznej pracownika, pracodawcy często monitorują działalność swoich pracowników przy użyciu urządzeń lokalizujących GPS. Firmy realizujące czynności handlowe, firmy transportu publicznego oraz przede wszystkim firmy transportu drogowego celem jak najbardziej efektywnego wykorzystania środków i optymalizacji kosztów korzystają z pomocy nowych technologii, dzięki którym mogą uzyskać przewagę konkurencyjną jednocześnie rozwijając swoją pozycję rynkową. Czasem monitorowanie lokalizacji pojazdów jest obowiązkiem prawnym pracodawcy, czego przykładem są przepisów ustawy o monitorowaniu przewozu drogowego towarów.

Czy przedsiębiorca może monitorować swoich pracowników za pomocą urządzeń lokalizujących (np. GPS)?

Kodeks pracy wprowadza możliwość stosowania innych form monitoringu aniżeli monitoring wizyjny czy monitoring poczty elektronicznej, jeżeli zastosowanie takiego monitoringu służy celowi, w zakresie zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Analogicznie jak w przypadku monitoringu poczty elektronicznej pracodawca obowiązany jest uprzedzić pracownika o stosowaniu urządzeń monitorujących samochód (GPS) przed przystąpieniem pracownika do pracy bądź na dwa tygodnie przed uruchomieniem monitoringu. Pracodawca ma obowiązek poinformowania pracownika na piśmie o celach, zakresie i sposobie monitorowania urządzenia, także umieszczenia w widocznym miejscu w samochodzie symbolu obrazkowego informującego o tym, iż trasa pojazdu i jego wykorzystanie będzie monitorowane za pomocą urządzenia lokalizującego oraz jakie dane będą przy pomocy takiego urządzenia zbierane, gdzie rejestrowane, jak długo przechowywane i kto będzie miał do nich dostęp. Pracodawca musi pamiętać, że nowe regulacje prawa w zakresie monitorowania są dla niego pomocą, ale i obowiązkiem. Dane, które będzie rejestrował muszą mieścić się w celu, jakim jest to niezbędne dla zapewnienia sprawnej organizacji pracy, a zasady zbierania i wykorzystywania danych muszą być rzetelne i przejrzyste, jasno określone oraz dostępne dla pracownika.

Jakie dane pracownika można pozyskiwać za pomocą urządzeń GPS?

Niejednokrotnie w trakcie monitorowania przy pomocy urządzeń lokalizujących pojazd pracodawca może uzyskać także dane o tym, jakim stylem jazdy porusza się dany kierowca, gdzie się zatrzymuje, gdzie tankuje, gdzie je. Istnieje zatem ryzyko, że za pomocą monitorowania lokalizującego pracodawca może uzyskać więcej informacji niż tego potrzebuje. Dodatkowy problem pojawia się w sytuacji, gdy pojazd służbowy wykorzystywany jest także w celach prywatnych. W takiej sytuacji zbierając dane o pojeździe jednocześnie pracodawca pozyskuje informacje o pracowniku np. gdzie obecnie przebywa. Pracodawca nie jest uprawniony do pozyskiwania takich danych chyba, że mamy do czynienia z sytuacją wyjątkową np. z kradzieżą samochodu lub koniecznością ustalenia odpowiedzialności pracownika za uszkodzenie pojazdu.

Czy można przetwarzać dane pracownika pozyskane za pomocą GPS, a dotyczące jego aktywności w czasie wolnym?

Rozwiązaniem jest precyzyjne określenie, że samochód służbowy używany jest tylko do celów służbowych. W innym wypadku należy dostosować lub zmienić regulamin wykorzystywania samochodu służbowego do celów prywatnych. W takiej sytuacji należy uzyskać zgodę pracownika na przetwarzanie tych danych oraz wypełnić wobec niego obowiązek informacyjny.

Czy umieszczenie w układzie zbiorowym pracy, regulaminie pracy czy obwieszczeniu informacji o celach, zakresie oraz sposobie zastosowaniu monitoringu jest wystarczające?

Niezupełnie, ważne, aby cel przetwarzania był rzeczywiście zgodny z danymi, które przetwarzamy i wykorzystujemy. Nie możemy bowiem wykorzystywać danych przy użyciu systemu GPS zamontowanego w użytkowanej przez nas flocie pojazdów w celu ochrony mienia, gdy tymczasem w regulaminie pracy pracodawca określił cel inny np. organizacja czasu pracy poprzez wytyczanie jak najkrótszych i najszybszych tras potrzebnych do zrealizowania transportu. Pracodawca musi pamiętać o tym, że cel wpisany w dokumentacji musi być tożsamy z celem wykorzystywania urządzenia i danych w ten sposób otrzymywanych. Nie zmienia to faktu, że cele, zakres oraz sposób zastosowania również takiej formy monitoringu muszą być ustalone w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.

05

5. INNE NIŻ OKREŚLONE W KODEKSIE PRACY FORMY ZATRUDNIENIA ORAZ PRACA TYMCZASOWA

Jako niepracownicze formy zatrudnienia wyróżniamy m.in:

- *umowę o dzieło (art. 627 Kodeksu cywilnego);*
- *umowę zlecenia (art. 734 Kodeksu cywilnego);*
- *umowę o świadczenie usług (art. 750 Kodeksu cywilnego);*
- *samozatrudnienie.*

Jednocześnie w rozdziale omówiono wybrane zagadnienia związane ze świadczeniem pracy tymczasowej.

5.1 Przetwarzanie danych osobowych w związku z wykonywaniem zadań na podstawie umów cywilnoprawnych

Jakie dane o osobie, która wykonuje zadania na podstawie umowy cywilnoprawnej, można zbierać?

Ze względu na mnogość możliwych form prawnych i charakteru współpracy między stronami, różny będzie zestaw danych osobowych, który jest niezbędny do zawarcia i realizacji takich umów. W odróżnieniu od pracowniczych form zatrudnienia, przepisy prawa cywilnego nie określają wprost zakresu danych, które mogą być pozyskiwane przez podmiot zatrudniający w ramach niepracowniczych form zatrudnienia. Prawo cywilne statuuje zasadę swobody umów, która umożliwia dowolne kształtowanie treści umów o ile nie sprzeciwia się to charakterowi i naturze stosunku zobowiązaniowego. W takiej sytuacji podmiot zatrudniający powinien dokonać analizy zakresu danych, których zebranie jest konieczne w związku z realizacją umowy i ciążącymi na nim obowiązkami wynikającymi z umowy (np. wypłata wynagrodzenia) lub z przepisów prawa (np. płatność składek na ubezpieczenie społeczne). Nie ma on tutaj pełnej swobody, gdyż jest on związany wymogami określonymi przez postanowienia RODO, a w szczególności musi zapewnić zgodność z zasadami ograniczenia celu oraz minimalizacji danych.

Jakie dane o przedsiębiorcy można zbierać, gdy zamierza się z nim współpracować?

Jeżeli osoba fizyczna prowadząca działalność gospodarczą zawiera umowę z inną osobą prowadzącą działalność gospodarczą z prawnego punktu widzenia należy uznać, że brak jest „silniejszej" strony stosunku zobowiązaniowego. Działalność gospodarcza jest prowadzona w celu zarobkowym, ma charakter zorganizowany i jest wykonywana w imieniu własnym, na własny rachunek, zatem po jednej, jak i po drugiej stronie umowy mamy do czynienia z podmiotami profesjonalnymi. Zgodnie zatem z zasadą swobody umów, obie strony umowy są równe i wspólnie powinny określić zakres potrzebnych im danych. Nie oznacza to jednak możliwości zupełnie dowolnego określania zakresu danych, gdyż zakres ten musi być zgodny z zasadą celowości oraz zasadą minimalizacji danych.

Jak długo można przetwarzać dane o współpracownikach wykonujących swoje zadania na podstawie umów cywilnoprawnych?

Zgodnie z zasadą ograniczenia przechowywania, dane osobowe mogą być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane są przetwarzane.

Przy określeniu czasu przechowywania podmiot zatrudniający takich współpracowników powinien wziąć pod uwagę:

- okres trwania umowy,
- okres ewentualnego dochodzenia roszczeń związanych z umową (okres przedawnienia roszczeń),
- obowiązki wynikające z przepisów prawa.

Podstawą przetwarzania danych osobowych w związku z wykonywaniem usługi na podstawie umowy cywilnoprawnej jest niezbędność do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub niezbędność do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy. Część danych może być natomiast zbierana ze względu na ciążące obowiązki prawne (np. w związku ze zgłoszeniem do ubezpieczenia zdrowotnego[19]).

Czy należy poinformować osobę, z którą zamierza się nawiązać współpracę o okolicznościach związanych z przetwarzaniem jej danych?

Tak. Podmiot zatrudniający musi spełnić obowiązek informacyjny wobec takiej osoby zgodnie z RODO. W szczególności powinien on poinformować osobę, od której bezpośrednio zbiera dane (również wtedy, gdy to ta osoba jest inicjatorem składającym ofertę) o istotnych kwestiach dotyczących tego przetwarzania (danych administratora, celu przetwarzania, okresie przechowywania itd.). Obowiązek informacyjny może być spełniony w postaci pisemnej lub elektronicznej (np. w treści umowy, w ogłoszeniu), jak również okoliczności mogą przemawiać za ustnym poinformowaniem lub wywieszeniem tych informacji w miejscu, gdzie bezpośrednio zbiera się dane od takich osób. Administrator danych powinien być wstanie wykazać spełnienie tego

[19] Obwieszczenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 29 marca 2018 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Pracy i Polityki Społecznej w sprawie określenia wzorów zgłoszeń do ubezpieczeń społecznych i ubezpieczenia zdrowotnego, imiennych raportów miesięcznych i imiennych raportów miesięcznych korygujących, zgłoszeń płatnika, deklaracji rozliczeniowych i deklaracji rozliczeniowych korygujących, zgłoszeń danych o pracy w szczególnych warunkach lub o szczególnym charakterze oraz innych dokumentów, t.j. Dz. U. z 2018 r. poz. 804 (http://dziennikustaw.gov.pl/DU/2018/804/1)

obowiązku. Należy podkreślić, że w razie zbierania danych bezpośrednio od osoby, której dane dotyczą, informacje powinny być przekazane najpóźniej w momencie zbierania danych. W praktyce należy też bardzo ostrożnie podchodzić do wyłączenia konieczności spełnienia tego obowiązku, gdy osoba, której dane dotyczą, posiada już informacje o przetwarzaniu jej danych. Powołanie się na ww. wyłączenie dla przykładu znajdowałoby uzasadnienie przy zawarciu drugiej tożsamej rodzajowo i zakresowo umowie.

Czy, a jeśli tak, to, na jakich zasadach osoby wykonujące usługi na podstawie umów cywilnoprawnych mają dostęp do danych będących w dyspozycji ich administratora?

Często rodzi się pytanie, w jakich ramach prawnych osoby fizyczne wykonujące usługi na podstawie umów cywilnoprawnych, w tym również osoby wykonujące zadania w ramach tzw. samozatrudnienia, mogą uzyskiwać dostęp do danych osobowych będących w dyspozycji podmiotu zatrudniającego te osoby w tych formach. Należy pamiętać, że podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego, mająca dostęp do danych osobowych, przetwarzają je wyłącznie na polecenie administratora, chyba, że inne przepisy przewidują od tego wyjątek. W razie pozostawania przez pracownika z pracodawcą w stosunku pracy, może on przetwarzać dane osobowe administrowane przez pracodawcę na podstawie udzielonego upoważnienia. W sytuacji, gdy administrator korzysta również z cywilnoprawnych form zatrudnienia (w tym także samozatrudnienia), gdzie tak zatrudnione osoby w efekcie przy przetwarzaniu danych osobowych korzystają ze środków i rozwiązań organizacyjnych administratora (np. systemów, pomieszczeń), a ponadto robią to na polecenie administratora, również należy uznać upoważnienie, jako warunek dopuszczający przetwarzanie danych. Administrator, zgodnie z zasadą rozliczalności, powinien móc udowodnić fakt udzielenia upoważnienia do przetwarzania danych. W takich sytuacjach, co do zasady nie dochodzi więc do powierzenia przetwarzania danych.

Na jakiej podstawie przedsiębiorcy wykonujący wybrane operacje na danych osobowych na zlecenie ich administratora mają do nich dostęp?

W sytuacji typowego zlecania części operacji przetwarzania danych osobowych (gałęzi – np. danych kadrowych, płacowych) innym podmiotom, które są wyodrębnione od jednostki organizacyjnej administratora, dokonują one przetwarzania w swoich własnych systemach, przekazując administratorowi ewentualnie efekt swoich działań. W konsekwencji należy uznać, że takie podmioty nie stanowią szeroko rozumianego personelu administratora, co oznacza, iż przetwarzają one dane na zasadach powierzenia. Determinuje to konieczność zawarcia z nimi umowy powierzenia. Dla przykładu może to dotyczyć prowadzenia księgowości przez biuro rachunkowe, hostingu, czy prowadzenia rekrutacji czy działań szkoleniowych realizowanych poza strukturą pracodawcy.

Czy jest dopuszczalne przetwarzanie danych dotyczących kontrahentów, z którymi aktualnie się już nie współpracuje, lecz taka współpraca może być nawiązana na nowo w przyszłości?

W przypadku posiadania przez administratora swojej bazy kontrahentów (osób fizycznych), podstawę przetwarzania ich danych w celach przyszłej współpracy należy upatrywać w udzielonej zgodzie. W razie stałej współpracy między podmiotami, można również wskazywać na niezbędność przetwarzania danych do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Uzasadniony interes administratora powinien być z góry określony i podany do wiadomości osoby, której dane dotyczą.

5.2 Przetwarzanie danych pracowników tymczasowych.

Szczególną cechą zatrudnienia pracowników tymczasowych jest to, że agencja pracy tymczasowej zatrudnia pracownika na podstawie umowy o pracę na czas określony lub umowy o pracę na czas wykonania pracy wyłącznie w celu delegowania go do pracodawcy użytkownika, który z pracy tej korzysta i ją nadzoruje[20].

Zatrudniam pracownika tymczasowego. Kto jest administratorem danych takiego pracownika: agencja pracy tymczasowej czy pracodawca użytkownik?

Pracownik tymczasowy jest osobą zatrudnioną przez agencję pracy tymczasowej. Zasadniczo zatem administratorem danych osobowych pracowników tymczasowych jest agencja pracy tymczasowej. Jednocześnie, stosunek pracy tymczasowej wymaga, aby agencja zawarła z pracodawcą użytkownikiem umowę powierzenia przetwarzania danych osób świadczących pracę tymczasową, która określałaby zakres i cel przetwarzania przez niego danych. Jednakże konieczność wykonywania przez pracodawcę użytkownika niektórych, wymienionych w ustawie o zatrudnianiu pracowników tymczasowych, uprawnień i obowiązków pracodawcy (np. dotyczących prowadzenia ewidencji czasu pracy pracownika tymczasowego w zakresie i na zasadach obowiązujących w stosunku do jego pracowników) powoduje, że w tym zakresie będzie mu przysługiwał status administratora danych osobowych osób świadczących u niego pracę tymczasową. Pracodawca użytkownik będzie zatem administratorem danych osobowych wszystkich pracowników, w tym pracowników tymczasowych, zawartych np. w ewidencji czasu pracy.

Z tego powodu to pracodawca użytkownik, jako administrator danych, winien uregulować kwestię dostępu do danych osobowych bezpośrednio z pracownikiem tymczasowym i wydać mu stosowne upoważnienie do przetwarzania danych osobowych, o ile oczywiście w ramach wykonywania powierzonych mu obowiązków służbowych ma do nich dostęp.

20 Sytuację prawną pracowników tymczasowych regulują przepisy ustawy z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych (t.j. Dz. U. z 2018 r., poz. 594).

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
https://uodo.gov.pl