Piotr Glen

Dane osobowe pracowników w pytaniach i odpowiedziach

experto24.pl

Spis treści

Wstęp

Wielu pracodawców uważa, że skoro w swojej działalności przetwarzają jedynie dane osobowe pracowników, to nie mają obowiązków wynikających z ustawy o ochronie danych osobowych. Część pracodawców natomiast pamięta o ochronie danych osobowych swoich klientów, jednak do ochrony danych pracowników nie przykłada dużej uwagi. Takie myślenie to jednak błąd. Wprawdzie pracodawca, który przetwarza tylko dane osobowe pracowników, nie musi zgłaszać zbiorów danych do rejestracji u Generalnego Inspektora Ochrony Danych Osobowych. Ma jednak wiele innych obowiązków wynikających z przepisów.

Jednym z nich jest zastosowanie odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanym danym. Trzeba też pamiętać, że nie można żądać od pracownika podania danych wrażliwych np. o stanie zdrowia czy karalności oraz że jego danych osobowych nie można dobrowolnie udostępniać.

Jakie są podstawy prawne przetwarzania danych osobowych pracowników?

W zakresie przetwarzania danych osobowych zawsze pierwszeństwo mają przepisy sektorowe, szczegółowe, w tym przypadku przepisy dotyczące prawa pracy. Ustawa o ochronie danych osobowych w sposób ogólny i końcowy opisuje zasady przetwarzania i ochrony danych. Zakres i cel przetwarzania danych pracowników dość szczegółowo opisany jest w Kodeksie pracy (art. 22^1). Dodatkowe wymagania często stawiają ustawy branżowe, jak na przykład ustawa o pracownikach samorządowych, Karta Nauczyciela czy ustawy dotyczące służb.

Podanie tam wskazanych danych jest obowiązkowe, bo jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Również ogólne rozporządzenie UE o ochronie danych osobowych (w skrócie „ogólne rozporządzenie" lub „rodo"), które będzie

obowiązywać od 25 maja 2018 r., oddaje pierwszeństwo przepisom szczegółowym w zakresie przetwarzania danych pracowników.

W prawie państwa członkowskiego lub w porozumieniach zbiorowych, w tym zakładowych porozumieniach z przedstawicielami pracowników, mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w kontekście zatrudnienia. W szczególności chodzi o warunki, na których dane osobowe w kontekście zatrudnienia można przetwarzać za zgodą pracownika do celów procedury rekrutacyjnej, wykonania umowy o pracę, w tym wykonania obowiązków określonych w przepisach lub w porozumieniach zbiorowych, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

Z pewnością ogólne rozporządzenie o ochronie danych wymusi wiele zmian w bardzo wielu polskich aktach prawnych, również w Kodeksie Pracy.

Czy pracodawca ma obowiązki informacyjne wobec swoich pracowników w związku z przetwarzaniem ich danych osobowych?

Zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych administrator danych jest obowiązany poinformować każdą osobę, której dane dotyczą o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
3) prawie dostępu do treści swoich danych oraz ich poprawiania;
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Przepisu tego nie stosuje się jednak jeżeli osoba, której dane dotyczą, posiada już powyższe informacje.

Każdy pracodawca jest oczywiście administratorem danych, chociażby ze względu na przetwarzanie danych swoich pracowników. Pracownik jednak wie przecież, gdzie pracuje, zna dane firmy, w której się zatrudnił. Ma świadomość, że jego dane, określone w przepisach prawa pracy, muszą być przetwarzane w celu zatrudnienia i dlatego ich podanie jest obowiązkowe.

Pracodawca z zasady nie udostępnia danych pracowników żadnym odbiorcom w rozumieniu art. 7 ust. 6 ustawy o ochronie danych osobowych. Odbiorcą danych natomiast nie jest między innymi podmiot, któremu administrator danych powierzył przetwarzanie danych na podstawie stosownej

umowy powierzenia, zgodnie z art. 31 ustawy o ochronie danych osobowych. Nie jest więc odbiorcą danych na przykład zewnętrzne biuro rachunkowo-księgowe, które prowadzi sprawy kadrowe przedsiębiorcy i o takim rozwiązaniu pracodawca wcale nie musi informować swoich pracowników.

Niemniej czyniąc zadość formalnościom, w regulaminie pracy lub przy okazji innych informacji, jakie pracodawca jest zobowiązany przekazać swoim pracownikom, można by zamieścić klauzulę informacyjną.

Jakie dane osobowe pracowników pracodawca może przetwarzać?

Zakres danych pracowników, jakie pracodawca może, a wręcz jest obowiązany gromadzić, wskazany jest w art. 22^1 Kodeksu Pracy. Niezależnie od danych osób ubiegających się o zatrudnienie, tj.:

1) imię (imiona) i nazwisko;
2) imiona rodziców;
3) datę urodzenia;
4) miejsce zamieszkania (adres do korespondencji);
5) wykształcenie;
6) przebieg dotychczasowego zatrudnienia.

Pracodawca ma prawo żądać od pracownika podania także innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, a ponadto numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL).

Zakres danych, jakich pracodawca może żądać od pracownika, doprecyzowany jest w rozporządzeniu ministra pracy i polityki socjalnej z 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz.U. z 1996 r. nr 62, poz. 286) i w określonym tam Załączniku nr 1a – Kwestionariusz osobowy dla pracownika. Należy zwrócić uwagę na aktualne wersje załączników, gdzie nie ma już mowy o nazwisku rodowym matki. Nie mylmy też obywatelstwa z narodowością.

Niezależnie od dyskusji i wątpliwości dotyczących tego, czy aby wskazany w art. 22^1 Kodeksu pracy zakres danych nie jest w obecnych warunkach zbyt wąski, to nie można zbierać dodatkowych danych bez odpowiedniej podstawy prawnej. Szczególnie gdy w grę wchodzą dane wrażliwe, czyli np. informacje dotyczące niekaralności czy stanu zdrowia. Pracodawca może przetwarzać tego typu dane pracowników, ale tylko wtedy, gdy określają to przepisy szczegółowe ustaw sektorowych. Inne dane osobowe będą więc wymagane np. od nauczyciela zatrudnianego w oparciu o Kartę Nauczyciela, która wymaga legitymowania się niekaralnością, a inne od sekretarki w szkole zatrudnianej już jedynie w oparciu o Kodeks pracy, a jeszcze inne od pracownika samorządowego czy funkcjonariusza służb.

Czy zbiory z danymi osobowymi pracowników należy rejestrować u Generalnego Inspektora Ochrony Danych Osobowych?

Zgodnie z art. 43 ust 1 pkt 4 ustawy o ochronie danych osobowych z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się. Dane pracowników czy kandydatów do pracy stanowią oczywiście zbiory danych, należy je ująć w wykazie zbiorów administratora danych, a same dane muszą być odpowiednio chronione, ale nie trzeba takich zbiorów zgłaszać do Generalnego Inspektora Ochrony Danych Osobowych.

Czy każdy pracownik powinien podpisać upoważnienie do przetwarzania danych osobowych?

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych (art. 37 ustawy o ochronie danych osobowych). Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38 ustawy o ochronie danych osobowych). Stosowne upoważnienia powinni więc otrzymać pracownicy, którzy wykonując swoje obowiązki służbowe muszą mieć dostęp do określonych danych osobowych.

Tym samym ewidencja osób upoważnionych do przetwarzania danych nie jest najczęściej równa ewidencji osób zatrudnionych. Upoważnienia do przetwarzania danych nie otrzyma na przykład personel techniczny, którego zakres obowiązków służbowych nie przewiduje możliwości dostępu do jakichkolwiek danych osobowych.

Kto powinien wydać pracownikowi upoważnienie do przetwarzania danych osobowych?

Artykuł 37 ustawy o ochronie danych osobowych brzmi:

„Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych”.

Należy jednak zwrócić uwagę, że forma upoważnienia do przetwarzania danych osobowych nie jest w żaden sposób określona i może być różna, tak jak i sposób i organizacja ich wydawania. Inaczej mogą

być nadawane upoważnienia w dużej korporacji zatrudniającej tysiące pracowników, zatrudnionych dodatkowo w wielu terenowych oddziałach, a inaczej w małej czy średniej firmie lub instytucji. Pamiętajmy też, że administrator danych to organ, jednostka organizacyjna decydująca o celach i środkach przetwarzania danych osobowych. Jest to więc na przykład spółka reprezentowana przez prezesa zarządu, jednostka organizacyjna reprezentowana przez dyrektora, czy firma reprezentowana przez właściciela.

Upoważnienia do przetwarzania danych powinny więc być wydawane (podpisywane) przez pracodawcę, jako administratora danych lub przez osoby, które posiadają stosowne pełnomocnictwo wydane przez pracodawcę. Procedura wydawania upoważnień, nadawania i odbierania uprawnień związanych z przetwarzaniem danych, powinna być określona w organizacji.

Czy każdy pracownik powinien przejść szkolenie z ochrony danych osobowych?

Każdy pracownik, zatrudniony na stanowisku pracy uprawniającym do dostępu do danych osobowych i innych informacji chronionych, musi być odpowiednio przeszkolony z zasad i przepisów dotyczących przetwarzania i ochrony danych osobowych. Obowiązek taki wynika z art. 36a ust. 1 pkt 2 lit. c ustawy o ochronie danych osobowych, który narzuca zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Podmioty, które wykonują zadania publiczne dodatkowo są do tego zobligowane rozporządzeniem Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526). Zgodnie z § 20 ust. 2 pkt 6 tego rozporządzenia podmiot, który realizuje zadania publiczne, powinien zapewnić szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenia bezpieczeństwa informacji,
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Rozporządzenie nie wskazuje, jak często i w jakiej formie mają takowe szkolenia być przeprowadzane. Na pewno pracownicy rozpoczynający pracę związaną z dostępem do danych powinni przejść stosowny instruktaż. Warto organizować szkolenia uzupełniające, przypominające, zwłaszcza w kontekście zachodzących zmian w przepisach prawa lub też ewentualnych aktualizacji czy zmian w polityce bezpieczeństwa informacji w danej organizacji. Może je przeprowadzać ABI (w przyszłości inspektor ochrony danych), można zapraszać zewnętrznych, wykwalifikowanych specjalistów, można

korzystać z różnego rodzaju szkoleń on-line, prezentacji uzupełnianych testami, video szkoleń. Przeprowadzenie szkolenia powinno zostać udokumentowane.

Warto przy tym wszystkim zwrócić jednak uwagę na praktyczność i skuteczność wszelkich instruktaży. Pracodawcy, jako administratorowi danych, powinno zależeć nie tylko na podpisanej liście obecności czy tak zwanym certyfikacie uczestnictwa w szkoleniu wydanym pracownikom, ale przede wszystkim na zdobytej wiedzy i świadomości, dzięki której pracownicy będą wiedzieli, jak przy obecnych zagrożeniach i pokusach chronić cenne informacje, jakimi są na przykład dane osobowe klientów. Nie wydają się więc dobrym pomysłem i rozwiązaniem szkolenia telefoniczne, oferowane czasami przez firmy, jakoby specjalizujące się w ochronie danych osobowych.

Czy pracodawca może zamieścić zdjęcie pracownika na swojej stronie internetowej bez jego zgody?

Wizerunek osoby fizycznej co do zasady jest dobrem osobistym prawnie chronionym (art. 23 Kodeksu cywilnego). Cytując zapadające już wyroki sądów, naruszenie prawa do wizerunku osoby fizycznej następowałoby wówczas, gdyby opublikowana bez zgody tej osoby fotografia wykonana była w sposób umożliwiający identyfikację tej osoby.

Zgodnie natomiast z art. 81 ustawy o prawie autorskim i prawach pokrewnych zezwolenia nie wymaga rozpowszechnianie wizerunku osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych, a także osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza. W przypadku braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

Czym innym będzie więc zamieszczenie zdjęcia prezesa czy dyrektora na stronie internetowej firmy, a czym innym opublikowanie zdjęcia pracownika obok nazwy stanowiska służbowego czy w służbowym adresie e-mailowym. Na publikacje wizerunku pracownika potrzebna jest jego zgoda. Zgoda ma być wyraźna, świadoma, dobrowolna. Nie musi być na piśmie, ale dla celów dowodowych zasadne są stosowne oświadczenia. Pozyskiwanie przez pracodawcę zgody pracownika będzie możliwe, jeżeli pracownik będzie miał możliwość odmowy jej udzielenia i nie spotkają go z tego powodu żadne konsekwencje. Należy pamiętać, że zgoda może być w każdym czasie odwołana.

Inne jednak zasady obowiązują przy służbowych identyfikatorach ze zdjęciem. Nie jest to rozpowszechnianie wizerunku. Tam, gdzie tego typu identyfikacja jest konieczna, najczęściej ze względów bezpieczeństwa, powinno być to określone w odpowiednich regulaminach pracodawcy.

Czy pytania i testy zadawane podczas procedury rekrutacyjnej są zgodne z ustawą o ochronie danych osobowych?

Pracownika można prosić o złożenie oświadczenia, wypełnienie kwestionariusza lub wykonanie testu zdolności, jedynie jeśli nie narusza to jego praw osobistych, a dostarcza informacji uznawanych za istotne do celów nawiązania stosunku pracy. Od pracowników nie wolno wymagać poddania się testowi ciążowemu lub przedstawienia jego wyników.

Pracownik ma prawo odmówić udzielenia odpowiedzi na pytania niezwiązane z określonym celem. Metody związane z oceną osobowości kandydata za pomocą testów psychologicznych czy wariografu, w całości lub w części, są nielegalne. Przed wypełnieniem kwestionariusza psychologicznego, osoba, której dane dotyczą, musi zostać poinformowana, na jakie pytania odpowie rozwiązując test i jaki jest cel tego rodzaju przetwarzania danych.

Należy podać nazwisko osoby analizującej test, ponieważ jedynie ona ma prawo poznać odpowiedzi. Po przeanalizowaniu testu mierzącego całość osobowości, należy przekazać wyniki osobie, której dane dotyczą. Osoba ta ma prawo zadecydować, czy wyniki mogą zostać przekazane osobie prowadzącej procedurę rekrutacyjną. W przypadku prostszych pytań, sprawdzających np. zdolności pracownika, nie jest konieczne uzyskanie zgody osoby zainteresowanej, a wyniki można przekazać bezpośrednio pracodawcy.

Zgodnie z zasadą ograniczenia celu przetwarzania danych, osoba, która otrzymała curriculum vitae od pracownika nie może przekazać go osobie trzeciej, ani nawet poinformować nikogo o fakcie złożenia CV, o ile osoba, której dane dotyczą nie udzieliła na to wyraźnej zgody. Osoba trzecia, to każda osoba fizyczna, osoba prawna bądź też jednostka organizacyjna nieposiadająca osobowości prawnej, której nie dotyczy dana umowa, stosunek prawny czy też inna, skonkretyzowana przepisami, relacja. Osoba trzecia, to po prostu każda nie będąca stroną umowy z pracownikiem.

Czy pracodawca ma prawo publikować na swoich stronach internetowych, takie dane osobowe pracowników jak ich imiona i nazwiska, stanowiska, dokładne miejsce pracy (numer pokoju, telefon, adres e-mail), bez zgody tych osób?

Informacje o pracowniku, takie jak jego imię i nazwisko czy służbowy adres e-mail, są ściśle związane z wykonywaną przez niego pracą. Informacje takie mogą zatem zostać podane do publicznej wiadomości przez pracodawcę, również bez zgody pracownika.

Ujawnienie przez pracodawcę nazwiska (imienia) pracownika bez jego zgody nie stanowi bezprawnego naruszenia dobra osobistego, jeżeli jest usprawiedliwione zadaniami i obowiązkami pracodawcy związanymi z prowadzeniem zakładu, jest niezbędne i nie narusza praw oraz wolności pracownika. W

stosunku do osób pełniących funkcje publiczne są to wręcz informacje publiczne. Niemniej ze względów bezpieczeństwa należałoby rozważyć upublicznianie informacji służbowych do niezbędnego minimum.

Czy obowiązek noszenia przez pracowników identyfikatorów narusza przepisy ustawy o ochronie danych osobowych?

Obowiązek noszenia przez pracowników identyfikatorów zawierających m.in. imię i nazwisko wynika z wewnętrznych uregulowań wydanych przez pracodawcę (np. z regulaminu pracy wydanego na podstawie art. 104 § 1 Kodeksu pracy). Regulamin ustala organizację i porządek pracy oraz związane z tym prawa i obowiązki pracowników. Obowiązek ujawniania w tej postaci swoich danych osobowych, jeżeli wynika z wewnętrznych przepisów obowiązujących w zakładzie pracy, nie jest sprzeczny z ustawą o ochronie danych osobowych.

Czy pracodawca może stosować monitoring w miejscu pracy (monitorowanie poczty e-mail, komunikatorów, nagrywanie rozmów telefonicznych pracowników, wideomonitoring)?

Pracodawcza ma prawo sprawdzać, w jaki sposób pracownik wykorzystuje mienie służbowe. Dlatego instalowanie systemów GPS w samochodach służbowych czy programów śledzących ruch sieciowy w Internecie jest dopuszczalne, pod warunkiem, że pracownik zostanie wcześniej poinformowany o takiej kontroli i procedurach jej przeprowadzania. Na tych samych zasadach dopuszczalna jest kontrola komputera służbowego pracownika, a nawet zawartości jego służbowej skrzynki pocztowej. Rozstrzygnął to nawet Europejski Trybunał Praw Człowieka w Strasburgu, który orzekł, że pracodawca może przeglądać służbową skrzynkę pocztową swoich pracowników i sprawdzać, czy korzystają z niej do celów prywatnych. Co więcej, szef może nawet zwolnić swojego podwładnego za wykorzystywanie poczty w ten sposób. W wyroku z 12 stycznia 2016 r. Europejski Trybunał Praw Człowieka w Strasburgu stwierdził, że:

„Nie jest nadużyciem, że pracodawca chce sprawdzić, czy jego pracownicy wykonują swoje obowiązki zawodowe w godzinach pracy. Pracodawca uzyskał dostęp do skrzynki pocztowej, myśląc, że zawiera ona jego korespondencję z klientami".

W każdym razie wykorzystanie rozmaitych technik nadzoru może być uzasadnione szczególnym charakterem pracy i działalności gospodarczej, jednak pracodawca ma obowiązek poinformowania pracowników o mechanizmach kontroli wykorzystywanych w spółce i sposobie ich zastosowania. Stosując monitoring, powinniśmy brać pod uwagę zasadę proporcjonalności, która oznacza, iż dane muszą być adekwatne i istotne dla celów przetwarzania. Dodatkowo, posługiwanie się monitoringiem

wizyjnym powinno być stosowane wyłącznie jako środek pomocniczy, w przypadku gdy istnieje cel faktycznie uzasadniający jego użycie.

Nie ma przepisów oraz orzecznictwa w zakresie stosowania kamer w miejscu pracy, ale należy brać pod uwagę kilka reguł. Nie wolno instalować kamer w miejscach, gdzie pracownik może zasadnie oczekiwać zachowania swojej prywatności, np. w przebieralni, toalecie (no chyba, że w kopalni diamentów ...). O monitorowaniu należy uprzedzić osoby, które mogą się znaleźć w zasięgu kamer, stosując np. stosowne tablice informacyjne, a zasady powinien określać odpowiedni regulamin lub instrukcja. Dokonane zapisy (taśmy) mogą być przechowywane jedynie na czas niezbędny dla celów monitorowania i w warunkach zabezpieczających je przed dostępem osób niepowołanych.

Czy pracodawca może sprawdzać trzeźwość pracowników?

Zgodnie z art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi kierownik zakładu pracy lub osoba przez niego upoważniona mają obowiązek niedopuszczenia do pracy pracownika, jeżeli zachodzi uzasadnione podejrzenie, że stawił się on do pracy w stanie po użyciu alkoholu albo spożywał alkohol w czasie pracy. Okoliczności stanowiące podstawę decyzji powinny być podane pracownikowi do wiadomości.

Uprawnienia kierownika zakładu pracy służą również organowi nadrzędnemu nad danym zakładem pracy oraz organowi uprawnionemu do przeprowadzenia kontroli zakładu pracy. Na żądanie kierownika zakładu pracy, osoby przez niego upoważnionej, a także na żądanie pracownika, badanie stanu trzeźwości pracownika przeprowadza uprawniony organ powołany do ochrony porządku (w praktyce jest to policja).

Przepisy nie rozstrzygają natomiast wyraźnie kwestii, czy badanie trzeźwości może być przeprowadzone samodzielnie przez pracodawcę przy pomocy alkomatu, czy też zawsze konieczne jest wzywanie uprawnionego organu. Niewątpliwie za dopuszczalne należy uznać badanie stanu trzeźwości także przez samego pracodawcę, jeśli odbywa się ono za zgodą pracownika. Pracodawca nie może natomiast samodzielnie przeprowadzić badania, jeżeli pracownik nie wyraża na to zgody. Nie można zmusić pracownika, aby poddał się badaniu alkomatem. Takie działanie mogłoby stanowić naruszenie dóbr osobistych pracownika. W takim przypadku pracodawca ma jednak prawo wystąpienia z żądaniem o przeprowadzenie badania przez uprawniony organ. Chodzi o to aby zapobiec sytuacjom, w których brak zgody pracownika na przeprowadzenie badania uniemożliwi pracodawcy dokonanie kontroli jego trzeźwości.

Jeżeli którakolwiek ze stron stosunku pracy sprzeciwia się przeprowadzeniu badania (najczęściej będzie to pracownik), druga strona może żądać przeprowadzenia takiego badania przez uprawniony organ. Jeżeli natomiast istnieje zgoda obu stron na przeprowadzenie badania, badanie może zostać dokonane samodzielnie przez pracodawcę, bez konieczności wzywania uprawnionego organu.

Czy pracodawca może stosować systemy mierzenia czasu pracy zbierające dane biometryczne?

Administrator danych, przetwarzający dane między innymi pracowników, powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Szczególnemu reżimowi prawnemu podlega przetwarzanie danych wrażliwych, a do takich możemy zaliczyć już dane biometryczne, czyli na przykład wizerunek twarzy lub dane daktyloskopijne (art. 9 ogólnego rozporządzenia o ochronie danych). Przetwarzanie danych biometrycznych w takim celu jak rozliczanie czasu pracy nie będzie adekwatne i uprawnione. Czytniki biometryczne mogą być natomiast wprowadzane np. ze względu na ograniczenie dostępu do tajnych informacji lub ze względów bezpieczeństwa, ale nie na potrzeby ewidencji czasu pracy.

Czy pracodawca powinien poinformować pracownika o przekazaniu jego danych do innej instytucji?

Artykuł 7 pkt 6 ustawy o ochronie danych osobowych definiuje pojęcie „odbiorcy danych" jako każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych,
- podmiotu, z którym została zawarta umowa powierzenia,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Nie jest więc odbiorcą danych Zakład Ubezpieczeń Społecznych, urząd skarbowy, policja, czy nawet komornik i o przekazywaniu danych do tego typu instytucji, zgodnie z przepisami bądź z prowadzonym postępowaniem, pracodawca nie ma obowiązku informować pracownika. Co innego jednak w przypadku zawierania umów na dodatkową opiekę medyczną dla pracowników czy przekazywanie danych pracownika do banku. W takich sytuacjach pracownicy muszą otrzymać odpowiednią informację.

Czy przekazując dane osobowe pracowników w ramach umowy powierzenia, pracodawca musi mieć ich zgodę?

Podstawą powierzenia danych osobowych do przetwarzania jest przepis prawa, a nie zgoda osoby, której dane dotyczą. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych (art. 31 ustawy o ochronie danych osobowych). Podmiot, któremu powierzono dane do przetwarzania nie jest odbiorcą danych (art. 7 pkt 6 ustawy o ochronie danych osobowych). Nie można mylić powierzenia przetwarzania danych osobowych z udostępnianiem danych osobowych. Pracodawca zlecając np. firmie zewnętrznej obsługę kadrową, podpisuje z taką firmą odpowiednią umowę, w tym umowę powierzenia przetwarzania danych osobowych. Nie zabiega o zgodę swoich pracowników na taką usługę.

Czy zlecając obsługę kadrową firmie zewnętrznej, należy zawrzeć z nią umowę powierzenia?

Tak, gdyż obowiązek ten wynika z ustawy o ochronie danych osobowych, a prowadzenie dokumentacji księgowej wiąże się nierozerwalnie z przetwarzaniem danych osobowych pracowników. Pracodawca udostępniając dane osobowe pracowników podmiotowi zewnętrznemu w celu prowadzenia obsługi księgowej swojej dokumentacji, ma obowiązek zawrzeć z nim odrębną umowę powierzenia przetwarzania danych osobowych. Często bowiem pracodawca mylnie uważa, że skoro udzielił podmiotowi zewnętrznemu pełnomocnictwa do jego reprezentowania (np. przed urzędem skarbowym i Zakładem Ubezpieczeń Społecznych) we wszystkich sprawach związanych z prowadzeniem księgowości, to pełnomocnictwo to stanowi podstawę powierzenia przetwarzania danych osobowych.

Zgodnie z art. 31 ustawy o ochronie danych osobowych administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Obowiązki i odpowiedzialność podmiotów przetwarzających dane (procesorów) jeszcze bardziej rygorystycznie określa ogólne rozporządzenie o ochronie danych osobowych (rodo).

Na jakich zasadach można przekazywać dane pracowników w ramach grupy kapitałowej?

Jeżeli grupę kapitałową tworzą spółki z Europejskiego Obszaru Gospodarczego (EOG), to przetwarzanie danych jest traktowane tak jak na terenie Polski. Jeżeli natomiast w ramach grupy kapitałowej dane miały by być przekazywane do tzw. państw trzecich, czyli poza EOG, zwłaszcza tych, które nie zapewniają na swoim terytorium odpowiedniego poziomu ochrony danych osobowych (np. USA) może to nastąpić po uzyskaniu zgody Generalnego Inspektora Ochrony Danych Osobowych, wydanej w drodze decyzji administracyjnej.

Zgoda Generalnego Inspektora Ochrony Danych Osobowych nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską lub prawnie wiążące reguły lub polityki ochrony danych osobowych, zwane dalej „wiążącymi regułami korporacyjnymi", które zostały zatwierdzone przez Generalnego Inspektora Ochrony Danych Osobowych.

Generalny Inspektor Ochrony Danych Osobowych zatwierdza, w drodze decyzji administracyjnej, wiążące reguły korporacyjne przyjęte w ramach grupy przedsiębiorców do celów przekazania danych osobowych przez administratora danych do należącego do tej samej grupy innego administratora danych w państwie trzecim (art. 48 ustawy o ochronie danych osobowych).

Czy pracodawca ma prawo w obecności innych pracowników wręczyć osobie zatrudnionej wypowiedzenie umowy o pracę lub nałożyć na nią karę porządkową?

Pracodawca nie może udostępniać danych pracownika osobom przypadkowym, których zakres obowiązków nie uzasadnia dostępu do danych innych pracowników. Udostępnienie informacji o wypowiedzeniu lub karze porządkowej osobom do tego nieupoważnionym może bowiem stanowić naruszenie dóbr osobistych zatrudnionego oraz prawa do ochrony jego danych osobowych. Informacje dotyczące pracowników, w tym dotyczące określonych zdarzeń takich jak wypowiedzenie umowy o pracę lub udzielenie kary porządkowej mogą być dostępne jedynie dla ograniczonego kręgu osób u danego pracodawcy. Do osób takich należą najczęściej osoby zarządzające, w imieniu pracodawcy, zakładem pracy, przełożeni danego pracownika, osoby prowadzące sprawy osobowe, zatrudnienia i płac, radcy prawni świadczący dla pracodawcy pomoc prawną, czy też przedstawiciel związku zawodowego, do którego to związku dany pracownik należy. Osoby te w ramach wykonywanych obowiązków są najczęściej upoważnione do przetwarzania danych.

Czy przetwarzanie przez pracodawcę danych dotyczących nazwiska rodowego matki pracownika jest zgodne z prawem?

Nie, gdyż w świetle przepisów prawa dane te wykraczają poza zakres informacji wymaganych od pracownika. Zakres informacji, jakie może przetwarzać pracodawca od pracownika reguluje art. 22^1 ustawy z 26 czerwca 1974 r. – Kodeks pracy. Z przepisów Kodeksu pracy nie wynika, aby pracodawca mógł pozyskiwać nazwisko rodowe matki pracownika. W związku z powyższym przetwarzanie danych dotyczących nazwiska rodowego matki pracownika nie może być uznane za zgodne z prawem, gdyż wykracza poza zakres danych osobowych wskazany w art. 22^1 § 1 i 2 Kodeksu pracy, a obowiązek ich

podania nie wynika z odrębnych przepisów prawa (cytat Zespołu Rzecznika Prasowego Biura Generalnego Inspektora Ochrony Danych Osobowych).

Czy dział kadr ma prawo przekazać akta osobowe pracownika innej osobie zatrudnionej u danego pracodawcy?

Tak, o ile jest to niezbędne do prawidłowego wykonywania obowiązków służbowych i o ile osoba, której pracodawca udostępnia akta personalne innej osoby u niego zatrudnionej, będzie posiadała nadane przez administratora danych (pracodawcę) upoważnienie do przetwarzania danych osobowych, w tym danych pochodzących z akt pracowniczych.

Zgodnie z ustawą z 29 sierpnia 1997 r. o ochronie danych osobowych, to administrator danych samodzielnie decyduje o dostępie poszczególnych osób u niego zatrudnionych do danych osobowych przez niego przetwarzanych. To bowiem administrator danych jest najlepiej zorientowany w szczegółach prowadzonej przez siebie działalności i dzięki temu najlepiej wie, kogo oraz w jakim zakresie upoważnić do przetwarzania danych osobowych.

Co ważne, dostęp do danych osobowych mogą mieć wyłącznie osoby mające udokumentowane upoważnienie do przetwarzania danych osobowych nadane przez administratora danych. Tak stanowi art. 37 ustawy, który ustanawia zakaz dopuszczania do przetwarzania danych osobowych osób innych, niż mających upoważnienie nadane przez administratora (Zespół Rzecznika Prasowego Biura Generalnego Inspektora Ochrony Danych Osobowych).

Czy pracownik ma prawo wglądu w swoją dokumentację zawierającą jego dane osobowe prowadzoną przez byłego pracodawcę?

Tak, każdy administrator danych (w tym przypadku były pracodawca) ma obowiązek udzielenia informacji osobie, której dane dotyczą, w trybie ustawy o ochronie danych osobowych. Kwestia uprawnienia pracownika do dostępu do dotyczących go danych osobowych uregulowana została w art. 32 ust. 1 pkt 5 ustawy o ochronie danych osobowych.

Zgodnie z wyżej wskazanym przepisem każdej osobie (w tym przypadku pracownikowi) przysługuje prawo do uzyskania informacji o sposobie udostępniania danych, w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane są udostępniane. W świetle przepisu art. 33 ust. 1 ustawy o ochronie danych osobowych, na wniosek osoby, której dane dotyczą, administrator danych (każdy były pracodawca) jest zobowiązany w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić odnośnie jej danych osobowych, informacji o których mowa w art. 32 ust. 1 pkt 1–5a (Zespół Rzecznika Prasowego Biura Generalnego Inspektora Ochrony Danych Osobowych).

Czy pracodawca możne przetwarzać informacje o relacjach rodzinnych i osobistych łączących zatrudnione u niego osoby?

Pracodawca może zbierać dane osobowe tylko w takim zakresie, w jakim jest to konieczne dla osiągnięcia celów zatrudnienia. W przypadku przetwarzania danych osobowych pracowników, celem będzie uzyskanie informacji czy osoba ubiegająca się o stanowisko posiada wymagane kwalifikacje, doświadczenie zawodowe oraz umiejętności. Zbieranie informacji o relacjach rodzinnych i osobistych nie jest uzasadnione charakterem stosunków łączących pracownika z pracodawcą.

Wyjątek może stanowić zakaz podległości służbowej między krewnymi w samorządzie. Zakazy i ograniczenia antykorupcyjne dotyczące pracowników samorządowych zawarte są w ustawie antykorupcyjnej oraz ustawie o pracownikach samorządowych. Ustawa ta zakazuje podległości służbowej między krewnymi i powinowatymi zatrudnionymi u pracodawców samorządowych.

Czy wyniki obowiązkowych badań lekarskich mogą zostać wydane pracodawcy, który na powyższe badania kieruje?

Podstawą do kierowania na badania lekarskie pracowników przez pracodawcę są przepisy ustawy Kodeks pracy, w tym szczególnie art. 229 oraz wydane na jej podstawie rozporządzenie Ministra Zdrowia i Opieki Społecznej z 30 maja 1996 r. w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy (Dz.U. z 1996 r. nr 69, poz. 332). Pracodawca otrzymuje jedynie zaświadczenie o braku przeciwwskazań lub też o przeciwwskazaniach zdrowotnych danego pracownika do pracy na określonym stanowisku. Rozporządzenie nie daje mu tym samym uprawnień do otrzymania wyników badań lekarskich pracownika, tym bardziej, że zgodnie z § 9 ust. 1 pkt 7 rozporządzenia wyniki badań diagnostycznych i (lub) konsultacyjnych zamieszczane są w karcie badania profilaktycznego stanowiącej dokumentację medyczną, którą prowadzi lekarz przeprowadzający badania profilaktyczne.

Jaką odpowiedzialność może ponieść pracownik za naruszenie przepisów o ochronie danych osobowych?

Dane osobowe to cenne aktywa każdej organizacji. Zasady ich ochrony muszą być opisane w polityce bezpieczeństwa. W przypadku naruszenia postanowień polityki bezpieczeństwa informacji pracownik, który dopuścił się takiego naruszenia lub przyczynił do niego (umyślnie lub nieumyślnie) może zostać ukarany zgodnie z obowiązującym regulaminem pracy, obowiązującymi przepisami prawa z zakresu ochrony informacji, a w skrajnych przypadkach pociągnięty do odpowiedzialności karnej.

Umyślne lub nieumyślne naruszenie postanowień polityki bezpieczeństwa informacji lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych. Dane osobowe stanowią też najczęściej tajemnicę przedsiębiorstwa.

Zgodnie natomiast z art. 23 ustawy o zwalczaniu nieuczciwej konkurencji ten, kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega ten, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej. Przestępstwa przeciwko ochronie informacji określa również Rozdział XXXIII Kodeksu karnego.

Za jakie konkretne naruszenia związane z ochroną danych może grozić odpowiedzialność?

Wśród naruszeń związanych z ochroną danych osobowych, za jakie może grozić odpowiedzialność, można wymienić:

- dopuszczenie do nieuprawnionego dostępu lub umożliwienie próby dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
- naruszenie lub próbę naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych);
- naruszenie lub próbę naruszenia integralności systemu, tj. jakakolwiek manipulacja w systemie informatycznym służącym do przetwarzania danych, zarówno zamierzona, jak i przypadkowa;
- zmiana lub utrata danych zapisanych na kopiach zapasowych;
- naruszenie lub próbę naruszenia poufności danych, czyli udostępnienie danych nieupoważnionym lub nieuprawnionym osobom;
- inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy;
- włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

Czy po zakończeniu stosunku pracy należy usunąć dane osobowe pracowników?

Pracodawca powinien przestrzegać kilku zasad, które zapewnią poszanowanie prywatności byłego pracownika. Należy przede wszystkim usunąć adresy e-mailowe i inne dane kontaktowe pracownika

ze strony internetowej pracodawcy po zakończeniu zatrudnienia. Takie same zasady dotyczą danych osobowych stażystów, praktykantów i pracowników tymczasowych.

Dobrą praktyką jest odsyłanie wiadomości przesłanych do usuniętej skrzynki z powrotem do nadawcy, wraz z informacją o kierowaniu korespondencji do nowej osoby. Pracownik ma prawo do informacji o tym, jak długo, przez kogo i w jakim celu jego dane osobowe będą przetwarzane po zakończeniu zatrudnienia. Natomiast zasady przechowywania akt osobowych byłego pracownika określają przepisy sektorowe.

Po jakim czasie należy usuwać dane osobowe pracowników?

Zgodnie z obowiązującymi jeszcze przepisami dokumentację osobową pracownika należy przechowywać przez cały okres zatrudnienia oraz przez 50 lat licząc od dnia zakończenia pracy u danego pracodawcy, a dokumentację płacową 50 lat licząc od dnia jej wytworzenia. Po zakończeniu zatrudnienia pracownika jego akta osobowe należy przekazać z upływem roku kalendarzowego, w którym zakończył się stosunek pracy do archiwum zakładowego. To ma się jednak zmienić. Ogólne rozporządzenie o ochronie danych osobowych (rodo) wymusi także zmiany w Kodeksie pracy.

Proponuje się skrócenie czasu, przez jaki pracodawcy mają przechowywać dane osobowe pracowników, z 50 do 10 lat. W uzasadnionych przypadkach, ze względu na szczególny interes pracownika, w odrębnych przepisach będzie można ustalić dłuższy czas przechowywania dokumentacji, która zawiera dane osobowe pracowników. Przykładem może być sytuacja, w której podczas trwania 10 okresu, zostanie wytoczony proces sądowy, w którym dokumentacja pracownicza będzie dowodem. Dokumenty takie będą wówczas przechowywane do momentu prawomocnego zakończenia postępowania sądowego.

Czy pracodawca ma obowiązek usunąć ze strony internetowej firmy dane osobowe byłego pracownika tj. jego wizerunek, imię i nazwisko oraz adresy jego poczty elektronicznej?

Tak, gdyż ich udostępnienie, ze względu na to, że ustało zatrudnienie, nie znajduje podstawy prawnej i stanowi naruszenie zasady celowości przetwarzania danych osobowych wskazanej w ustawie o ochronie danych osobowych. Skoro pracownik nie reprezentuje już firmy, nie ma celu eksponowania na stronie internetowej jego byłych danych służbowych. Nie dotyczy to oczywiście obowiązku archiwizowania dokumentacji pracowniczej.

Czy można udostępniać dane osobowe byłych pracowników innym podmiotom?

Zarówno dane pracowników, jak i byłych pracowników mogą być udostępniane jedynie podmiotom uprawnionym na podstawie szczególnych przepisów prawa.

Autor:
Piotr Glen

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-6219-6
E-book nr:	2HH0556
Wydawnictwo:	Wydawnictwo Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł