

OCHRONA DANYCH OSOBOWYCH W ZAKŁADACH PRACY

1. Kodeksowe zasady przetwarzania danych pracowników	str. 1	6. Jakich danych o pracowniku może żądać komornik?	str. 3
2. Przetwarzanie danych osobowych przez pracodawcę w czasie epidemii	str. 2	7. Przechowywanie zaświadczeń z danymi dzieci pracowników	str. 3
3. Czynności kontrolne pracodawcy a ochrona danych pracowników	str. 2	8. Nazwiska pracowników obsługujących maszynę	str. 4
4. Przetwarzanie danych biometrycznych pracowników	str. 3	9. Dane osobowe pracowników w zakładzie medycyny pracy	str. 4
5. Papierowa lista obecności pracowników	str. 3	10. Umowa powierzenia z firmą odkażającą	str. 4
		11. Prowadzenie szkoleń z zakresu bhp	str. 4
		12. Zatrudnianie cudzoziemców w świetle RODO	str. 4

1. Kodeksowe zasady przetwarzania danych pracowników

Przepisy Kodeksu pracy wyrażnie określają, jakich danych na etapie zatrudnienia może żądać pracodawca od kandydata do pracy, a także od zatrudnionych już pracowników. Katalog danych, których pracodawca może żądać od kandydata do pracy, w celu podjęcia działań zmierzających do zawarcia z nim umowy, określa art. 22¹ § 1 Kodeksu pracy. Zakres danych, jakich może żądać pracodawca od zatrudnionego już pracownika określa art. 22¹ § 3 Kodeksu pracy (patrz tabela). Pracodawca żąda podania innych danych osobowych niż określone we wskazanych przepisach, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której dane dotyczą. Pracodawca może żądać udokumentowania danych osobowych osób, w zakresie niezbędnym do ich potwierdzenia. Zgoda kandydata do pracy lub pracownika na przetwarzanie jego danych osobowych nie jest potrzebna, gdy chodzi o zakres danych wynikających z art. 22¹ K.p., bowiem w procesie rekrutacyjnym lub w sprawach związanych z zatrudnianiem pracowników uprawnienie do przetwarzania danych osobowych wynika z tego przepisu.

Pozostałe podstawy przetwarzania

Opisane zasady nie oznaczają, że pracodawca nie może żądać od kandydata do pracy lub pracownika innych danych osobowych niż te wymienione w art. 22¹ Kodeksu pracy. Pracodawca może bowiem zażądać podania innych danych osobowych, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Przykładowo, pracodawca nie może domagać się danych dotyczących ewentualnej ciąży pracownicy, jednak wyjątkowo jest to dopuszczalne, gdy chodzi o zatrudnienie

przy pracy wzbронionej pracownikom ciężarnym. Może się też zdarzyć, że osoba kandydująca na konkretne stanowisko będzie musiała spełnić pewne określone prawem wymogi, np. wymóg dotyczący niekaralności i wówczas pracodawca będzie uprawniony do pozyskania informacji o niej w tym zakresie.

Na przekazanie swoich danych osobowych kandydat na pracownika może również wyrazić zgodę. Przy czym na podstawie zgody nie mogą być przetwarzane dane dotyczące wyroków i skazań (ich przetwarzanie może dopuszczać tylko przepis prawa). Natomiast do przetwarzania danych szczególnych kategorii (inaczej wrażliwych np. o stanie zdrowia) określonych w art. 9 ust. 1 RODO może dojść wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie.

Do przetwarzania danych osobowych szczególnych kategorii mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

RODO a praca zdalna

W związku z wciąż trwającym stanem epidemii w wielu zakładach pracy część załogi przeszła w tryb pracy zdalnej i pracuje z domu, nierzadko na własnym sprzęcie i korzystając z prywatnej poczty elektronicznej. Taka praca często wiąże się z przetwarzaniem danych osobowych innych pracowników, kontrahentów czy klientów. Inne warunki pracy oraz korzystanie z narzędzi elektronicznych powoduje większe niebezpieczeństwo utraty lub naruszenia ochrony danych osobowych.

W celu przeciwdziałania

COVID-19 pracodawca może polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna). Skierowanie pracowników do pracy zdalnej powinno poprzedzać wprowadzenie odpowiednich regulacji, np. w zakresie ochrony danych. Niewątpliwie home-office w wielu przypadkach wiąże się z przetwarzaniem danych osobowych. Pracownicy tworzą np. korespondencję wysłaną do kontrahentów czy klientów, operując ich danymi osobowymi. To wiąże się z potencjalnymi zagrożeniami, które należy uwzględnić i im przeciwdziałać. Co więcej, mogą też pojawiać się zupełnie inne zagrożenia niż te, z którymi pracownik miał do czynienia w biurze.

Pracodawca powinien kwestie pracy zdalnej uregulować w swojej wewnętrznej dokumentacji. Dobrym rozwiązaniem jest opracowanie i wdrożenie regulaminu pracy zdalnej. Ponadto w razie potrzeby warto dostosować lub uaktualnić obowiązującą u administratora dokumentację dotyczącą ochrony danych osobowych. Eksperti wskazują, że konieczne jest też stworzenie lub aktualizacja dokumentu zawierającego wykaz zabezpieczeń stosowanych w celu ochrony danych oraz prowadzenie ewidencji urządzeń przenośnych, które mają dostęp do danych firmowych. Trzeba bowiem przypomnieć, iż to na administratorze danych (spółce, jednoosobowym przedsiębiorcy, szkole, instytucji) ciąży obowiązek ewentualnego wykazania, iż przetwarza on dane osobowe zgodnie z wymaganiami RODO (zasada rozliczalności).

UODO na swojej stronie internetowej www.uodo.gov.pl udostępnił kilka porad dotyczących bezpieczeństwa danych osobowych podczas pracy poza biurem. Oczywiście ich zastosowanie jest zróżnicowane i zależne od tego, czy pracownik pracuje na sprzęcie przekazanym mu przez pracodawcę, czy też na własnym.

Przed wszystkim UODO zwraca uwagę, iż przystępując do pracy zdalnej w domu warto wydzielić sobie odpowiednią przestrzeń, tak aby inne osoby (np. dzieci) nie miały dostępu do dokumentów aktualnie wykorzystywanych w pracy. Odchodząc od stanowiska pracy, każdorazowo należy zablokować urządzenie, na którym się pracuje. Komputer, na którym pracuje zdalnie pracownik, powinien być dobrze zabezpieczony m.in. poprzez używanie silnych haseł dostępu czy wielopoziomowe uwierzytelnianie. Takie działania ograniczają ryzyko utraty danych w przypadku kradzieży lub zgubienia urządzenia. Wszystkie urządzenia, na których pracuje pracownik, muszą mieć niezbędne aktualizacje systemu operacyjnego, oprogramowania oraz systemu antywirusowego. Mimo pracy w domu pracownik powinien postępować zgodnie z przyjętymi w jego jednostce (firmie czy instytucji) zasadami ochrony danych, np. dotyczącymi wysyłania poczty elektronicznej czy przenoszenia danych na nośnikach zewnętrznych. Do wysyłania poczty elektronicznej należy używać służbowych kont. Jeżeli pracownik wykorzystuje prywat-

nego e-maila, powinien jego treść i załączniki właściwie szyfrować. Nie należy przysyłać e-mailem informacji zaszyfrowanej razem z hasłem, nawet w osobnej wiadomości. Przed wysłaniem e-maila trzeba upewnić się, że wysyła się go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe. Nie należy otwierać wiadomości od nieznanego nadawcy, zwłaszcza załączników oraz zawartych w takich wiadomościach linków. Nie można wpisywać danych osobowych lub poufnych informacji w temacie wiadomości pocztowej.

Pracownik powinien podejmować szczególne środki, aby urządzenia, z których korzysta podczas pracy, szczególnie te wykorzystywane do przenoszenia danych, jak dyski zewnętrzne, nie zostały zgubione. Jeżeli takie urządzenie zostanie zagubione lub skradzione, natychmiast należy podjąć odpowiednie kroki, aby, o ile to możliwe, zdalnie wyczyścić jego pamięć. Oprócz tego trzeba korzystać tylko z zaufanego dostępu do sieci lub chmury oraz przestrzegać wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych.

Dane przetwarzane na etapie rekrutacji	Dodatkowe dane uzyskiwane od pracowników
- imię (imiona) i nazwisko,	- adres zamieszkania,
- data urodzenia,	- numer PESEL a w przypadku jego braku - rodzaj i numer dokumentu potwierdzającego tożsamość,
- dane kontaktowe wskazane przez taką osobę,	- inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,
- wykształcenie,	- wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie,
- kwalifikacje zawodowe,	- numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.
- przebieg dotychczasowego zatrudnienia	
pracodawca może żądać podania tych danych, jeśli jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku.	

2. Przetwarzanie danych osobowych przez pracodawcę w czasie epidemii

W czasie trwania epidemii dane o stanie zdrowia osób fizycznych przetwarzają zarówno służby ochrony zdrowia, instytucje publiczne, ale także pracodawcy. To właśnie ci ostatni mają największe problemy, bowiem muszą decydować o dopuszczeniu pracownika do wykonywania obowiązków czy też skierowania go do pracy zdalnej. W grę wchodzi np. aspekty dotyczące informowania pozostałych pracowników o zakażeniu jednego z nich.

Dane w kontekście epidemii

Wskazówki dotyczące tego co może, a czego nie powinien robić pracodawca można znaleźć w oświadczeniu Europejskiej Rady Ochrony Danych (EROD) w sprawie przetwarzania danych osobowych podczas zwalczania światowej pandemii koronawirusa. Przede wszystkim Rada wyraźnie potwierdza, iż RODO nie ogranicza możliwości przetwarzania danych osobowych w czasie trwania pandemii. Pozwala właściwym organom do spraw zdrowia publicznego i pracodawcom na przetwarzanie danych osobowych w kontekście epidemii, zgodnie z prawem krajowym i na określonych w nim warunkach. Obecnie problemem w naszym kraju jest brak regulacji ustawowych w tym zakresie, a to właśnie do nich odwołuje się EROD. Motyw 46 RODO stanowi, że

przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest to niezbędne do ochrony interesu, który ma istotne znaczenie dla życia osoby, której dane dotyczą, np. gdy przetwarzanie jest potrzebne do celów humanitarnych, w tym monitorowania epidemii i jej rozprzestrzeniania się. Z kolei motyw 54 RODO stwierdza, że możliwe jest przetwarzanie danych szczególnych kategorii np. o stanie zdrowia ze względu na istotny interes publiczny w dziedzinie zdrowia publicznego. W tych okolicznościach osoby fizyczne nie muszą wyrażać zgody na przetwarzanie ich danych.

Jednocześnie Rada wskazuje, iż dane osobowe, które są niezbędne do osiągnięcia zamierzonych celów, powinny być przetwarzane w konkretnych i wyraźnych celach. Zawsze, również w czasie tak szczególnym jak pandemia, należy pamiętać o prawach, jakie przysługują osobom, których dane są przetwarzane. Jednym z głównych uprawnień jest prawo do informacji. Osoby, których dane dotyczą, powinny otrzymywać przejrzyste informacje na temat prowadzonych działań w zakresie przetwarzania oraz ich głównych cech, w tym okresu przechowywania gromadzonych danych i celach przetwarzania. Dostarczane informacje powinny być łatwo dostępne oraz przedstawione jasnym i pro-

stym językiem. Przetwarzane dane muszą być właściwie zabezpieczone, a służyć temu powinny odpowiednie środki bezpieczeństwa i polityki poufności zapewniające, że dane osobowe nie są ujawniane nieupoważnionym stronom.

Środki wdrożone w celu zarządzania bieżącą sytuacją nadzwyczajną oraz leżący u ich podstaw proces decyzyjny powinny być odpowiednio udokumentowane.

Pomiar temperatury

Duży problem z przetwarzaniem danych osobowych dotyczących zdrowia mają obecnie pracodawcy. Ich głównym celem powinno być teraz zapewnienie bezpieczeństwa pracowników w miejscu pracy oraz utrzymanie miejsc pracy. Rodzi to pytanie, w jakim zakresie mogą przetwarzać dane osobowe pracowników dotyczące ich zdrowia. EROD stwierdza, iż w kontekście zatrudnienia przetwarzanie danych osobowych może być konieczne do wypełnienia obowiązku prawnego, któremu podlega pracodawca, np. obowiązków związanych ze zdrowiem i bezpieczeństwem w miejscu pracy lub z interesem publicznym, takim jak kontrola chorób i innych zagrożeń dla zdrowia.

Zasadniczo RODO przewiduje zakaz przetwarzania danych wrażliwych i dopuszcza odstępstwa od tego zakazu tylko w szczególnych przypadkach, np. gdy jest to ko-

nieczne ze względu na istotny interes publiczny w dziedzinie zdrowia publicznego (art. 9 ust. 2 lit. i), na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego lub gdy istnieje potrzeba ochrony żywotnych interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. c), ponieważ motyw 46 wyrażnie odnosi się do kontroli epidemii.

Na pytanie, czy pracodawca może przeprowadzać badania pracowników, niestety odpowiedź Rady jest bardzo ogólna. Stwierdza bowiem, iż powinny o tym decydować krajowe przepisy dotyczące zatrudnienia lub zdrowia i bezpieczeństwa pracowników. Pracodawcy powinni mieć dostęp do danych dotyczących zdrowia i przetwarzać je tylko wtedy, gdy wymagają tego ich własne zobowiązania prawne.

Póki co takie przepisy nie znalazły się w ustawie o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz w jej nowelizacji. Obecnie eksperci stoją na stanowisku, iż pracodawca nie może samodzielnie dokonywać żadnej oceny stanu zdrowia pracownika np. poprzez mierzenie mu temperatury. Jeśli stan pracownika budzi jego wątpliwości, powinien skierować go do lekarza lub umożliwić mu wykonywanie pracy zdalnej. Niektó-

rzy eksperci stoją na stanowisku, że pracodawca może zapewnić pracownikom możliwość samodzielnego pomiaru temperatury albo dokonywać pomiaru, jednak bez rejestracji tego faktu.

Informowanie o zakażeniach

Drugie z zagadnień, z którymi zmierzyła się Rada, dotyczyło możliwości ujawniania przez pracodawcę pracownikom lub innym osobom informacji o pracownikach zakażonych koronawirusem, w aspekcie ochrony ich danych osobowych. Rada uznała, że: „Pracodawcy powinni informować pracowników o przypadkach COVID-19 i podejmować środki ochronne, ale nie powinni przekazywać więcej informacji niż jest to konieczne. W przypadkach, w których konieczne jest ujawnienie nazwiska pracownika, który zarażony jest wirusem (np. w kontekście profilaktyki), a prawo krajowe na to zezwala, pracownicy, których sprawa dotyczy, powinni zostać poinformowani z wyprzedzeniem, a ich godność i uczciwość powinny być chronione”. Na gruncie polskiego prawa aspekt ten na razie nie został uregulowany. Wydaje się więc, iż taka informacja powinna być ujawniona jedynie osobom, które np. miały bezpośredni kontakt z zakażonym pracownikiem i muszą poddać się obowiązkowej kwarantannie.

3. Czynności kontrolne pracodawcy a ochrona danych pracowników

Pracodawcy w stosunku do zatrudnionych przez niego pracowników przysługują pewne uprawnienia kontrolne. Przykładowo ma prawo monitorować służbową pocztę elektroniczną pracownika czy też korzystać z urządzeń monitorujących przejazd samochodem służbowym. Przy czym z przysługujących mu uprawnień może korzystać po spełnieniu wymagań określonych przepisami. W takich przypadkach również należy pamiętać o ochronie danych osobowych kontrolowanych pracowników.

Rodzaje monitoringu

Możliwość stosowania monitoringu wizyjnego, monitoringu poczty elektronicznej oraz innych form monitoringu dopuszczają art. 22² i 22³ § 4 Kodeksu pracy.

Wprowadzenie monitoringu wizyjnego nad terenem zakładu pracy lub wokół niego jest możliwe, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników, ochrony mienia lub kontroli produkcji albo zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Pracodawca, który planuje wprowadzić monitoring, musi przede wszystkim sprawdzić, czy ma ku temu podstawę prawną, tzn. czy właściwe przepisy upoważniają go do przetwarzania danych osobowych w ramach monitoringu. Przesłanką do zainstalowania kamer monitoringu może być wypełnianie obowiązku prawnego, jaki spoczywa na administratorze, wykonywanie zadań realizowanych w interesie publicznym albo uzasadniony interes administratora. Drugim krokiem, jaki musi podjąć pracodawca, jest poinformowanie pracowników o prowadzeniu mo-

onitoringu na terenie zakładu pracy (instytucji). W związku z tym należy spełnić obowiązki informacyjne wynikające z art. 13 ust. 1 i 2 RODO.

Kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej) można stosować w przypadku, gdy jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Taki monitoring nie może jednak naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Przed wprowadzeniem monitoringu poczty pracodawca musi określić cele, zakres oraz sposób zastosowania monitoringu. Informacje te muszą znaleźć się 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. O wprowadzeniu monitoringu należy poinformować pracowników w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem. Również przed dopuszczeniem każdego nowego pracownika do pracy trzeba przekazać mu na piśmie informacje dotyczące zasad monitorowania poczty elektronicznej pracowników.

GPS w firmowych autach

Wprowadzenie urządzeń monitorujących samochód (GPS) możliwe jest po spełnieniu analogicznych warunków, jak w przypadku wprowadzenia w firmie monitoringu poczty elektronicznej. Należy więc poinformować pracowników o stosowaniu takie-

go monitoringu przed przystąpieniem pracownika do pracy bądź na 2 tygodnie przed uruchomieniem monitoringu. Poza tym w monitorowanych pojazdach trzeba umieścić oznakowanie informujące o tym, że trasa pojazdu i jego wykorzystanie będzie monitorowane za pomocą urządzenia lokalizującego. Informacje o tym, jakie dane przy pomocy takiego urządzenia będą zbierane, gdzie rejestrowane, jak długo przechowywane i kto będzie miał do nich wgląd, muszą być dostępne dla pracowników.

Problemy pojawiają się w sytuacji, gdy pojazd jest wykorzystywany przez pracownika również w celach prywatnych. Najlepszym rozwiązaniem jest precyzyjne określenie, że samochód służbowy używany jest tylko do celów służbowych. Jeżeli jednak nie jest to możliwe, należy dostosować lub zmienić regulamin wykorzystywania samochodu służbowego do celów prywatnych i uzyskać zgodę pracownika na przetwarzanie jego danych w omawianym zakresie oraz wypełnić wobec niego obowiązków informacyjny określony w art. 13 ust. 1 i 2 RODO.

Badania trzeźwości

Prezes Urzędu Ochrony Danych Osobowych stoi na stanowisku, iż nie można traktować badania stanu trzeźwości pracowników jako formy monitorowania pracy pracowników, o której mowa w art. 22³ § 4 Kodeksu pracy, ani jako działania niezbędnego dla zapewnienia ogółowi pracowników bezpiecznych lub higienicznych warunków pracy, czy też jako usprawiedliwione ze względu na uzasadniony interes pracodawcy. Stan nietrzeźwości pracownika zalicza się do danych dotyczących zdrowia, określonych w art. 9 ust. 1

RODO. Zasady, na jakich można przeprowadzić badanie trzeźwości pracownika, określa art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2019 r. poz. 2277 ze zm.). Stanowi on, że stan trzeźwości pracowników można sprawdzać, ale tylko wtedy, gdy łącznie są spełnione dwa warunki:

- badanie odbywa się na żądanie kierownika zakładu pracy, osoby przez niego upoważnionej lub pracownika, co do którego zachodzi uzasadnione podejrzenie, że spożywał alkohol w czasie pracy lub stawiał się do niej w stanie po użyciu alkoholu,
- badanie stanu trzeźwości pracownika przeprowadza uprawniony organ powołany do ochrony porządku publicznego (np. policja), zaś zabiegu pobrania krwi dokonuje osoba posiadająca odpowiednie kwalifikacje zawodowe, co ma zapewnić wiarygodność wyniku badania.

Zgodnie z ustawą o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi dopiero, gdy zachodzi uzasadnione podejrzenie, że pracownik stawiał się do pracy w stanie po użyciu alkoholu albo spożywał alkohol w czasie wykonywania obowiązków służbowych, to kierownik zakładu pracy lub osoba przez niego upoważniona mają obowiązek niedopuszcze-

nia takiej osoby do pracy. W takiej sytuacji pracodawca w ogóle nie musi np. wzywać policji, by zbadała alkomatem pracownika. Samo uzasadnione podejrzenie, że dana osoba jest pod wpływem alkoholu jest wystarczające, by nie dopuścić jej do pracy. Brzmienie ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi wyklucza więc wyrwykowe czy prewencyjne badania pracowników alkomatem.

W związku z takim stanowiskiem Prezes UODO w wnioskiem o wydanie objaśnień prawnych w tej materii wystąpił do Ministerstwa Rodziny, Pracy i Polityki Społecznej Rzecznik Małych i Średnich Przedsiębiorców. W swojej odpowiedzi Ministerstwo potwierdziło stanowisko Prezesa UODO w sprawie przeprowadzania kontroli trzeźwości pracowników. Wskazało również, że objaśnienia prawne ustawy – Prawo przedsiębiorców służą jedynie zapewnieniu jednolitego stosowania przepisów prawa z zakresu działalności gospodarczej. Nie powinny one zatem być stosowane do przepisów RODO, czyli aktu prawnego o zakresie szerszym niż działalność gospodarcza. Ministerstwo wskazało, że organem sprawującym nadzór nad właściwym przestrzeganiem przepisów o ochronie danych osobowych jest zaś Prezes UODO.

W obecnym stanie prawnym pracodawcy nie mogą samodzielnie prowadzić kontroli stanu trzeźwości pracowników, w tym kontroli wyrwykowych. Przesądza o tym art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi. W opinii UODO wiedza o tym, czy ktoś jest nietrzeźwy, jest informacją o stanie zdrowia. Badanie stanu trzeźwości pracownika może przeprowadzić policja, ale nie pracodawca.

źródło: www.uodo.gov.pl

4. Przetwarzanie danych biometrycznych pracowników

Spółka planuje instalację czytników linii papilarnych, uprawniających niektórych pracowników do wstępu do pomieszczeń szczególnie chronionych. Czy przepisy RODO zezwalają pracodawcy na przetwarzanie danych za pomocą takich urządzeń?

Dane biometryczne służące do jednoznacznego zidentyfikowania osoby fizycznej należą do szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO). Zasadniczo unijne rozporządzenie zabrania przetwarzania takich danych. Wyjątki od tej zasady przewiduje art. 9 ust. 2 RODO. Przykładowo przetwarzanie takich danych możliwe jest, gdy jest to niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Przetwarzanie takich danych możliwe jest również, gdy osoba, której dane dotyczą, udzieliła na to wyraźnej zgody. Na gruncie krajowych przepisów zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 ust. 1 RODO, wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika.

Kodeks pracy w art. 22^{1b} § 2 daje podstawę do przetwarzania tzw. danych biometrycznych. Przepis ten wyraźnie stanowi, że przetwarzanie danych biometrycznych pracownika jest dopuszczalne także wtedy (bez jego zgo-

dy oraz inicjatywy), gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony. Urząd Ochrony Danych Osobowych na stronie www.uodo.gov.pl wyraził stanowisko, iż: „Przetwarzanie danych biometrycznych mocno ingeruje w prywatność osób, powoduje liczne zagrożenia, jak np. możliwość ujawnienia danych szczególnych kategorii czy doprowadzenie do dyskryminacji. Dlatego budowa każdego systemu przetwarzania danych biometrycznych powinna być poprzedzona przeprowadzeniem oceny skutków dla ochrony danych, a ostateczna decyzja o jego zastosowaniu uwzględniać podstawowe zasady ochrony danych osobowych, takie jak niezbędność, celowość oraz proporcjonalność”.

Trzeba pamiętać, iż do przetwarzania danych osobowych, o których mowa w art. 9 ust. 1 RODO (tj. szczególnych kategorii), mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych nadane przez pracodawcę, a osoby dopuszczone do ich przetwarzania są obowiązane do zachowania tajemnicy.

7. Przechowywanie zaświadczeń z danymi dzieci pracowników

Pracownica chce zgłosić do ubezpieczenia dziecko, które ukończyło 18 lat i kontynuuje naukę. Czy w takiej sytuacji pracodawca powinien przechowywać zaświadczenie o pobieraniu nauki przez dziecko pracownicy?

Wydaje się, iż w przypadku, o którym mowa w pytaniu, przechowywanie takiego zaświadczenia będzie niepotrzebnym gromadzeniem tzw. danych nadmiarowych przez pracodawcę. Wystarczające w tym zakresie będzie odebranie od pracownika oświadczenia o kontynuowaniu nauki przez jego dziecko, ewentualnie zażądanie wglądu do takiego dokumentu. Zakres danych, jakie może przetwarzać pracodawca, określa art. 22¹ Kodeksu pracy. Na etapie rekrutacji pracodawca ma prawo wymagać podania danych osobowych obejmujących:

- imię (imiona) i nazwisko,
- datę urodzenia,
- dane kontaktowe wskazane przez taką osobę,
- wykształcenie,
- kwalifikacje zawodowe,
- przebieg dotychczasowego zatrudnienia.

Niezależnie od tych danych pracodawca ma prawo żądać od pracownika podania:

- adresu zamieszkania,
- numeru PESEL, a w przypadku jego braku – rodzaju i numeru dokumentu potwierdzającego tożsamość,
- innych danych osobowych pracownika, a także danych osobowych dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez

pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,

- wykształcenia i przebiegu dotychczasowego zatrudnienia, jeśli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie,
- numeru rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Oczywiście pracodawca ma prawo żądać podania innych danych osobowych niż określone w przytoczonych katalogach, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Zasadniczo udostępnienie pracodawcy danych osobowych na-

stępuje w formie oświadczenia osoby, której one dotyczą.

Rodzic podlegający ubezpieczeniu zdrowotnemu ma obowiązek zgłosić do ubezpieczenia zdrowotnego swoje dziecko do ukończenia przez nie 18 lat. Takiemu zgłoszeniu podlega też dziecko do ukończenia 26 lat kontynuujące naukę (nieposiadające innego tytułu do tego ubezpieczenia). Pracownik dokonuje takiego zgłoszenia u płatnika składek, czyli u pracodawcy. Choć niektórzy pracodawcy wymagają przedłożenia zaświadczenia o kontynuowaniu nauki przez pełnoletnie dziecko, to przepisy nie wymagają dokumentowania tych danych. Oświadczenie pracownika w tym zakresie wydaje się więc być wystarczające.

Dokumentacja pracownicza według UODO

„To, w jaki sposób i jak długo należy przetwarzać dane osobowe pracowników oraz przechowywać dokumenty wchodzące w skład zasobu kadrowego, określają przepisy sektorowe. Od 1 stycznia 2019 r. obowiązują nowe przepisy dotyczące dokumentacji pracowniczej, tj. rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej w sprawie dokumentacji pracowniczej. Mają one zastosowanie do dokumentacji pracowników, których stosunek pracy został nawiązany począwszy od 1 stycznia 2019 r. (§ 19). Natomiast do dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników, pozostających w dniu wejścia w życie ww. rozporządzenia w stosunku pracy, zgromadzonych przed tym dniem, odnośnie do zakresu przetwarzanych danych stosuje się przepisy obowiązujące przed dniem wejścia w życie niniejszego rozporządzenia, tj. przepisy obowiązujące w dniu pozyskania danych”.

5. Papierowa lista obecności pracowników

W zakładzie prowadzona jest papierowa lista obecności pracowników. Czy taką listę należy prowadzić dla każdego pracownika oddzielnie, czy na jednej stronie swoją obecność może odnotowywać kilku pracowników? W jakim miejscu powinno się taką listę przechowywać?

Kwestia list obecności pracowników wciąż jest dość kontrowersyjna. Dokument ten jest dokumentem wewnętrznym pracodawcy i nie jest wprost regulowany przepisami prawa (w przeciwieństwie do ewidencji czasu pracy).

Wielu ekspertów stoi na stanowisku, że dane osobowe zawarte w liście obecności, która jest dostępna tylko wewnątrz jednostki (wśród pracowników), nie podlegają szczególnej ochronie. Imię i nazwisko oraz ewentualna nieobecność pracownika, bez po-

dawania przyczyny nieobecności, nie podlegają ochronie, gdyż są jawne, jako związane z życiem zawodowym pracownika. Takie stanowisko potwierdza też Ministerstwo Cyfryzacji w poradniku „RODO dla administracji”. Czytamy w nim, że: „Imiona i nazwiska pracowników widnieją na drzwiach w zakładach pracy, umieszcza się je na pieczętkach imiennych, pismach sporządzanych w związku z pracą, prezentuje w informatorach o instytucjach i przedsiębiorstwach, co oznacza,

że zgodnie z powszechną praktyką są one zasadniczo jawne. Tym bardziej zatem jest uzasadnione, a nawet wskazane, aby imiona i nazwiska pracowników były udostępniane wewnątrz zakładu pracy. Na listach nie powinna być jednak ujawniana ewentualna przyczyna nieobecności w pracy, tj. urlop wypoczynkowy czy zwolnienie lekarskie”. Ministerstwo nie odnosi się jednak do kwestii praktycznego redagowania list. Wciąż można spotkać się ze stanowiskiem, zgodnie z którym na-

leży listy obecności objąć ochroną i unikać udostępniania danych osobowych zawartych w takich listach innym pracownikom. Wydaje się więc, że warto zadbać o to, by lista była skonstruowana w ten sposób, aby w jak najmniejszym stopniu udostępniać dane osób, innym osobom (np. współpracownikom). Najlepszym rozwiązaniem wydaje się być redagowanie odrębnych list obecności dla każdego z pracowników (tj. jeden pracownik na jednej stronie takiego dokumentu).

Kolejnym problemem, z którym borykają się pracodawcy, to miejsce przechowywania takich list. W wielu firmach i instytucjach

takie listy znajdują się np. w portierniach. Nie wydaje się to być błędne, pod warunkiem że dostępu do takich list nie mają osoby postronne (niebędące pracownikami) i wdrożono odpowiednie zabezpieczenia, np. w momencie opuszczenia miejsca pracy przez portiera listy są chowane. Korzystnym rozwiązaniem, zwłaszcza w małych firmach, niezatrudniających wielu pracowników, będzie odnotowywanie ich obecności na liście wydawanej przez bezpośredniego przełożonego. W większych firmach dobrym rozwiązaniem może okazać się wprowadzenie systemu elektronicznego ewidencjonowania obecności.

6. Jakich danych o pracowniku może żądać komornik?

Jako pracodawca otrzymuję od komorników pisma dotyczące pracowników, z wezwaniem do udostępnienia szeregu ich danych osobowych, takich jak np. data i miejsce urodzenia, numer rachunku bankowego, na który przekazywane jest wynagrodzenie, czy inne znane pracodawcy numery rachunków bankowych pracownika, a także wszystkie numery telefonów pracownika. Jakże dane możemy udostępniać komornikowi, aby nie narazić się na naruszenie przepisów RODO?

Niestety od lat między komornikami a organem nadzoru (Prezesem UODO – wcześniej GIODO) istnieje spór na gruncie tego, jakich danych osobowych pracownika można żądać od pracodawcy w postępowaniu egzekucyjnym. Komornicy uważają, że mogą żądać udostępnienia wszelkich danych, które umożliwią im dokonanie egzekucji majątkowej. W związku z tym wnoszą o przekazywanie im takich danych osobowych jak np.:

- NIP,
- data i miejsce urodzenia,

- numer rachunku bankowego, na który przekazywane jest wynagrodzenie,
- inne znane pracodawcy numery rachunków bankowych pracownika,
- wszystkie znane numery telefonów pracownika.

Ponadto gdy pracownik już nie pracuje wnoszą o przekazanie kopii ostatniej karty wynagrodzenia, a nawet przyczyny zwolnienia pracownika.

Jako podstawę prawną swoich żądań komornicy podają

art. 882 oraz art. 761 Kodeksu postępowania cywilnego (Dz. U. z 2020 r. poz. 1575 ze zm.).

Zgodnie z art. 882 K.p.c., dokonując zajęcia wynagrodzenia za pracę, komornik wzywa pracodawcę, aby w ciągu tygodnia: przedstawił za okres 3 miesięcy poprzedzających zajęcie, za każdy miesiąc oddzielnie, zestawienie periodycznego wynagrodzenia dłużnika za pracę oraz oddzielnie jego dochodu z wszelkich innych tytułów. Ponadto wzywa pracodawcę, aby podał, w jakiej kwocie

i w jakich terminach zajęte wynagrodzenie będzie przekazywane wierzycielowi oraz w razie istnienia przeszkód do wypłacenia wynagrodzenia za pracę, złożył oświadczenie o rodzaju tych przeszkód, a w szczególności podał, czy inne osoby roszczą sobie prawa, czy i w jakim sądzie toczy się sprawa o zajęte wynagrodzenie i czy oraz o jakie roszczenia została skierowana do zajętego wynagrodzenia egzekucja przez innych wierzycieli.

Natomiast, w myśl art. 761 K.p.c., komornik może zasięgać od organów administracji publicznej, organów wykonujących zadania z zakresu administracji publicznej, organów podatkowych, rentowych, banków, spółdzielczych kas

oszczędnościowo-kredytowych, przedsiębiorstw maklerskich, organów spółdzielni mieszkaniowych, zarządów wspólnot mieszkaniowych oraz innych podmiotów zarządzających mieszkaniami i lokalami użytkowymi, jak również innych instytucji i osób nieuczestniczących w postępowaniu, informacji niezbędnych do prowadzenia egzekucji.

Zatem komornicy mogą uzyskiwać od pracodawców tylko te informacje, do których żądania upoważnieni są na mocy obowiązujących ich przepisów. Chodzi tu o wspomniany art. 882 K.p.c. Pozostałe informacje, jak np. numer rachunku bankowego, mogą uzyskiwać od innych, uprawnionych do tego instytucji.

8. Nazwiska pracowników obsługujących maszynę

W zakładzie produkcyjnym do obsługi konkretnej maszyny uprawnionych jest kilka osób. Chcemy, aby obok każdej z takich maszyn wisiała lista pracowników uprawnionych do jej obsługi, zawierająca imię i nazwisko pracownika. Czy musimy uzyskać zgodę pracowników na umieszczenie ich danych na takiej liście?

Dane pracowników, takie jak imię i nazwisko, adres e-mail (wykorzystywany służbowo) czy numer telefonu są danymi osobowymi w rozumieniu art. 4 pkt 1 ogólnego rozporządzenia o ochronie danych osobowych (tzw. RODO). Przy czym wymienione powyżej dane osobowe są ściśle związane ze sferą zawodową pracownika i jako takie są jawne, a pracodawca ma prawo przetwarzać je również bez zgody pracownika.

Warto w tym miejscu przytoczyć, zachowujący swą ważność również pod rządami RODO,

wyrok Sądu Najwyższego z dnia 19 listopada 2003 r., sygn. akt I PK 590/02, w którym czytamy, iż: „W normalnym (...) układzie nie ma racjonalnych powodów, dla których pracownik byłby zainteresowany zachowaniem w tajemnicy swego nazwiska, i co za tym idzie, faktu związania z danym zakładem pracy. Imiona i nazwiska pracowników widnieją na drzwiach w zakładach pracy, umieszcza się je na pieczętkach imiennych, pismach sporządzanych w związku z pracą, prezentuje w informatorach o instytucjach i przedsię-

biorstwach, co oznacza że zgodnie z powszechną praktyką są one zasadniczo jawne”.

W związku z tym, lista zawierająca imię i nazwisko pracownika uprawnionego do obsługi danej maszyny, umiejscowiona w zakładzie pracy nie narusza zasad ochrony danych osobowych. Warto też zwrócić uwagę, iż lista ta nie jest upubliczniana poza miejscem pracy. Krąg osób, które mają do niej dostęp, jest więc ograniczony do innych pracowników.

Takie przetwarzanie danych osobowych pracownika nie wymaga

uzyskania jego zgody. Pracodawca może bowiem powołać się na przesłankę zawartą w art. 6 ust. 1 lit. f) RODO, na mocy której przetwarzanie danych osobowych jest zgodne z prawem, jeżeli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Takim uzasadnionym interesem pracodawcy będzie w tym przypadku prawidłowa organizacja pracy.

Pomimo braku obowiązku uzyskania zgody na przetwarzanie danych osobowych w omawianym przypadku, należy pamiętać o przekazaniu pracownikom klauzul informacyjnych zawierających informacje określone w art. 13 RODO.

12. Zatrudnianie cudzoziemców w świetle RODO

Firma planuje zatrudnić obcokrajowców. Będzie od nich żądać przedstawienia dokumentów potwierdzających ich prawo do przebywania na terytorium Polski. Na jakiej podstawie prawnej pracodawca może przetwarzać ich dane osobowe wynikające z tych dokumentów? Jak długo może je przechowywać?

Zasadniczo to, jakie dane osobowe pracowników oraz osób ubiegających się o pracę może przetwarzać pracodawca, określają przepisy Kodeksu pracy. Na mocy art. 22¹ § 1 i 3 tej ustawy są to imię i nazwisko, data urodzenia, dane kontaktowe, wykształcenie, kwalifikacje zawodowe oraz przebieg dotychczasowego zatrudnienia. Jednocześnie art. 22¹ § 4 Kodeksu pracy stanowi, iż pracodawca żąda podania innych danych osobowych niż te wspomniane wyżej, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. I z taką sytuacją będziemy mieli do czynienia w przypadku, gdy pracodawca zatrudnia cudzoziemca. Podstawą prawną do przetwarzania ich danych będzie więc art. 6 ust. 1 lit. c) RODO, uprawniający administratora do przetwarzania danych, gdy jest to niezbędne do wypełnienia ciążącego na nim obowiązku prawnego. Ten prawny obowiązek wynika z kolei z art. 2 ustawy o skutkach powierzania wykonywania pracy cudzoziemcom... (Dz. U. z 2012 r. poz. 769 ze zm.), który stanowi, iż podmiot powierzający wykonywanie pracy cudzoziemcowi jest obowiązany żądać od cudzoziemca przedstawienia przed rozpoczęciem pracy ważnego dokumentu uprawniającego do pobytu na terytorium Rzeczypospolitej Polskiej. Powołana ustawa wymaga przechowywania przez pracodawcę kopii tego dokumentu przez cały okres wykonywania pracy przez cudzoziemca.

Unijne rozporządzenie RODO dostępne jest w serwisie www.przepisy.gofin.pl.

9. Dane osobowe pracowników w zakładzie medycyny pracy

Spółka jako pracodawca zamierza podpisać umowę z zakładem medycyny pracy na badania pracowników z zakresu medycyny pracy. Czy strony powinny zawrzeć umowę powierzenia w zakresie ochrony danych osobowych?

NIE. Zgodnie z interpretacjami m.in. Urzędu Ochrony Danych Osobowych, zakłady medycyny pracy nie są podmiotami przetwarzającymi w rozumieniu art. 4 pkt 8 ogólnego rozporządzenia o ochronie danych osobowych (tzw. RODO). Takim podmiotem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Podmiot przetwarzający musi być odrębnym od administratora podmiotem i musi wykonywać operacje przetwarzania w imieniu

administratora danych. O konieczności scedowania niektórych obowiązków na rzecz innego pomiotu decyduje sam administrator danych (w niektórych okolicznościach taki obowiązek może wynikać z obowiązujących przepisów np. w sferze publicznej). Co istotne, pomimo przekazania tych obowiązków o celach przetwarzania danych osobowych nadal decyduje administrator danych, on również odpowiada za prawidłową ochronę danych osobowych, w stosunku do których jest administratorem. Podmiot przetwarzający może natomiast

dokonywać tylko takich czynności przetwarzania na danych osobowych, które mu powierzono, do jakich obliguje go umowa.

Ośrodki medycyny pracy nie są podmiotami przetwarzającymi. W zakresie wykonywanych czynności są odrębnymi administratorami danych. Zakład medycyny pracy nie przetwarza danych w imieniu pracodawcy, tylko realizuje własne cele wynikające z obowiązków prawnych. Pomimo skierowania pracownika przez pracodawcę, to zakład medycyny pracy samodzielnie zbiera dane medyczne

pacjenta i realizuje szereg celów wynikających z obowiązujących go przepisów np. rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy, a także rozporządzenia Ministra Zdrowia w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzorów stosowanych dokumentów. W związku z powyższym nie ma potrzeby zawierania umowy powierzenia przez pracodawcę z takim zakładem.

10. Umowa powierzenia z firmą odkażającą

W związku z panującą sytuacją epidemiczną chcemy przekazywać wyspecjalizowanej firmie dokumenty do fumigacji. Dokumenty będą znajdować się w opisanych i zamkniętych kartonach. Czy z taką firmą powinniśmy zawrzeć umowę powierzenia?

Fumigacja (odkażanie) ma na celu zwalczanie drobnoustrojów, szkodników, bakterii i wszelkich grzybów, które mogą rozwijać się na różnego rodzaju materiałach, również na dokumentach. To, czy podmiot świadczący usługi fumigacji ma status podmiotu przetwarzającego, zależy od tego, czy przekazywane dokumenty zawierają dane osobowe. Nie ma tu znaczenia, czy dokumenty te są zapakowane w kartony czy też nie. Jeżeli dokumenty, które podlegają fumigacji zawierają dane osobowe, wówczas podmiot, który bę-

dzie przeprowadzał odkażanie, jest podmiotem przetwarzającym i konieczne jest zawarcie z nim umowy powierzenia. Takie stanowisko prezentuje UODO na swojej stronie internetowej www.uodo.gov.pl. Czytamy w nim, iż: „Powierzenie przetwarzania danych osobowych będzie uzasadnione w sytuacji, jeśli administrator danych – w celu skorzystania z usługi fumigacji – przekazuje dokumenty zawierające dane osobowe, niezależnie od tego, czy dokumenty te są zapakowane w kartony. Powierzenie przetwarzania danych jest

bowiem wówczas uzasadnieniem prawnym dla przekazania danych innemu, zewnętrznemu podmiotowi, a jednocześnie instrumentem służącym zapewnieniu przez administratora kontroli nad przetwarzanymi danymi osobowymi i ich bezpieczeństwem”.

To na administratorze danych, który chce skorzystać z usług podmiotu przetwarzającego, ciąży obowiązek wyboru tylko takiego podmiotu przetwarzającego, który daje odpowiednie gwarancje spełnienia wymogów wynikających z RODO. Podmiot przetwarzający

musi również zagwarantować, aby osoby, które będą miały do czynienia z dokumentami zawierającymi dane osobowe, były właściwie upoważnione do przetwarzania danych osobowych oraz żeby zostały zobowiązane do zachowania tajemnicy, chyba że podlegają one takiemu obowiązkowi z mocy przepisów ustawowych.

Umowa o powierzenie przetwarzania danych musi określać:

- przedmiot i czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych,
- kategorie osób, których dane dotyczą,
- obowiązki i prawa administratora.

11. Prowadzenie szkoleń z zakresu bhp

Jednostka chce zatrudnić zewnętrzną firmę do prowadzenia szkoleń z zakresu bhp. Czy wystarczające jest upoważnienie osoby prowadzącej takie szkolenie do przetwarzania danych osobowych pracowników, czy należy zawrzeć umowę powierzenia z taką firmą?

Podmiotem przetwarzającym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Cele i zakres tego przetwarzania określa administrator danych. W celu określenia, czy dany podmiot będzie podmiotem przetwarzającym, należy odpowiedzieć na pytanie, czy administrator danych mógłby powierzyć te czynności przeprowadzić we własnym zakresie. Odpowiedź będzie twierdząca, bowiem wielu pracodawców zadania służby bhp deleguje wyspecjalizowanemu pracownikowi. W takim przypadku osoba będąca jednocześnie

pracownikiem, przetwarza dane osobowe innych pracowników zatrudnionych w zakładzie pracy wyłącznie z upoważnienia administratora.

Jeżeli jednak administrator danych zdecyduje się wybrać zewnętrzną firmę, wówczas konieczne wydaje się zawarcie umowy powierzenia danych osobowych. Taka umowa może być częścią umowy na usługi lub zlecenia. Nie musi być konieczne odrębną umową, ale musi zawierać wszystkie elementy określone w przepisach RODO.

Takie stanowisko potwierdza również Ministerstwo Cyfryzacji w publikacji „RODO w administra-

cji”, w której czytamy, że: „Jeżeli administrator zdecydował się jednak na zewnętrzny podmiot, który obsługuje go w tym zakresie (bhp – przypis redakcji), należy podpisać umowę powierzenia. W takim przypadku administrator powierza bowiem innemu podmiotowi zadanie, które mógłby zrealizować samodzielnie”.

Umowa powierzenia powinna stanowić w szczególności, że podmiot przetwarzający:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora,
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały

się do zachowania tajemnicy lub aby podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

- wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić właściwy stopień bezpieczeństwa przetwarzanym danym,
- pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,
- uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO (m.in. zgła-

sza do Prezes UODO naruszenia ochrony danych osobowych),

- po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

Podstawa prawna

Ustawa z dnia 26.06.1974 r. – Kodeks pracy (Dz. U. z 2020 r. poz. 1320)
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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