Program
Uczenie się
przez całe życie

Ochrona prywatności w miejscu pracy

Przewodnik dla pracowników

Program
Uczenie się
przez całe życie

Projekt partnerski Leonardo da Vinci – 2012-1-PL1-LEO04-28097 1
"Zwiększanie świadomości w zakresie ochrony danych osobowych
wśród pracowników zatrudnionych w krajach Unii Europejskiej"

Niniejsza publikacja powstała w ramach Projektu Partnerskiego Leonardo da Vinci "Zwiększanie świadomości w zakresie ochrony danych osobowych wśród pracowników zatrudnionych w krajach Unii Europejskiej" (2012-1-PL1-LEO04-28097 1). Projekt ten został sfinansowany przy wsparciu Komisji Europejskiej w ramach programu Uczenie się przez całe życie.

Przewodnik „Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników" stanowi owoc współpracy międzynarodowej pomiędzy ekspertami reprezentującymi cztery organy ochrony danych:

- Biuro Generalnego Inspektora Ochrony Danych Osobowych z Polski
- Biuro Ochrony Danych z Republiki Czeskiej
- Agencja Ochrony Danych Osobowych z Chorwacji
- Komisja Ochrony Danych Osobowych z Republiki Bułgarii.

Niniejsza publikacja odzwierciedla jedynie poglądy autorów. Komisja Europejska nie ponosi odpowiedzialności za wykorzystanie zawartych w niej informacji w jakikolwiek sposób.

Niniejsza publikacja dostępna jest na stronach internetowych partnerskich organów ochrony danych, skąd można pobrać ją dla celów niekomercyjnych.

úřad pro ochranu osobních údajů
the office for personal data protection

azop

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Spis treści

Wstęp

Publikacja "Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników" została przygotowana jako rezultat międzynarodowej współpracy między czterema organami ochrony danych osobowych reprezentującymi Polskę, Republikę Czeską, Chorwację i Bułgarię w ramach programu partnerskiego Leonardo da Vinci „Zwiększanie świadomości w zakresie ochrony danych wśród pracowników zatrudnionych w krajach Unii Europejskiej" (numer umowy 2012-1-PL1-LEO04-28097 1).

Obecnie dane osobowe posiadają dużą wartość ekonomiczną, która może być mierzona w milionach Euro. Zbieranie, analiza oraz przekazywanie danych do innych podmiotów w kraju lub za granicę powoli staje się poważnym biznesem, gdzie głównym produktem są dane osobowe. To mogą być również twoje dane. W związku z tym ważna jest wiedza na temat tego, komu udostępniasz swoje dane osobowe oraz co stanie się z tymi danymi.

W niniejszej publikacji staramy się porównać różne praktyki stosowane w krajach partnerskich uczestniczących w realizacji tego projektu oraz staramy się zidentyfikować ogólne zasady, które są wspólne dla wszystkich lub większości krajów członkowskich Unii Europejskiej w obszarze ochrony danych osobowych, istotne z punktu widzenia osób fizycznych poszukujących pracy lub zatrudnionych w jednym z krajów UE.

Niniejsza publikacja jest skierowana do osób fizycznych poszukujących pracy lub zatrudnionych w sektorze publicznym lub prywatnym. Mając na uwadze fakt, że zatrudnienie w administracji publicznej w każdym kraju podlega specjalnemu reżimowi prawnemu, informacje zawarte w tej publikacji odnoszą się do urzędników administracji publicznej w zakresie, w jakim nie mają zastosowania inne krajowe uregulowania.

Publikacja obejmuje swoim zakresem cały okres zatrudnienia – od momentu poszukiwania pracy, poprzez rozmowy kwalifikacyjne, do podjęcia i zakończenia zatrudnienia. Ponadto omówione zostały kwestie dotyczące np. przetwarzania danych osobowych pracowników przez byłych pracodawców, czy prawa pracowników oraz rola i kompetencje organów ochrony danych osobowych. Znaleźć tu można także krótki słownik, wyjaśniający wybrane pojęcia używane w niniejszej publikacji. Przygotowując przewodnik staraliśmy się skoncentrować na ogólnych zasadach i regułach dotyczących ochrony danych osobowych obowiązujących na europejskim rynku pracy, jednakże staraliśmy się jednocześnie zwrócić uwagę na możliwe różnice występujące pomiędzy poszczególnymi krajami członkowskimi.

Mamy nadzieję, że przewodnik pozwoli ci uzyskać spójny obraz zasad ochrony danych osobowych mających zastosowanie w obszarze zatrudnienia, obowiązków pracodawców i innych zainteresowanych stron, np. agencji zatrudnienia, oraz informacji skierowanych do osób, których dane dotyczą (pracowników, byłych pracowników, osób poszukujących pracy), w zakresie swoich praw i sposobów ich stosowania. Jednocześnie chcielibyśmy, aby publikacja ta była użyteczna dla wszystkich zainteresowanych stron.

1. Poszukiwanie pracy

Pomimo tego, że regulacje prawne z zakresu ochrony danych osobowych przyjęte przez poszczególne państwa członkowskie Unii Europejskiej oparte są na tych samych fundamentalnych zasadach, przepisy te mogą nieco różnić się w każdym z nich. Z tego względu, jeżeli zamierzasz szukać pracy w jednym z krajów UE, warto wcześniej zapoznać się z podstawowymi zasadami dotyczącymi ochrony danych osobowych obowiązującymi w kraju twojego przyszłego pracodawcy. Pamiętaj, że bez względu na to, czy szukasz pracy samodzielnie, czy też korzystasz z usług agencji zatrudnienia, przysługuje ci takie samo prawo do ochrony danych osobowych.

1.1. Dane wymagane od kandydata w toku rekrutacji.

Bez względu na stosowaną metodę poszukiwania pracy, proces ten jest zawsze związany z udostępnianiem danych osobowych różnym podmiotom i instytucjom, do których kandydaci wysyłają swoje dokumenty aplikacyjne (CV, listy motywacyjne). Dlatego też tak ważne jest, aby w toku tego procesu kandydaci udostępniali jedynie te dane, które są niezbędne w procesie rekrutacji. Oznacza to, że dane przekazywane przez nich potencjalnym pracodawcom powinny być istotne oraz adekwatne do osiągnięcia celu, jakim jest podjęcie przez pracodawcę decyzji o zatrudnieniu nowego pracownika. Innymi słowy, pracodawca nie może żądać od kandydata nadmiernych danych, czy też danych, które nie mają znaczenia w toku rekrutacji, a także danych, które zbytnio ingerują w prywatność kandydata (ujawniają o nim więcej informacji niż jest niezbędne), jeżeli kwestie istotne dla pracodawcy można ustalić w sposób mniej inwazyjny.

Jakie dane powinienem zamieścić w CV?

Co do zasady w CV zamieszczane są dane osobowe, które możemy ogólnie określić jako: 1) dane identyfikacyjne (imię, nazwisko, data urodzenia); 2) dane kontaktowe (adres zamieszkania, numer telefonu, adres e-mail) oraz 3) dane o wykształceniu, umiejętnościach, doświadczeniu zawodowym i historii zatrudnienia (ukończonych szkołach oraz studiach, przebytych szkoleniach oraz kursach, poprzednich pracodawcach, zajmowanych stanowiskach oraz obowiązkach zawodowych). Decyzja o tym, jakie konkretnie informacje zamieścisz w swoim CV, należy do ciebie. Niemniej jednak do dobrych praktyk należy unikanie podawania w nim danych zbędnych dla procesu rekrutacji (np. danych o stanie cywilnym, indywidualnych numerach identyfikacyjnych takich jak numer PESEL czy NIP, czy też zainteresowaniach i hobby, które nie mają związku z pracą, o którą się starasz).

Czy są dane, których pracodawca nie może się domagać od kandydata do pracy?

Potencjalny pracodawca nie może żądać od kandydata danych osobowych, dla których pozyskania nie posiada podstawy prawnej (tzn. brak jest przepisów prawnych umożliwiających mu domaganie się podania takich informacji[1]), jak również danych nieadekwatnych lub będących bez związku z celem

1 Osoby poszukujące pracy w Polsce znajdą takie regulacje prawne w art. 22^1 § 1 ustawy z dnia 26 czerwca 1974 r. kodeks pracy (Dz.U. z 1998 Nr 21 poz. 94 z późn. zm.).

przetwarzania, jakim jest podjęcie decyzji o zatrudnieniu pracownika (np. informacji o stanie cywilnym kandydata, posiadanym lub planowanym potomstwie, orientacji seksualnej, poprzednich zarobkach, wyznaniu, przekonaniach, poglądach politycznych).

Co mogę zrobić, jeżeli mam wrażenie, że zakres danych, których wymaga ode mnie pracodawca, jest zbyt szeroki?

Jeżeli potencjalny pracodawca wymaga od ciebie wypełnienia np. formularza dla kandydata do pracy, powinien zawsze poinformować cię, czy uzupełnienie wszystkich pól takiego kwestionariusza jest obligatoryjne, czy też są w nim pola, które wypełniasz opcjonalnie (np. pola obowiązkowe może oznaczyć gwiazdką). W przypadku informacji podawanych obligatoryjnie powinien także wskazać podstawę prawną tego obowiązku. Jeżeli natomiast nie uzyskasz od niego powyższych informacji lub gdy pracodawca nie jest w stanie uzasadnić prawnie swojego żądania, możesz odmówić podania mu takich danych.

Gdzie powinienem szukać informacji o przetwarzaniu danych osobowych kandydatów do pracy przez mojego potencjalnego pracodawcę?

Każdy administrator danych, któremu udostępniasz swoje dane osobowe (np. przedsiębiorstwo, w którym strasz się o pracę, agencja zatrudnienia) jest zobowiązany przekazać ci informacje na temat:

- pełnej nazwy i adresu swojej siedziby,
- celu przetwarzania danych,
- znanych mu w chwili gromadzenia danych odbiorców danych lub ich kategorii,
- prawa dostępu do danych i ich poprawiania,
- dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, podać jego podstawę prawną.

Powyższe informacje powinny zostać podane w sposób jasny, czytelny i łatwo dostępny dla kandydata do pracy (np. w treści oferty pracy lub na stronie internetowej administratora danych).
Prawo do uzyskania takich informacji przysługuje ci także w toku rozmowy kwalifikacyjnej. Zatem, jeżeli masz wątpliwości co do podstawy prawnej, na jakiej twój potencjalny pracodawca domaga się od ciebie konkretnych informacji, nie wahaj się go o nią zapytać.
Jeżeli poszukujesz pracy w jednej z europejskich instytucji lub agencji, informacje, o których mowa powyżej, znajdziesz w oświadczeniu o ochronie prywatności kandydatów do pracy dostępnym na stronie internetowej Europejskiego Urzędu Doboru Kadr (ang. European Personnel Selection Office).

Czy powinienem odpowiadać na dostępne w Internecie oferty pracy, w których znajduje się jedynie adres e-mail, brak jest natomiast informacji o samym pracodawcy?

Nie. Pracodawca, który gromadzi dane kandydatów do pracy (CV, listy motywacyjne, formularze aplikacyjne) jest zobowiązany ujawnić swoją tożsamość.

1.2. Znaczenie zgody na przetwarzanie danych osobowych[2].

Zgoda jest jedną z podstaw prawnych uprawniających administratora danych do przetwarzania informacji o osobie, która taką zgodę wyraziła. Może ona zostać udzielona w formie pisemnej lub ustnej. Obecnie niektórzy pracodawcy wymagają od kandydatów do pracy zamieszczenia w CV zgody na przetwarzanie danych osobowych w celach rekrutacyjnych. Generalnie jednak, jeżeli wysyłasz swoje CV bezpośrednio do pracodawcy w odpowiedzi na określoną ofertę pracy, możesz, ale nie musisz zamieszczać w nim takiej zgody. Wyraźna zgoda na przetwarzanie danych może być niezbędna jedynie w określonych sytuacjach.

W jakich sytuacjach powinienem pomyśleć o zamieszczeniu w moim CV zgody na przetwarzanie danych osobowych w celach rekrutacyjnych?

Dobrze jest zamieścić taką zgodę w CV, jeżeli chcesz, aby pracodawca wykorzystał je w toku kolejnych selekcji nowych pracowników. W przeciwnym przypadku może okazać się, że krajowe przepisy o ochronie danych osobowych zobowiązują go do usunięcia twoich danych z chwilą, gdy stanowisko pracy, na które aplikowałeś zostanie obsadzone. Jeżeli chcesz tego uniknąć, z twojej zgody powinno jasno wynikać, że zgadzasz się na wprowadzenie twoich danych osobowych do bazy danych kandydatów do pracy prowadzonej przez takiego pracodawcę, w celu wykorzystania ich na potrzeby obecnych i przyszłych rekrutacji. Zgoda na przetwarzanie danych osobowych zawartych w twoim CV może okazać się potrzebna także, jeżeli zamierzasz zarejestrować się w bazie danych kandydatów do pracy prowadzonej przez agencję zatrudnienia (w sytuacji gdy przepisy prawa krajowego nie uprawniają agencji do przetwarzania twoich danych w oparciu o inną niż zgoda podstawię prawną). Również w sytuacji, gdy z własnej inicjatywy chcesz ujawnić swojemu potencjalnemu pracodawcy pewne informacje uznawane na mocy przepisów o ochronie danych osobowych za tzw. dane szczególnie chronione[3] (np. dane o stanie zdrowia), niezbędne będzie udzielenie mu wyraźnej zgody na przetwarzanie takich danych osobowych (zakładając, że nie może on tego czynić w oparciu o inną przesłankę). Zwróć jednocześnie uwagę na fakt, że w niektórych krajach UE (np. Polsce) zgoda na przetwarzanie danych szczególnie chronionych musi być wyrażona w formie pisemnej.

Jak powinna wyglądać zgoda na przetwarzanie danych osobowych?

Każda zgoda powinna zawierać w swej treści odpowiedzi na następujące pytania: jakich danych dotyczy, kto jest uprawniony do przetwarzania tych danych i w jakich celach. Warto wiedzieć, że twoja zgoda na przetwarzanie danych może być ograniczona w czasie.

2 Definicję zgody znajdziesz w słowniku.
3 Definicję danych szczególnie chronionych znajdziesz w słowniku.

Przykłady:

"Niniejszym udzielam zgody firmie X na przetwarzanie danych osobowych zawartych w moim CV na potrzeby rekrutacji asystenta kierownika – oferta pracy nr ABCD."

"Niniejszym udzielam zgody firmie X na przetwarzanie moich danych osobowych, w tym danych szczególnie chronionych, znajdujących się w moich dokumentach aplikacyjnych w celach związanych z rekrutacją pracowników, przez rok."

"Niniejszym udzielam zgody firmie X na przetwarzanie danych osobowych zawartych w moim CV w celach związanych naborami pracowników, zarówno obecnymi, jak i organizowanymi w przyszłości."

"Niniejszym wyrażam zgodę aby moje dane osobowe, w zakresie wskazanym powyżej, zostały wprowadzone do bazy danych agencji zatrudnienia X i były przetwarzane przez nią w związku ze świadczeniem mi usług związanych z poszukiwaniem pracy."

Czy mogę wycofać swoją zgodę?

Tak. Możesz wycofać swoją zgodę na przetwarzanie danych osobowych w celach rekrutacyjnych w każdym czasie! Jeżeli zdecydujesz się to uczynić, administrator danych (np. firma, w której ubiegałeś się o pracę) utraci podstawę do dalszego przetwarzania twoich danych w tym celu. W takiej sytuacji twoje dane (np. CV, list motywacyjny) powinny zostać zniszczone, chyba że prawo kraju siedziby administratora danych osobowych stanowi inaczej.

1.3. Cele przetwarzania danych osobowych kandydatów do pracy.

Potencjalny pracodawca powinien przetwarzać dane osobowe kandydatów do pracy jedynie w celu podjęcia decyzji o zatrudnieniu nowego pracownika. Jeżeli cel rekrutacyjny ustał, powinien on usunąć lub zniszczyć takie dane. Nie może wykorzystać danych zawartych w ich CV do celów innych niż rekrutacja, np. w celu prowadzenia wobec kandydatów do pracy marketingu bezpośredniego.

1.4. Poszukiwanie pracy on-line.

Gromadzenie danych przez Internet jest obecnie jedną z najbardziej popularnych form tworzenia baz danych, często wykorzystywaną także w procesie rekrutacji pracowników. Jeżeli potencjalny pracodawca zdecyduje się pozyskiwać dane kandydatów przez Internet (np. poprzez swoją stronę internetową lub na adres e-mail), powinien wdrożyć w celu ich ochrony środki techniczne i organizacyjne, odpowiednie do zagrożeń i kategorii danych objętych ochroną. Obowiązek ten ma zastosowanie także do administratorów danych innych niż pracodawcy, np. agencji zatrudnienia, czy też właścicieli stron internetowych, które umożliwiają zamieszczenie swojego CV on-line. Każdy bowiem administrator danych, bez względu na sposób ich gromadzenia, musi działać zgodnie z przepisami o ochronie danych osobowych.

Z jakich stron internetowych powinienem korzystać w celu przekazania danych?

Najważniejsze to zawsze korzystać wyłącznie ze sprawdzonych i zaufanych stron internetowych. Pamiętaj, że twoje CV ujawnia o tobie wiele informacji, które nie powinny trafić do osób niepowołanych. Zawsze zatem sprawdzaj, czy strona internetowa lub adres e-mail, z których zamierzasz skorzystać, są oficjalnie rekomendowane przez podmiot, któremu za ich pośrednictwem chcesz przesłać swoje dane. Pamiętaj też, aby upewnić się, kto jest administratorem danych oraz że używana przez ciebie strona internetowa zapewnia szyfrowany transfer danych (szukaj ciągu „https" w adresie strony internetowej w twojej przeglądarce).

O czym powinienem pomyśleć przed zamieszczeniem swojego CV na stronie internetowej?

Oto cztery podstawowe zasady postępowania w takiej sytuacji:

1. Pamiętaj, że umieszczenie CV w serwisie internetowym może wymagać założenia konta użytkownika serwisu oraz wyrażenia jego właścicielowi zgody na przetwarzanie danych osobowych. Zanim to uczynisz dokładnie przeczytaj regulamin oraz politykę prywatności serwisu[4]. Może bowiem okazać się, że właściciel serwisu chce przetwarzać twoje dane także w celach marketingowych nie tylko własnych produktów, ale też produktów innych podmiotów.
2. Zamieść w CV tylko takie dane, które są istotne i niezbędne w procesie rekrutacji.
3. Miej na uwadze, że zamieszczając swoje CV w Internecie umożliwiasz wgląd w znajdujące się w nim dane nieograniczonej liczbie użytkowników. Mogą one zostać wykorzystane w sposób nie koniecznie zgodny z twoimi oczekiwaniami (kradzież tożsamości, spam, marketing telefoniczny). Pamiętaj, że nawet jeśli usuniesz swoje CV ze strony internetowej, będzie ono nadal dostępne w archiwach wyszukiwarek internetowych. Warto zatem szukać stron, które umożliwiają zamieszczenie CV w formie anonimowej (bez podawania danych identyfikacyjnych i kontaktowych) – możesz wtedy wybrać pracodawcę, którego ofertą pracy jesteś zainteresowany i tylko jemu udostępnić swoje szczegółowe dane.
4. Zawsze sprawdzaj, jakie są domyślne ustawienia prywatności na stronie internetowej, poprzez którą szukasz pracy. Wiele z nich umożliwia swoim użytkownikom ich indywidualne dostosowanie.

1.5. Agencje zatrudnienia.

Jeżeli obawiasz się samodzielnie szukać pracy w innym państwie UE, możesz skorzystać z pomocy agencji zatrudnienia. Podmioty te świadczą usługi w zakresie: doradztwa zawodowego, pośrednictwa pracy oraz pracy tymczasowej. Tym samym należy uznać je jako jeden z kanałów poszukiwania pracy. Oznacza to, że agencje zatrudnienia mogą zbierać i przetwarzać dane osobowe kandydatów do pracy także jako odrębni administratorzy danych.

4 Regulamin strony zawiera w szczególności postanowienia w zakresie świadczonych w jej ramach usług, jak również określa prawa i obowiązki użytkowników i usługodawcy. Większość ze stron posiada także tzw. "politykę prywatności", czyli dokument określający zasady przetwarzania i ochrony danych osobowych jej użytkowników.

Jakie dane osobowe kandydatów może gromadzić agencja zatrudnienia?

Generalnie agencja zatrudnienia może gromadzić w celach rekrutacyjnych taki sam zakres danych osobowych kandydatów do pracy jak potencjalny pracodawca. Jednocześnie, jak każdy administrator danych, agencja powinna zapewnić, aby dane te były niezbędne i adekwatne do celu ich przetwarzania.

Czy powinienem udzielić agencji zatrudnienia zgody na przetwarzanie danych osobowych?

Tak, jeżeli agencja nie posiada innych podstaw prawnych do przetwarzania twoich danych osobowych (np. w kraju, w którym mieści się jej siedziba brak jest szczegółowych regulacji prawnych w zakresie przetwarzania przez tego typu podmioty danych osobowych kandydatów do pracy). Zgoda ta może być przez ciebie wycofana w każdym czasie![5]

W jakim celu agencja zatrudnienia może wykorzystywać moje dane osobowe?

Agencja zatrudnienia może przetwarzać twoje dane osobowe w celu związanym z realizacją świadczonych ci usług (np. w zakresie poradnictwa zawodowego, szkoleń, pośrednictwa pracy).

Czy agencja zatrudnienia może przekazać moje dane osobowe do potencjalnych pracodawców?

Udostępnienie danych do innych podmiotów mieści się w pojęciu przetwarzania danych osobowych. Z tego względu agencja zatrudnienia może przekazać twoje dane potencjalnemu pracodawcy jedynie w sytuacji gdy posiada podstawę prawną do takiego działania (np. posiada twoją uprzednią zgodę na udostępnienie danych). Agencja zatrudnienia, której przekazujesz swoje dane osobowe, powinna poinformować cię o odbiorcach twoich danych, lub przynajmniej ich kategoriach, którzy są jej znani w chwili pozyskiwania danych[6].

5 Więcej informacji na temat zgody na przetwarzanie danych oraz jej przykłady znajdziesz w Rozdziale 1.2.

6 Przeczytaj także: "Gdzie powinienem szukać informacji o przetwarzaniu danych osobowych kandydatów do pracy przez mojego potencjalnego pracodawcę?".

Zalecenia

1. Unikaj umieszczania w swoim CV danych zbędnych w procesie rekrutacji.
2. Pamiętaj, że masz prawo odmówić podania potencjalnemu pracodawcy żądanych przez niego danych, jeżeli brak jest przepisów prawnych zobowiązujących cię do ich ujawnienia.
3. Udziel wyraźnej zgody na przetwarzanie danych jeżeli: 1) chcesz, aby twoje dane były przetwarzane w ramach przyszłych rekrutacji, 2) korzystasz z usług agencji zatrudnienia, 3) z własnej inicjatywy ujawniasz potencjalnemu pracodawcy dane szczególnie chronione.
4. Pamiętaj, że w każdym czasie możesz wycofać swoją zgodę na przetwarzanie danych osobowych!
5. Upewnij się, że posiadasz pełne informacje o sposobie i celach przetwarzania danych przez określony podmiot, zanim udostępnisz mu swoje dane osobowe.
6. Szukając pracy poprzez Internet, korzystaj wyłącznie ze sprawdzonych i zaufanych stron internetowych.
7. Pomyśl o bezpieczeństwie swoich danych zanim zamieścisz CV w Internecie – CV wprowadzone raz do Internetu będzie w nim dostępne, nawet jeżeli usuniesz je ze strony internetowej, na której zostało pierwotnie zamieszczone!

2. Proces rekrutacyjny

W toku rekrutacji twój potencjalny pracodawca może zechcieć spotkać się z tobą osobiście, aby zweryfikować twoje doświadczenie zawodowe, a także sprawdzić, czy jesteś właściwą osobą na stanowisko pracy, które oferuje (np. podczas rozmowy kwalifikacyjnej, testu psychologicznego lub testu wiedzy i umiejętności). W trakcie tego procesu także dochodzi do gromadzenia twoich danych osobowych.

Jakie dane kandydata mogą być gromadzone w trakcie rozmowy kwalifikacyjnej?

Podczas rozmowy kwalifikacyjnej pracodawca może zadawać ci szczegółowe pytania w zakresie informacji, które podałeś w swoim CV. Powinny one zawsze odnosić się do kwestii związanych z pracą na stanowisku, na które aplikujesz. Każdy z kandydatów do pracy ma prawo do równego traktowania bez względu na płeć, wiek, przekonania, wyznanie czy też jakiekolwiek cechy osobiste. Pamiętaj, że zawsze masz prawo do odmowy udzielenia odpowiedzi na pytanie, które cię zawstydza lub narusza twoje prawo do prywatności czy też godność osobistą (np. dotyczące twojego wyznania, przekonań politycznych, stanu cywilnego, życia prywatnego, orientacji seksualnej, rodzicielstwa i planowanego potomstwa).
W pewnych sytuacjach pracodawca może być jednak uprawniony do zadania ci niedyskretnego pytania (np. w Polsce kobiety mogą spotkać się z pytaniem o ciążę, jeżeli praca, o którą się ubiegają jest niedozwolona dla kobiet w ciąży z uwagi na ochronę macierzyństwa, natomiast osoby starające się o pozycję nauczyciela w szkole publicznej mogą zostać zapytane o to, czy były karane za przestępstwo popełnione umyślnie). Obowiązek udzielenia odpowiedzi na takie pytanie powinien wynikać bezpośrednio z przepisów prawnych.

Czy potencjalny pracodawca może skontaktować się z moim poprzednim pracodawcą w celu uzyskania informacji na mój temat?

Niektórzy pracodawcy mogą chcieć pozyskać informacje o kandydacie do pracy bezpośrednio z miejsca jego poprzedniego zatrudnienia. Nie powinno jednak dochodzić do tego bez zgody kandydata. Jeżeli potencjalny pracodawca chce uzyskać opinię o tobie jako pracowniku, może poprosić cię o referencje. Może również wykorzystać informacje zawarte w twoim świadectwie pracy.

Co powinienem wiedzieć na temat testów psychologicznych?

Testy psychologiczne są metodą oceny kandydata wykorzystywaną przez pracodawców w celu wyróżnienia osób odpowiadających wymaganiom stawianym na określonym stanowisku pracy. Tego typu testy umożliwiają także uzyskanie przez pracodawcę informacji o kandydacie, których on sam dobrowolnie nie chciałby ujawniać lub starałby się ukryć. Z tego względu wykorzystanie testów psychologicznych w procesie rekrutacyjnym budzi wiele kontrowersji, gdyż niektóre testy mogą ujawniać nie tylko informacje o cechach kandydatów pożądanych na danym stanowisku pracy, lecz także informacje osobiste, do których pracodawca nie powinien mieć dostępu. Mogą na przykład zdradzać informacje o jego stanie zdrowia, poglądach, życiu prywatnym oraz inne dane. Z tego właśnie powodu powinny być przeprowadzane w sposób profesjonalny przez psychologa zobowiązanego do zachowania tajemnicy zawodowej. Powinieneś zostać również dokładnie poinformowany o celu takich testów, zakresie

informacji, które zostaną na jego podstawie pozyskane oraz osobach, które będą miały wgląd w jego wyniki. Dopuszczalność stosowania testów psychologicznych w procesie rekrutacji jest traktowana w różny sposób w poszczególnych państwach członkowskich. W niektórych z nich musi ona wynikać wprost z przepisów prawa. W innych niezbędna jest zgoda kandydata, który powinien zostać jednocześnie poinformowany o możliwości odmowy udziału w teście.

Sprawdzanie kandydata w Internecie - na czym to polega?

Internet i portale społecznościowe stanowią dużą pokusę dla pracodawców jako dodatkowe źródło danych o ich potencjalnych pracownikach, o które nie mogliby oficjalnie zapytać w toku rekrutacji. Miej na uwadze, że nawet w sytuacji, gdy potencjalny pracodawca oficjalnie nie może korzystać z informacji pozyskanych dzięki przeglądaniu twoich profili internetowych, czy też śledzeniu twoich wpisów na forach, informacje te mogą mieć realny wpływ na jego decyzję o twoim zatrudnieniu. Warto zatem wiedzieć, że możesz w pewien sposób oddziaływać na to, jakie dane na twój temat będą dostępne w Internecie. Dla przykładu można wskazać, że wyszukiwarki internetowe zazwyczaj zapewniają ci możliwość usunięcia niepożądanych informacji na swój temat z wyników wyszukiwania. Najważniejsze jednak jest, abyś dobrze się zastanowił zanim opublikujesz osobiste informacje w sieci. Pamiętaj, że sposób, w jaki chronisz swoją prywatność w Internecie, zależy od ciebie.

Co stanie się z moimi danymi, jeżeli nie zostanę zatrudniony?

Administrator danych nie może ich przetwarzać dłużej niż jest to niezbędne dla osiągnięcia celu przetwarzania. Zatem po zakończeniu rekrutacji powinien on niezwłocznie usunąć dane kandydatów do pracy, którzy zostali przez niego odrzuceni (niezależnie od tego, czy zostali oni zaproszeni na rozmowę kwalifikacyjną, czy nie). Wyjątek stanowi sytuacja, gdy kandydat udzielił wyraźnej zgody na przetwarzanie jego danych w przyszłych procesach rekrutacyjnych. W oparciu o taką zgodę pracodawca może korzystać z danych kandydata w każdym przypadku, gdy prowadzi rekrutację na stanowisko odpowiadające jego kwalifikacjom zawodowym.

Zalecenia:

1. Pamiętaj, że pytania zadawane ci w toku rekrutacji powinny odnosić się jedynie do kwestii związanych z zatrudnieniem na stanowisku, na które aplikujesz. Zawsze możesz odmówić odpowiedzi na pytanie, które zawstydza cię lub narusza twoją godność osobistą.
2. Zanim przystąpisz do testu psychologicznego upewnij się, że prawo krajowe państwa członkowskiego dopuszcza jego przeprowadzenie w procesie rekrutacyjnym. Możesz odmówić udziału w takim teście.
3. Miej świadomość, że dane na twój temat, które udostępniasz w Internecie, mogą mieć wpływ na twoje zatrudnienie.

3. Okres zatrudnienia

W ramach stosunku pracy istnieje nieunikniona potrzeba wymiany informacji, nie zawsze o charakterze zawodowym. Potrzeba ta czasami wynika z przepisów krajowego prawa pracy, czasami zaś ze specyfiki działalności zawodowej i interesów twojego pracodawcy. Fakt, czy jest ona zgodna z prawem, należy oceniać w każdym konkretnym przypadku. Ochrona twojej prywatności w okresie zatrudnienia nie jest absolutna. Wręcz przeciwnie, przetwarzanie twoich danych osobowych nie zawsze zależy od twojej zgody.

Prawo pracy zawiera względnie niewiele przepisów określających granice kontroli sprawowanej przez pracodawcę oraz przypadki, gdy granica twojej prywatności zostaje przekroczona. Dobrą praktyką, jaką powinni stosować pracodawcy, jest wdrożenie polityki prywatności, która powinna być przejrzysta i cały czas dostępna dla pracowników. Polityka ta powinna określać: rodzaje danych osobowych pracowników, które są gromadzone i dalej przetwarzane; cele tego przetwarzania; osoby (w tym pracowników), które posiadają prawo dostępu do nich; informacje na temat tego, czy podanie danych jest dobrowolne czy obowiązkowe, oraz jakie są konsekwencje w przypadku odmowy; okres przechowywania; metody usunięcia danych po upłynięciu okresu przechowywania; prawa pracowników w sferze ochrony danych; możliwe operacje przekazania danych do innych krajów oraz informację, dlaczego jest to konieczne; dane kontaktowe urzędnika ds. ochrony danych (jeżeli taki istnieje).

3.1. Konkretne kwestie związane z przetwarzaniem danych w okresie zatrudnienia.

Wraz z powstaniem stosunku pracy powstają określone prawa i obowiązki pracodawcy i pracownika. Ich realizacja rozpoczyna się wraz z zawarciem umowy o pracę i może obejmować przetwarzanie danych osobowych pracownika.

3.1.1. Zawarcie umowy o pracę i akta osobowe pracownika.

Zawarcie umowy o pracę oznacza utworzenie akt osobowych pracownika, które zawierają dokumenty potrzebne do zawarcia i realizacji umowy. Niektóre z nich przedkładasz ty, inne są wydawane przez pracodawcę. Niektóre z nich zawierają twoje dane osobowe, na przykład kserokopia paszportu lub innego dokumentu tożsamości czy też świadectwo szkolne.

Konkretne informacje, które zawierają akta osobowe pracownika, określone są we właściwym ustawodawstwie krajowym.

Czy pracodawcy mogą wykonać kserokopię mojego dokumentu tożsamości, gdy mnie zatrudniają?

Zależy to od właściwego ustawodawstwa krajowego pracodawcy. Zazwyczaj nie istnieje prawnie uzasadniona potrzeba, aby pracodawca wykonał kserokopię twojego dokumentu tożsamości, ponieważ twój dokument tożsamości zawiera niektóre informacje nie związane z wykonywaniem twojej pracy. Posiadasz prawo wyrażenia sprzeciwu przeciwko kopiowaniu twojego dokumentu tożsamości, chyba że pracodawca jest w stanie udowodnić istnienie podstaw prawnych dotyczących konkretnego przypadku.

Czy przechowywanie informacji związanych z moim życiem osobistym w moich aktach osobowych jest konieczne?

Mogą mieć miejsce sytuacje, że twoje akta osobowe będą zawierać tylko informacje związane ze stosunkiem pracy. Jednakże mogą one zawierać również dane związane z twoim życiem osobistym. Zazwyczaj musisz podać te dane w celu realizacji określonych praw lub umożliwienia pracodawcy wykonania określonych zobowiązań. Przykładem może być urlop w związku z realizacją zobowiązań cywilnych, publicznych lub innych (zawarcie małżeństwa, oddanie krwi, śmierć krewnego, wezwanie do sądu, itp.).

Jaki jest okres przechowywania moich danych osobowych przez pracodawcę?

Pracodawca może przechowywać twoje dane osobowe tylko przez okres przewidziany przez ustawodawstwo krajowe (np. zgodnie z polskim prawem akta osobowe pracownika powinny być przechowywane przez okres zatrudnienia oraz przez 50 lat od daty zakończenia stosunku pracy, zaś lista płac – przez 50 lat od daty jej sporządzenia). Po upłynięciu tego okresu pracodawca zobowiązany jest do usunięcia twoich danych osobowych.

3.1.2. Ujawnianie i dostęp do danych osobowych w kontekście zatrudnienia.

Twoje dane osobowe są poufne i nie mogą być ujawniane i udostępniane bez wyraźnej zgody lub podstawy prawnej. Twoje dane mogą być udostępniane dwóm grupom ludzi: pracownikom pracującym na rzecz pracodawcy, których wyraźnie upoważniono do dostępu do takich danych oraz podmiotom zewnętrznym w przypadku istnienia podstawy prawnej takiego udostępnienia.

Kto ma dostęp do moich akt osobowych w ramach organizacji, która mnie zatrudnia?

Dostęp do twoich danych w ramach organizacji, dla której pracujesz, mogą mieć pracownicy, których obowiązki zawodowe wymagają przetwarzania danych i są należycie upoważnieni przez twojego pracodawcę (na przykład pracownik o długim stażu, działy personalne, działy finansowe, etc).

Jakie podmioty zewnętrzne mogą mieć dostęp do moich danych osobowych?

Pracodawca jest zobowiązany do nieudostępniania informacji dotyczących pracownika stronom trzecim. Dostęp może być zapewniony tylko wówczas, gdy pracodawca jest zobowiązany prawem do przekazania danych właściwym organom publicznym lub o takie dane odpowiednio zwróciły się właściwe organy (na przykład w przypadku audytów finansowych czy inspekcji pracy); gdy udzieliłeś wyraźnej zgody na udostępnienie twoich danych osobowych konkretnej stronie trzeciej; lub we wszelkich innych sytuacjach przewidzianych w ustawodawstwie krajowym (na przykład w sprawie sądowej w celu ochrony praw i interesów pracodawcy).

3.1.3. Transgraniczne przekazywanie danych osobowych.

W obecnym zglobalizowanym świecie, w których jesteśmy świadkami zwiększonej wymiany informacji i zasobów ludzkich, przekazywanie twoich danych osobowych do innych krajów jest coraz częściej konieczne. Powody takiego przekazywania mogą być różne. Przekazanie danych zazwyczaj jest prowadzone w ramach przedsiębiorstw międzynarodowych (między siedzibą główną i filiami zależnymi) w celu

globalizacji określonego zakresu i rodzaju przetwarzania danych lub na mocy umowy outsourcingowej.

Czy przekazywanie danych w ramach Unii Europejskiej wymaga zgody organu ochrony danych?

Nie. Przekazywanie danych od pracownika do innego podmiotu (innej filii prywatnego przedsiębiorstwa, organu państwowego, etc.) w Unii Europejskiej i Europejskim Obszarze Gospodarczym jest swobodne i nie jest potrzebna zgoda krajowego organu ochrony danych. Przekazanie danych do kraju trzeciego[7] może w niektórych sytuacjach wymagać zgody właściwego organu ochrony danych.

Czy moja zgoda na przekazanie danych osobowych jest zawsze potrzebna?

Nie. Mogą mieć zastosowanie inne podstawy prawne przekazania, np. gdy pracodawca musi wypełnić zobowiązania wynikające z prawa pracy lub posiada inny tytuł prawny do celów zarządzania zasobami ludzkimi, gdy przetwarzanie jest konieczne do realizacji umowy między pracodawcą a pracownikiem, również w przypadkach, gdy istnieje konieczność prowadzenia dochodzeń w sprawie przestępstw, etc. Jednak jeżeli chodzi o przekazanie danych pracowników do kraju trzeciego, pracodawca jest zobowiązany do posiadania podstawy prawnej nie tylko do przekazania ogólnie, ale również do przekazania tych danych do podmiotu z siedzibą w kraju trzecim. Zaleca się, abyś przed realizacją operacji przekazania danych został o tym powiadomiony.

Jakie informacje dotyczące przekazania moich danych osobowych powinienem otrzymać?

Dobrą praktyką jest, aby informować osoby przed przekazaniem ich danych, o zakresie i rodzaju danych, które mają być przekazane, celach tego przekazania, odbiorcach danych oraz ich prawach dotyczących ochrony danych, w tym prawie do wyrażenia sprzeciwu wobec przetwarzania nieprawidłowo zgromadzonych danych ich dotyczących oraz prawie do zwrócenia się o ich usunięcie. Informacje te powinny obejmować odniesienie do poziomu ochrony danych w kraju przeznaczenia, jeżeli dane będą przekazane do kraju trzeciego.

Kiedy dozwolone jest przekazywanie danych szczególnie chronionych?

Tak zwane „dane szczególnie chronione" (wrażliwe) mogą być przekazane w przypadku, gdy istnieje potrzeba realizacji określonych praw i obowiązków pracodawcy lub w przypadku wyraźnej zgody właściwych pracowników. Pracodawca musi cię poinformować o przekazywaniu tych danych.

3.2. Prawo dostępu do informacji vs. prawo do ochrony danych osobowych.

Prawo do ochrony danych osobowych nie jest prawem absolutnym[8], a zatem istnieją wyłączenia odnoszące się jego stosowania, które zawsze muszą być określone prawem. Na przykład w przypadku, gdy zajmujesz stanowisko urzędnika publicznego, dopuszczalne jest upublicznienie niektórych twoich danych w związku z prawem dostępu do informacji publicznych innych osób. W takich sytuacjach na-

7 Kraj trzeci – kraj niebędący członkiem Unii Europejskiej ani Europejskiego Obszaru Gospodarczego.

8 Prawa absolutne mają zastosowanie do wszystkich podmiotów i nie podlegają żadnym ograniczeniom.

leży zachować równowagę miedzy ochroną danych a prawem do informacji przy zachowaniu zasady proporcjonalności[9].

Czy dane osobowe wszystkich pracowników są na równi chronione?

Poziom ochrony prywatności osób sprawujących funkcje publiczne jest niższy. Wobec tych osób mają zastosowanie zasady przejrzystości i rozliczalności, które nie mają zastosowania do innych osób. Przykładem niższego poziomu ochrony danych osobowych dotyczących niektórych z tych osób jest ich obowiązek do złożenia publicznej deklaracji na temat ich dochodu, posiadanych nieruchomości, majątku, oszczędności lub innych danych chronionych w celu zapobieżenia konfliktowi interesów.

Czy moja zgoda na ujawnienie danych osobowych jest konieczna w przypadku, gdy wniosek o dostęp oparty jest na właściwej ustawie o dostępie do informacji publicznej?

Ustawodawstwa europejskie nie zapewniają wyraźnej odpowiedzi na to pytanie.
Ustawodawstwo w niektórych państwach (np. w Bułgarii) przewiduje, że jeżeli dane informacje należą jednocześnie do kategorii informacji publicznych i danych osobowych, twoja zgoda jest konieczna. W przypadku sprzeciwu informacje muszą być udostępnione w sposób nie umożliwiający ujawnienia twoich danych osobowych.
W innych krajach (np. w Republice Czeskiej) zgoda nie zawsze jest potrzebna, szczególnie gdy dane osobowe należą do osób dobrze znanych społeczeństwu i ujawniają informacje na temat ich działalności publicznej lub oficjalnej.

W jakich przypadkach moje dane osobowe są dostępne?

W przypadku, gdy jesteś osobą sprawującą funkcje publiczne, twoja zgoda nie jest konieczna do ujawnienia danych osobowych. Przykładem są tu:

- Dane dotyczące twojego stanowiska w organizacji – takie informacje, mimo że cię dotyczą, odnoszą się do ciebie w twojej roli osoby piastującej stanowisko w organizacji;
- Dane dotyczące liczby, celów i długości twoich podróży służbowych – są to dane związane z wykonywaniem obowiązków służbowych;
- Dane dotyczące członków komisji w organie publicznym – informacje te nie obejmują danych identyfikacyjnych związanych z życiem prywatnym osób, których dane dotyczą, ale jedynie ujawniają kwestie dotyczące ich pracy;
- Informacje dotyczące podanych w deklaracji informacji dotyczących nieruchomości i dochodu – urzędnicy wysokiego szczebla mają prawny obowiązek corocznego składania deklaracji na temat ich nieruchomości i dochodu, co stanowi środek antykorupcyjny;
- Informacje na temat wykształcenia i kwalifikacji urzędników wysokiego szczebla oraz wszelkie inne informacje, które są warunkiem wstępnym objęcia publicznego stanowiska – dla przykładu są to ministrowie, zastępcy ministrów, sekretarze generalni, członkowie gabinetów politycznych ministrów, członkowie samorządu lokalnego. Informacje te są potrzebne do sformułowania opi-

9 Zasada proporcjonalności oznacza równowagę między dwoma konkurującymi ze sobą prawami, gdy żadne z nich nie jest nadrzędne.

nii na temat tego, czy dany członek gabinetu politycznego posiada niezbędne wykształcenie i kwalifikacje zawodowe do skutecznego wdrożenia określonej polityki.

- Wszelkie inne informacje związane ze stanowiskiem publicznym i związanymi z nim obowiązkami lub z wydawaniem pieniędzy publicznych.

3.3. Udostępnienie informacji opinii publicznej w celu poprawy wizerunku zawodowego i instytucjonalnego.

W ramach codziennej pracy pracodawcy publiczni i prywatni upubliczniają określoną ilość informacji o sobie i o tobie. Jest to normalny proces udostępniania informacji w celu zapewnienia przejrzystości w relacjach z konsumentami/klientami i podniesienia świadomości na temat funkcjonowania danego organu publicznego lub prywatnego przedsiębiorstwa. Ogólnie akceptowany jest fakt, że publikowane przez pracodawcę (na przykład na stronie przedsiębiorstwa) informacje na temat kierownictwa czy pracowników dotyczą ich w ich oficjalnym charakterze. Dobrą praktyką jest na przykład publikowanie danych kontaktowych (służbowego adresu e-mail i numeru telefonu) określonych pracowników w celu ułatwienia kontaktu zewnętrznym użytkownikom z danym organem publicznym/prywatnym przedsiębiorstwem.
Publikowanie zdjęć w przypadku wydarzeń związanych z pracą (np. konferencji) jest częścią wizerunku korporacyjnego lub instytucyjnego danej organizacji. W przypadku osób sprawujących wysokie funkcje publiczne oczekuje się przejrzystości, na przykład publikowania curriculum vitae takich osób na stronie internetowej instytucji.
Konieczność ujawnienia dotyczących ciebie informacji może wynikać nie tylko z oczekiwań co do zapewnienia przejrzystości, ale również z przepisu prawa. Na przykład ustawodawstwo bułgarskie wymaga publikowania na stronach internetowych organów publicznych listy nazwisk pracowników, którzy wypełnili deklaracje zgodnie z ustawą o zapobieganiu konfliktowi interesów.
Wszystkie te przykłady ujawniania informacji wiążą się z oficjalnymi funkcjami pracowników i nie stanowią naruszenia ich prywatności, ponieważ są nierozerwalnie związane z wykonywaniem ich obowiązków zawodowych.

3.4. Dane szczególnie chronione, które pracodawca powinien przetwarzać / których pracodawca nie powinien przetwarzać.

Europejskie ustawodawstwo w zakresie ochrony danych generalnie zakazuje przetwarzania danych osobowych obejmujących informacje na temat rasy, wyznania, przekonań politycznych lub filozoficznych, przynależności związkowej, życia seksualnego lub orientacji seksualnej oraz stanu zdrowia. Pracodawca ma prawo przetwarzać takie dane tylko wówczas, gdy jest to wymagane do realizacji określonych praw i obowiązków w zakresie prawa pracy, które są wyraźnie wskazane w prawie. Innym tytułem prawnym, który w niektórych konkretnych przypadkach pozwala na przetwarzanie takich danych może być twoja zgoda.
W celu realizacji określonych przywilejów powinieneś podać pracodawcy określone dane szczególnie chronione. Przykładami są:

- dodatkowy urlop na działalność związkową;
- uzyskanie zwolnienia od pracy w określonych dniach świąt religijnych, jeżeli dana religia nie jest oficjalną religią w danym państwie;
- pracodawca jest zobowiązany zwolnić z obowiązku świadczenia pracy pracownice, które są w ciąży lub na zaawansowanych etapach leczenia in vitro i muszą zostać poddane badaniom lekarskim (np. w Bułgarii).

Prawo pracy przewiduje różne prawa do szczególnej ochrony i integracji dla osób niepełnosprawnych. Jeżeli jesteś osobą niepełnosprawną, w twoim interesie leży przedłożenie dokumentów potwierdzających twój stan zdrowia w celu realizacji praw, które musi zapewnić pracodawca.

Czy konieczne jest, aby mój pracodawca otrzymał informacje na temat mojego stanu zdrowia?

Pracodawca ma prawo do zapoznania się z ogólnymi informacjami na temat twojego stanu zdrowia, gdy jest to konieczne w celu wypełnienia zobowiązań w zakresie bezpieczeństwa pracy oraz przestrzegania prawa pracy i prawa ubezpieczeniowego. Pracodawca i każdy, kto przetwarza informacje na temat stanu zdrowia, jest zobowiązany do zapewnienia odpowiednich środków ochrony[10] danych osobowych przed nieuprawnionym dostępem i niewłaściwym wykorzystaniem.

Do przedstawienia jakich dokumentów związanych z ubezpieczeniem społecznym i ubezpieczeniem zdrowotnym, zawierających informacje na temat stanu zdrowia, jestem zobowiązany w celu uzyskania wynagrodzenia?

Nieobecność z powodu przejściowej niezdolności do pracy jest weryfikowana w oparciu o zaświadczenie wydane i potwierdzone przez właściwe organy, zawierające dane na temat twojego stanu zdrowia. Takie zaświadczenie przedstawiane jest pracodawcy w przypadku, gdy jesteś nieobecny z powodu choroby, w celu otrzymania wynagrodzenia.

3.5. Wykorzystanie wewnętrznych zasobów telekomunikacyjnych.

Weź pod uwagę fakt, że powinieneś korzystać z wewnętrznych zasobów korporacyjnych zgodnie z wewnętrznymi zasadami przyjętymi przez pracodawcę. Twój pracodawca ma prawo sprawdzić, w odpowiedni sposób, czy spełniasz ten wymóg. Mimo to twój pracodawca nie ma prawa do naruszenia twojej prywatności w miejscu pracy (na przykład poprzez monitorowanie rozmów telefonicznych, śledzenie korespondencji e-mail czy sprawdzanie przesyłek adresowanych do ciebie) bez poważnego powodu związanego z charakterem twojej pracy.

3.5.1. Monitorowanie korzystania z Internetu oraz poczty elektronicznej.

Obecnie korzystanie z Internetu i poczty elektronicznej stało się nieodłączną częścią obowiązków służbowych. Ważne jest, aby znać granicę między prywatnością a wypełnianiem obowiązków służbowych.

Czy mój adres e-mail może być uważany za dane osobowe?

Nie ma jednolitej praktyki europejskiej w tej kwestii. W większości przypadków ogólnie uznane jest, że adresy e-mail stanowią dane osobowe, jeżeli zawierają informacje, które są lub mogłyby być powiązane z osobą, np. Jan.Kowalski@giodo.gov.pl. W Bułgarii adresy e-mail uważane są za dane osobowe tylko

10 Odpowiednie środki zależą od ustawodawstwa krajowego.

w połączeniu z innymi danymi osobowymi identyfikującymi określoną osobę.

Czy monitorowanie mojej służbowej poczty elektronicznej oraz dostępu do Internetu prowadzone w imieniu pracodawcy stanowi przetwarzanie danych osobowych?

Monitorowanie poczty elektronicznej i wykorzystania Internetu prowadzone w imieniu pracodawcy bez wątpienia oznacza przetwarzanie danych osobowych. Ochrona danych i prywatności nie kończy się na granicy miejsca pracy. Korespondencja e-mail i komunikacja elektroniczna korzystają z takiej samej ochrony praw podstawowych jak poczta papierowa. W trakcie twojego życia zawodowego rozwijasz kontakty ze światem zewnętrznym. Trudno jest wyraźnie rozróżnić, które działania stanowią cześć twojego życia zawodowego czy biznesowego, a które – twojego życia prywatnego. Z tego powodu uznane jest, że monitorowanie poczty e-mail i dostępu do Internetu w miejscu pracy rzeczywiście stanowi przetwarzanie danych osobowych.

Czy mój pracodawca powinien mnie powiadamiać o możliwym nadzorze i monitorowaniu służbowej korespondencji e-mail oraz dostępu do Internetu?

W niektórych krajach, na przykład w Chorwacji i Republice Czeskiej, pracodawcy muszą powiadamiać swoich pracowników o nadzorze i monitorowaniu służbowej korespondencji e-mail. W innych krajach, takich jak Bułgaria czy Polska, nie jest to przewidziane w prawie, ale za dobrą praktykę uważa się wdrożenie przez pracodawców polityki przejrzystości w odniesieniu do swoich pracowników. Gdy pracodawca cię zatrudnia, powinien przedstawić ci wewnętrzne zasady organizacji oraz poinformować cię o możliwym monitorowaniu twojej służbowej korespondencji e-mail i wykorzystania Internetu. Musi cię poinformować o następujących kwestiach: czy i pod jakimi warunkami możesz korzystać z prywatnej poczty elektronicznej podczas godzin pracy oraz ze służbowej poczty elektronicznej do prywatnych celów; jaka jest procedura w zakresie otwierania twoich wiadomości e-mail w przypadku przedłużonej nieobecności; jeżeli możesz korzystać z Internetu w godzinach pracy, jakie są środki techniczne i organizacyjne podjęte przez pracodawcę w celu ochrony danych osobowych.

Czy mój pracodawca może ograniczyć wykorzystanie Internetu w miejscu pracy?

Tak. Pracodawca ma prawo do kontroli i ustawiania systemów komputerowych i dostępu do Internetu w sposób, jaki mu najbardziej odpowiada. Pracodawcy zależy także na zapewnieniu, że spędzasz możliwie jak najwięcej czasu nad wykonywaniem swoich obowiązków, a nie na portalach społecznościowych czy przeglądaniu Internetu do własnych celów. Pozwala to na ograniczenie dostępu do niektórych stron internetowych, takich jak portale społecznościowe (Facebook, Twitter, G+) czy aplikacje (Skype). Ograniczenie to powinno być przewidziane w regulaminie wewnętrznym (zasadach wewnętrznego funkcjonowania). Pracownicy muszą przestrzegać ograniczeń stanowiących część regulaminu wewnętrznego, które są im należycie przedstawione (na przykład stanowią część umowy o pracę). Zatem, jeżeli chodzi o korzystanie z Internetu, pracodawca powinien wyraźnie poinformować cię o warunkach korzystania z Internetu w celach prywatnych oraz o rodzajach materiałów i stron internetowych, korzystanie z których jest zabronione. Powinieneś także posiadać informacje na temat systemów wykorzystywanych do monitoringu i kontroli.
Jednakże zaleca się, aby pracodawca raczej kładł nacisk na zapobieganie niewłaściwemu wykorzystaniu Internetu, a nie na monitorowanie dostępu pracowników. Zapobieganie obejmuje środki techniczne

ograniczające dostęp do stron internetowych wskazanych przez pracodawcę.

Czy pracodawca ma prawo dostępu do moich prywatnych wiadomości e-mail bez mojej zgody?

Nie. Prywatna komunikacja elektroniczna (e-mail, sms, historia chatu) stanowi korespondencję i nie wolno naruszać jej poufności, chyba że istnieje wyrok sądowy stanowiący inaczej. Prywatność komunikacji jest konstytucyjnie uznanym prawem w Europie. Jeżeli pracodawca narusza prywatność komunikacji, podlega karze zgodnie z prawem karnym. W przypadku, gdy naruszenia dokonał pracodawca w swoim oficjalnym charakterze, wówczas prawo przewiduje jeszcze poważniejszą karę.
Kwestia kontroli korespondencji zależy od jej charakteru: w przypadku gdy ma ona charakter prywatny, wszelka ingerencja ze strony pracodawcy czy innej osoby jest niezgodna z prawem.

Czy mój pracodawca ma prawo dostępu do mojej służbowej korespondencji e-mail bez mojej zgody?

Tak, w celu ochrony określonych praw i interesów, zapewnienia sprawnego przebiegu procesu pracy i ochrony przed możliwymi nielegalnymi działaniami pracowników pracodawca ma prawo dostępu do służbowej korespondencji e-mail. Jednakże w takich przypadkach zawsze musi istnieć równowaga między interesami pracodawcy a prawem do prywatności pracowników. Istnieje kilka zaleceń w przypadku podejmowania takich działań monitorujących: powinien istnieć konkretny, wyraźny i zgodny z prawem cel, gromadzone dane muszą być proporcjonalne do celu działań monitorujących, zaś pracownicy muszą mieć możliwość dostępu do zbieranych danych, które ich dotyczą.
Jeżeli pracodawca zamierza monitorować twoją służbową korespondencję e-mail, jej wykorzystanie do prywatnych celów musi być ściśle zabronione lub zorganizowane w taki sposób, aby twoje konstytucyjnie uznane prawa nie były naruszone poprzez dostęp do twojej osobistej korespondencji. Takie postanowienie musi być określone w wewnętrznych zasadach ustanowionych przez pracodawcę, a pracownicy muszą być o nim poinformowani.

3.5.2. Systemy nadzoru i kontroli samochodów i pojazdów firmy służących do publicznego transportu towarów i pasażerów.

Pracodawca ma prawo instalować systemy nadzoru i kontroli samochodów firmowych bez twojej zgody tylko wówczas, gdy wymagają tego charakter prowadzonej działalności zawodowej oraz środki bezpieczeństwa.
Najpopularniejsze systemy monitoringu i kontroli samochodów i pojazdów firmowych służących do transportu pasażerów i towarów to systemy tachografów oraz systemy GPS.
Jeżeli wykorzystywane są takie systemy, pracodawca musi poinformować cię o ich istnieniu i warunkach wykorzystania. Istnieje również potrzeba uregulowania wykorzystania tych systemów w formie regulaminu wewnętrznego, a dane muszą być przetwarzane tylko w celach przewidzianych w regulaminie. Przykładem konieczności instalowania takich systemów są firmy zajmujące się publicznym transportem towarów i pasażerów, świadczące usługi kurierskie oraz samochody przewożące pieniądze. Instalacja podobnych systemów umożliwia pracodawcy uzyskać informacje na temat tego, gdzie znajduje się samochód, na temat zużycia paliwa, etc., co prowadzi do optymalizacji jakości prowadzonej działalności gospodarczej. Nie ma przeszkód w instalowaniu podobnych systemów w innych pojazdach, na przy-

kład w celu śledzenia, gdzie znajduje się samochód, w przypadku kradzieży.
Wykorzystanie danych z systemu GPS zainstalowanego w samochodzie firmowym powinno być uregulowane w wewnętrznym regulaminie pracodawcy, szczególnie jeżeli pracownikowi wolno korzystać z takiego samochodu w prywatnych celach.

3.6. Techniki nadzoru i metody stosowane przez pracodawców.

Nie istnieją ujednolicone zasady dotyczące technik i metod nadzoru. Obecnie każdy kraj stara się rozwiązywać te kwestie samodzielnie, w połączeniu z powszechnymi międzynarodowymi zasadami dotyczącymi ochrony prywatności.
Niedawno miał miejsce wzrost liczby pracodawców wykorzystujących systemy nadzoru w odniesieniu do swoich pracowników w celu kontroli dostępu, kontroli czasu pracy, ochrony własności firmy oraz zwiększenia dyscypliny pracy.
Zważywszy na obecną nierówność w relacji pracodawca-pracownik, we wszystkich przypadkach nadzór nie jest wynikiem zobowiązania prawnego. W niektórych krajach, na przykład w Bułgarii, pracodawca może wykorzystywać takie techniki za twoją zgodą, która musi być wyrażona zanim staniesz się przedmiotem nadzoru, i musi spełniać następujące wymogi: musi być dobrowolna, konkretna i świadoma, jak również wyraźna.
To pracodawca musi udowodnić, że pracownik (czy też pracownicy) rzeczywiście wyraził zgodę dobrowolnie i bez żadnych zewnętrznych środków przymusu.
Posiadasz podstawowe prawo do tego, aby nie być monitorowanym, fotografowanym, filmowanym, nagrywanym ani poddawanym innym działaniom tego rodzaju bez twojej wiedzy lub mimo twojego wyraźnego sprzeciwu, z wyłączeniem przypadków przewidzianych prawem.
W innych krajach, na przykład w Republice Czeskiej, wykorzystywanie narzędzi nadzoru możliwe jest tylko w niektórych konkretnych sytuacjach wyraźnie przewidzianych w prawie pracy, a zgoda pracownika nie odgrywa żadnej roli.

3.6.1. Wykorzystanie technik nadzoru CCTV (telewizji przemysłowej)[11].

Nagrania wideo jako środek nadzoru zawierają „dane osobowe", ponieważ można cię na ich podstawie zidentyfikować w niezaprzeczalny sposób. Nadzór wideo stanowi czynność przetwarzania danych za pomocą środków zautomatyzowanych tylko wówczas, gdy ma miejsce nagrywanie.

Czy mój pracodawca ma prawo prowadzić wideonadzór w miejscu pracy?

Gdy celem wideonadzoru jest monitorowanie przebiegu pracy i kontrola czasu pracy, administrator może dokonywać nagrań wideo w ramach nadzoru swoich pracowników tylko wówczas, gdy istnieje podstawa prawna do takiego działania. W niektórych krajach, na przykład w Bułgarii, możliwe jest to po wyrażeniu wyraźnej zgody przez osoby poddawane wideonadzorowi (na przykład można zawrzeć taką klauzulę w umowie o pracę). W innych krajach, na przykład w Republice Czeskiej oraz Polsce, monitorowanie pracowników możliwe jest tylko ze względu na szczególny charakter działalności. Jeżeli warunki

11 Telewizja przemysłowa (CCTV) to wykorzystywanie sprzętu wideo do transmisji sygnału do określonego miejsca, na ograniczonej liczbie monitorów.

te nie są spełnione, pracodawca nie może monitorować swoich pracowników, nawet jeżeli zgadzają się na to.
Pracodawcy wolno również prowadzić wideonadzór w celu zapewnienia bezpieczeństwa pracy swoich pracowników lub ochrony życia i zdrowia osób, na przykład w przypadku zdalnego nadzoru pacjentów w salach reanimacyjnych. Mimo to nie wolno mu prowadzić nadzoru w miejscach takich jak przebieralnie, toalety czy pomieszczenia, w których toczy się życie towarzyskie pracowników.
Niektóre rodzaje działalności w obszarze publicznym, ze względu na swoją specyfikę, wymagają wykorzystania systemów wideonadzoru. Należą do nich sfery bezpieczeństwa narodowego i obrony, ochrony porządku publicznego, kontroli granic, bankowości oraz działalność kasyn.

Czy mam prawo do bycia poinformowanym przez administratora danych na temat prowadzonego wideonadzoru?

Tak. Pracodawca musi cię powiadomić o wykorzystywaniu technicznych środków wideonadzoru oraz o monitorowaniu określonego miejsca za pomocą tablic umieszczonych w łatwo widocznych miejscach, bez wskazania lokalizacji urządzeń stosowanych do nadzoru. Tablice muszą zawierać także informacje na temat administratora danych. Wymóg ten uznaje się za spełniony, gdy tablica informacyjna zawiera po prostu symbol, na przykład kamery.
Na przykład w Chorwacji ustawodawstwo przewiduje, że pracodawca musi skonsultować się z przedstawicielami pracowników przed wprowadzeniem nowych technologii, w tym wideonadzoru.

Czy mam prawo do wyrażenia sprzeciwu wobec prowadzenia wobec mnie wideonadzoru?

Tak, możesz wyrazić sprzeciw wobec bycia filmowanym z użyciem systemów wideonadzoru, chyba że pracodawca udowodni, że istnieje podstawa prawna do prowadzenia wideonadzoru. Jeżeli twoje obowiązki wymagają pracowania w pomieszczeniach lub w miejscu, w którym muszą być zainstalowane systemy wideonadzoru (na przykład w kasynie), pracodawca powinien powiadomić się o obowiązku prowadzenia wideonadzoru przed zatrudnieniem cię.
Stosowanie systemów nadzoru w miejscach, które nie są wykorzystywane do pracy (takich jak pomieszczenia rekreacyjne dla personelu, toalety, łazienki, przebieralnie) jest generalnie zabronione.

Czy mam prawo dostępu do dotyczących mnie nagrań wideo, które zostały nagrane z użyciem kamery do wideonadzoru?

Tak. Każda osoba fizyczna ma prawo dostępu do dotyczących jej danych osobowych (w tym nagrań wideo). W przypadkach, gdy w ramach realizacji prawa dostępu pracownicy mogą otrzymać dane osobowe osoby trzeciej, administrator zobowiązany jest do zapewnienia, że udostępnione zostaną tylko dane dotyczące określonego pracownika. W tej kwestii pracodawca powinien podjąć odpowiednie środki techniczne w celu zamazania/zaciemnienia twarzy innych osób będących przedmiotem wideonadzoru. W przypadku braku takiej możliwości technicznej dostęp do nagrań wideo może być zapewniony tylko za zgodą wszystkich osób, których dane osobowe można znaleźć na nagraniach z wideonadzoru.

3.6.2. Dane biometryczne[12].

Czy wykorzystanie systemów biometrycznych przez pracodawcę stanowi przetwarzanie danych osobowych?

Tak. Identyfikacja osoby, na przykład poprzez skan odciskow palców, stanowi automatyczne przetarzanie danych osobowych w każdej systuacji. Dane biometryczne mają szczególny charakter i w niektórych państwach, na przykład w Republice Czeskiej, uznawane są przez prawo za dane szczególnie chronione.

Czy mój pracodawca jest uprawniony do stosowania - jako narzędzia nadzoru i środka służącego do zwiększenia dyscypliny – systemów wykorzystujących dane biometryczne należące do pracowników?

Brak jest jednolitych regulacji dotyczących stosowania systemów wykorzystujących dane biometryczne do celów kontroli dyscypliny pracy. Jednakże wykorzystanie takich systemów zawsze powinno być uważnie rozważone pod względem proporcjonalności, np. czy pracodawca ma inne możliwości kontroli i monitorowania przebiegu pracy, które nie ingerują w prywatność pracowników w tak istotny sposób. W Polsce pracodawcy nie wolno stosować systemów biometrycznych opartych na danych uzyskanych na podstawie odcisków palców w celu rejestracji czasu pracy pracownika.

3.6.3. Wykorzystywanie zaawansowanych technologii (wykrywacz kłamstw).

Wraz z postępem technologicznym pracodawcy wykazują tendencję do stosowania różnych technologii w celu sprawdzania lojalności swoich pracowników. Technologie te stanowią poważną ingerencję w prywatność. Ich wykorzystywanie wywołuje nie tylko problemy prawne, ale również etyczne.

Czy mój pracodawca może poddawać mnie różnym testom i badaniom, np. z użyciem wykrywacza kłamstw, w celu ustalenia mojej lojalności i rozwagi przy wykonywaniu moich obowiązków zawodowych?

Jeżeli nie ma szczególnych regulacji prawnych, takie testy i badania mogą być przeprowadzane tylko za twoją świadomą zgodą. Równość relacji pracodawca-pracownik budzi wątpliwości w kontekście pracy (ze względu na strukturę hierarchiczną wyjątkowo trudno jest udowodnić, że zgoda została udzielona dobrowolnie i bez żadnych środków zewnętrznego przymusu). Poddanie pracowników badaniu wykrywaczem kłamstw jest nadmierne, chyba że jest przewidziane prawem. Na przykład w Polsce istnieją szczególne uregulowania dotyczące wykorzystania wykrywacza kłamstw, w przepisach dotyczących straży granicznej.

Czy wyniki takich testów mogłyby być wykorzystane jako przesłanka lub bodziec do nałożenia kar lub jednostronnego rozwiązania umowy o pracę?

Nie. Według prawa pracy wyniki uzyskane w oparciu o takie testy nie stanowią podstawy prawnej do przyjęcia odpowiedzialności dyscyplinarnej lub rozwiązania umowy o pracę.

12 Dane biometryczne są związane z cechami fizycznymi, fizjologicznymi lub behawioralnymi osoby, które pozwalają na jej identyfikację, na przykład obrazy twarzy (zdjęcia) czy dane daktyloskopijne (odciski palców). Zgodnie z wyżej wskazaną zasadą różne ustawodawstwa mogą zawierać różne przepisy na temat znaczenia pojęcia "danych biometrycznych".

Zalecenia

1. Twój pracodawca nie może żądać od ciebie więcej informacji niż przewidziano w prawie pracy, stawiając to jako wymóg przyjęcia cię do pracy.
2. Twój pracodawca nie ma prawa udostępniania twoich danych osobowych stronom trzecim bez twojej zgody, z wyjątkiem sytuacji gdy prawo stanowi inaczej.
3. Twój pracodawca musi cię poinformować o celach stosowania technologii nadzoru i monitoringu, zasad ich wykorzystywania, zakresu i metod, przed ich zainstalowaniem.
4. Twój pracodawca musi zapewnić odpowiednie środki techniczne i organizacyjne w celu ochrony twoich danych przetwarzanych w kontekście zatrudnienia.

4. Ochrona danych a zakończenie stosunku pracy

4.1. Przetwarzanie danych byłych pracowników.

Po zakończeniu stosunku pracy znacznemu ograniczeniu podlegają podstawy prawne przetwarzania danych byłych pracowników. Jednakże były pracodawca często nadal przechowuje dane osobowe byłych pracowników. Przetwarzanie tych danych jest dozwolone wyłącznie na podstawie przepisów prawa, np. przepisów emerytalnych, przepisów dotyczących ochrony zdrowia, przepisów podatkowych, przepisów dotyczących archiwizacji.
Ponadto w przypadku sporów prawnych toczących się przed sądem pracodawca może przechowywać dane osobowe byłych pracowników dopóki istnieje interes prawny uprawniający do takiego działania.
Należy zaznaczyć, że przepisy prawne obowiązujące w niektórych krajach pozwalają pracodawcom na przechowywanie danych osobowych byłych pracowników nawet do 50 lat.

Co może zrobić były pracodawca z moimi danymi osobowymi po zakończeniu stosunku pracy?

Twoje dane osobowe mogą być przechowywane tylko w sytuacji, gdy istnieje legalna lub ważna podstawa do tego. W innych przypadkach dane osobowe muszą być usunięte. Jedną z zasad zbierania i przetwarzania danych jest zasada proporcjonalności. Oznacza ona, że zbierane i przetwarzane dane osobowe powinny być adekwatne do osiągnięcia ważnego celu i nie powinny być poddawane przetwarzaniu niezgodnemu z tym celem.
Ponadto twoje dane osobowe powinny być przechowywane wyłącznie zgodnie z innymi przepisami prawa regulującymi cel zbierania i przetwarzania danych, np. zgodnie z przepisami emerytalnymi, podatkowymi czy przepisami z zakresu ochrony zdrowia, przez czas niezbędny do osiągnięcia celu określonego w tych przepisach. Poza tym w celu realizacji tych wymogów twój poprzedni pracodawca może być zobowiązany do lub mieć możliwość udostępnienia twoich danych osobowych różnym odbiorcom zgodnie z przepisami prawa.

Czy mogę mieć dostęp do moich danych osobowych w dalszym ciągu przetwarzanych przez mojego byłego pracodawcę?

Tak, pomimo faktu zakończenia stosunku pracy, twój poprzedni pracodawca ciągle jest administratorem twoich danych, które nie zostały usunięte. Prawo dostępu do twoich danych osobowych oznacza, że posiadasz prawo (jako osoba, której dane dotyczą) do uzyskania potwierdzenia, czy twoje dane są przetwarzane oraz do uzyskania informacji co najmniej o celu przetwarzania danych, kategoriach przetwarzanych danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane.

Co mogę zrobić, jeżeli uważam, że mój poprzedni pracodawca nie wywiązuje się ze wszystkich swoich zobowiązań w odniesieniu do moich danych osobowych?

W związku z tym, że w dalszym ciągu jesteś osobą, której dane dotyczą, a twój poprzedni pracodawca jest ciągle administratorem danych (w odniesieniu do twoich danych osobowych), masz prawo złożyć

skargę do właściwego organu ochrony danych osobowych, jeżeli uważasz, że twój poprzedni pracodawca przechowuje lub przetwarza twoje dane osobowe dłużej lub w szerszym zakresie niż minimum wymagające osiągnięcia ważnego celu.

4.2. Przekazywanie danych osobowych między poprzednim a obecnym lub potencjalnym pracodawcą.

Istnieją sytuacje, w których poprzedni i obecny lub potencjalny pracodawca mogą wymieniać się informacjami o pracownikach.

Czy mój poprzedni pracodawca może przekazać moje dane osobowe do obecnego lub potencjalnego pracodawcy?

Twój poprzedni pracodawca może przekazać twoje dane osobowe potencjalnemu lub przyszłemu pracodawcy wyłącznie w przypadku istnienia podstawy prawnej do tego typu działania. Taką podstawą prawną mogłaby być twoja zgoda lub legalna przesłanka obligująca poprzedniego pracodawcę. Na przykład w wielu krajach obowiązują przepisy dotyczące postępowania egzekucyjnego obligujące poprzedniego pracodawcę do przekazania twoich danych osobowych nowemu pracodawcy w przypadku spraw związanych z twoimi długami i postępowaniami egzekucyjnymi.
Twój poprzedni pracodawca (podobnie jak obecny czy potencjalny) nie jest upoważniony do udostępniania twoich danych w sytuacjach wykraczających poza relacje pracownicze z wyjątkiem sytuacji, w których wyraziłeś na to zgodę.
Należy podkreślić, że w niektórych krajach (np. Chorwacji) dane osobowe pracownika mogą być przekazywane do odbiorców wyłącznie przez pracodawcę lub osobę upoważnioną przez pracodawcę. Celem tego zapisu jest konieczność zachowania poufności danych osobowych pracownika w miejscu pracy i udostępnienie innym pracownikom tylko minimum informacji na temat danych osobowych pracownika.

4.3. Wiadomości e-mail, telefony komórkowe i inne urządzenia zawierające dane osobowe.

Często zdarza się, że były pracownik posiadał założone służbowe konto e-mail oraz mógł korzystać z telefonów komórkowych lub innych urządzeń elektronicznych należących do pracodawcy. Z chwilą zakończenia stosunku pracy konieczna jest wiedza, co należy zrobić ze służbowym adresem e-mail byłego pracownika oraz z danymi osobowymi znajdującymi się w urządzeniach, z których korzystał były pracownik, tak aby chronić jego prywatność i prawa.

Co dzieje się z moim służbowym kontem e-mail z momentem zakończenia pracy?

W przypadku, gdy twój poprzedni adres e-mail składa się z danych osobowych – twojego imienia, nazwiska lub pseudonimu, wówczas są to twoje dane osobowe i nikt inny nie ma prawa korzystać z tego adresu e-mail bez twojej zgody. Ponadto adres ten powinien być usunięty z chwilą zakończenia stosunku pracy.
Należy tu zaznaczyć, że twój były pracodawca ma prawo poprosić cię o skontaktowanie się ze wszystkimi klientami/partnerami, z którymi pozostawałeś w służbowych relacjach, celem poinformowania ich o usunięciu twojego adresu e-mail oraz o ustaleniu przez pracodawcę nowej formy kontaktu z nimi. Do-

datkowo przed usunięciem twojego konta e-mail powinieneś przekazać swojemu byłemu pracodawcy wszystkie dane związane z wykonywaną przez ciebie pracą.
W przypadku zarejestrowania na ciebie służbowych numerów telefonu, numerów faksu, telefonów komórkowych, itp., twój pracodawca powinien dokonać koniecznych zmian celem przerejestrowania ich na siebie. Egzekwując swoje prawo do usunięcia wszystkich nieaktualnych danych możesz uniknąć wszelkich nieporozumień i komplikacji, które mogą pojawić się w przyszłości.

Co dzieje się z moimi danymi osobowymi, które nie zostały usunięte z urządzeń elektronicznych należących do mojego byłego pracodawcy, których używałem pracując dla niego?

Dane odnoszące się do twojego życia prywatnego, które nie zostały usunięte i ciągle są przechowywane w urządzeniach elektronicznych użytkowanych przez ciebie (np. prywatne zdjęcia) ciągle są twoją własnością i nikt nie ma prawa do przetwarzania tych danych w jakikolwiek sposób bez twojej zgody lub bez zaistnienia ważnej legalnej przesłanki do tego działania.
Z chwilą, kiedy twój były pracodawca zorientuje się, że takie dane przechowywane są w tych urządzeniach, powinien skontaktować się z tobą. Podobnie gdy ty uzmysłowisz sobie, że twoje prywatne dane są ciągle przechowywane w urządzeniach elektronicznych użytkowanych przez ciebie a należących do twojego byłego pracodawcy, powinieneś niezwłocznie poprosić o kopię tych danych, a następnie o ich usunięcie z urządzenia. Musisz pamiętać, że z chwilą poinformowania ciebie przez byłego pracodawcę o istnieniu takich danych, zobowiązany jest on do przechowywania ich wyłącznie przez uzasadniony okres. Po tym czasie Twój były pracodawca ma prawo usunąć te dane bez Twojej zgody.
Mając na uwadze fakt, że nie zawsze jesteś w stanie stwierdzić, w czyich rękach mogą znaleźć się twoje prywatne dane, przed zakończeniem stosunku pracy nie zapomnij sprawdzić wszystkich urządzeń elektronicznych, z których korzystałeś w trakcie wykonywania pracy, i usunąć wszystkie niepotrzebne dane osobowe. Jednocześnie musisz zachować szczególną ostrożność usuwając dane – pamiętaj, że usunięcie danych związanych z wykonywaną przez ciebie pracą może być karalne.

4.4. Zakończenie stosunku pracy w drodze decyzji sądowej a przetwarzanie danych.

W przypadku, gdy prowadzone jest postępowanie sądowe dotyczące byłego pracownika i byłego pracodawcy, należy być świadomym faktu, że sprawy rozpatrywane przez sąd pracy są generalnie jawne. Co do zasady, dane osobowe zawarte w decyzjach sądu muszą być zanonimizowane.

Czy moje dane osobowe mogą zostać upublicznione w przypadku rozwiązywania konfliktu z byłym pracodawcą przed sądem?

Sąd ma prawo dokonać niezależnej oceny, które dowody powinny być uwzględnione w sprawie. W związku z tym sąd może zadecydować o przyjęciu dowodów zawierających również twoje dane osobowe. W tym przypadku, jeśli opinia publiczna i media wyrażą zainteresowanie twoją sprawą, która jest jawna, Twoje dane osobowe mogą być ujawnione. Zatem w takiej sytuacji zbieranie i przetwarzanie twoich danych osobowych jest legalne, a twoje dane wykorzystywane w sprawach sądowych mogą być upublicznione. W niektórych krajach, np. Chorwacji czy Bułgarii, dane osobowe muszą być zanonimizowane przed opublikowaniem ich na sądowych stronach internetowych.

W jaki sposób bankructwo mojego pracodawcy może mieć wpływ na moje dane osobowe?

Jak już wcześniej wspomniano, ogłoszenie bankructwa jest procedurą prawną, która może wystąpić w przypadku nieterminowego płacenia długów. W tym przypadku przedsiębiorstwo, dla którego pracujesz, może zostać zamknięte; jednakże twoje dane osobowe powinny być zbierane, przetwarzane i wykorzystywane wyłącznie gdy jest to konieczne i uregulowane odpowiednimi przepisami prawa (np. podatkowego, opieki zdrowotnej, emerytalnego, upadłościowego, archiwizacyjnego lub innymi przepisami) lub za twoją zgodą.

Zalecenia

1. Przed zakończeniem twojego stosunku pracy upewnij się, że wykasowałeś lub usunąłeś wszystkie dane osobowe nie związane bezpośrednio z wykonywaną przez ciebie pracą.
2. Twój pracodawca nie ma prawa przechowywać Twoich danych osobowych przez nieokreślony czas. Okres przechowywania danych musi zostać zdefiniowany zgodnie z przepisami prawa obowiązującymi w danym kraju. Po wygaśnięciu tego terminu pracodawca musi usunąć te dane.
3. Pamiętaj, że kiedy masz wątpliwości odnośnie zakresu przetwarzania twoich danych osobowych przez byłego pracodawcę, masz prawo do uzyskania informacji o celu przetwarzania danych, kategoriach przetwarzanych danych oraz odbiorcach, którym dane te są udostępniane (prawo dostępu do danych).
4. Twój były pracodawca zobowiązany jest do usunięcia Twojego poprzedniego konta e-mail oraz innych danych osobowych znajdujących się w różnych rejestrach (np. książce telefonicznej). W każdym momencie możesz przypomnieć mu o tym obowiązku.

5. Prawa pracowników i wsparcie organów nadzorczych

Twoje dane osobowe mają wartość, z której możesz nie zdawać sobie sprawy. Niezgodne z prawem przetwarzanie danych osobowych przez twojego pracodawcę lub inne podmioty może mieć znaczący wpływ na twoją prywatność, nie tylko w kontekście subiektywnym i psychologicznym, lecz także w zakresie strat materialnych.

Nawet wówczas, gdy ty będziesz postępował zgodnie z zaleceniami przedstawionymi w niniejszym przewodniku, twoje dane osobowe mogą być przetwarzane przez twojego pracodawcę niezgodnie z prawem. Taka niezgodność, niezależnie od tego, czy przypadkowa czy też umyślna, może przybrać różne formy, np. przekazywanie twoich danych do innych podmiotów bez twojej wiedzy na temat przyczyn lub sposobów ich dalszego przetwarzania. W ten sposób dostęp do twoich danych osobowych uzyskać mogą osoby nieupoważnione, np. twoi koledzy, którzy mogą pozyskać informacje na temat twoich zarobków lub też twoje akta osobowe zawierające dane szczególnie chronione mogą ulec zagubieniu. Innym przykładem nieprawidłowości przy przetwarzaniu danych osobowych może być śledzenie twoich zachowań w miejscu pracy przez system wideonadzoru, o istnieniu którego nie zostałeś wcześniej poinformowany przez swojego pracodawcę lub nie zgadzasz się z uzasadnieniem jego instalacji.

5.1. Ogólne prawa pracowników.

W sytuacji jakiegokolwiek zaniepokojenia związanego z przypuszczalnym naruszeniem twojej prywatności lub danych osobowych, możesz zawsze egzekwować swoje prawa w stosunku do pracodawcy. Szczególnie dzięki twojemu aktywnemu podejściu w wielu przypadkach można zapobiec niezgodnej z prawem ingerencji w twoją prywatność, doprowadzić do zakończenia takich niepożądanych sytuacji lub przyczynić się do zakończenia ciągłego wpływu na twoją prywatność. W ten sposób zadbasz o ochronę swoich praw.

Jeśli wydaje ci się, że twój pracodawca niewłaściwie wykorzystuje lub w inny sposób nielegalnie przetwarza twoje dane osobowe będące w jego posiadaniu, możesz dochodzić swoich praw bezpośrednio u pracodawcy. W tym celu powinieneś zgłosić wniosek do twojego pracodawcy, który zobowiązany jest do udzielenia ci informacji o przetwarzaniu twoich danych. Co więcej, możesz zwrócić się do pracodawcy o poprawienie twoich danych, jeżeli przedstawisz dowody na to, że są nieprawidłowe.

Jakie informacje musi dostarczyć mój pracodawca w związku z przetwarzaniem moich danych osobowych?

Pracodawca na twój wniosek musi dostarczyć ci niezbędne informacje na temat przetwarzania danych, np. na temat tego, jakie dane lub kategorie danych są przetwarzane (np. imię i nazwisko, adres domowy, data urodzenia, historia zatrudnienia, informacje potrzebne do celów podatkowych lub do wypełnienia innych zobowiązań prawnych). Masz również prawo do uzyskania informacji o źródle tych danych. Co więcej, pracodawca musi poinformować cię o celu przetwarzania twoich danych (cele podatkowe, wypłata pensji, sprawy personalne, itp.) oraz o tym, komu zostały lub mogą zostać przekazane.

Czy pracodawca może obciążyć mnie finansowo za te informacje?

Jako generalną zasadę należy przyjąć, że pracodawca nie powinien obciążyć cię finansowo za dostęp do informacji o przetwarzaniu twoich danych osobowych, innymi słowy informacja ta powinna być nieodpłatna.
Inne regulacje mogą odnosić się do poszczególnych państw członkowskich Unii Europejskiej, np. w Republice Czeskiej pracodawca może obciążyć pracownika finansowo za uzyskanie informacji, jednakże wyłącznie w sytuacji, gdy pracodawca ponosi określone i policzalne koszty. Opłata nie może jednak przewyższać tych kosztów. W praktyce trudno jest jednak szczegółowo określić koszty, w związku z czym z reguły pracodawcy rezygnują z tej opłaty.

Czy pracodawca zobowiązany jest do dostarczenia żądanych informacji w określonym czasie?

Pracodawca musi odpowiedzieć na twoją prośbę bez zbędnej zwłoki, co zwykle oznacza odpowiedź w ciągu kilku dni.

Jak często mogę zwracać się do pracodawcy o informacje na ten temat?

Generalnie nie ma ograniczeń dotyczących częstotliwości składania wniosków do pracodawcy odnośnie dostępu do informacji o przetwarzaniu twoich danych osobowych. Oznacza to, że możesz prosić pracodawcę o te informacje w każdej sytuacji, kiedy uznasz to za niezbędne. Generalnie prośba ta jest nieodpłatna, jednakże np. w Polsce możesz wnioskować o informacje bez opłat tylko raz na 6 miesięcy. Z drugiej strony w Republice Czeskiej pracodawca może zwrócić się z prośbą o pokrycie kosztów przygotowania dokumentów (np. kopii dokumentów, poszukiwania informacji, kosztów wysyłki itp.).

Czy mogę wyraźnie zażądać od administratora danych dostarczenia mi informacji w formie papierowej?

Pracodawca może dostarczyć ci żądane informacje w formie ustnej lub pisemnej. W sytuacji, gdy zwracasz się do niego z konkretną prośbą o dostarczenie ci informacji w formie papierowej, np. w celu uzyskania dowodów na przetwarzanie danych osobowych niezgodnie z obowiązującym prawem, twój pracodawca powinien dostarczyć ci te informacje w formie papierowej.

Czy mam prawo bezpośredniego dostępu do moich akt osobowych?

Problem ten odnosi się do przepisów prawa pracy i może być różnie traktowany w zależności od kraju. Na przykład w Republice Czeskiej każdy pracownik ma prawo wglądu w swoje akta osobowe oraz otrzymania kopii wszystkich dokumentów znajdujących się w tych aktach na koszt pracodawcy.

Co powinienem zrobić w sytuacji, gdy mój pracodawca przetwarza nieprawidłowe informacje o mnie?

Pracodawcy zobowiązani są do przetwarzania wyłącznie prawidłowych i aktualnych danych osobowych. Jeśli zauważysz, że twój pracodawca przetwarza nieprawidłowe dane o tobie (np. niewłaściwą datę urodzenia lub numer konta, nieprawdziwe informacje o twoim stanie cywilnym itp.) i zgłosisz to swojemu pracodawcy, organizacja zobowiązana jest do poprawienia tych danych lub ich usunięcia.

Wniosek taki powinien być w miarę możliwości odpowiednio udokumentowany (aktem małżeństwa, potwierdzeniem zameldowania, itp.).

Do kogo i w jaki sposób powinienem zwrócić się z wnioskiem o informacje, sprostowanie czy usunięcie danych?

W tym celu możesz skontaktować się ze swoim przełożonym lub działem kadr, chyba że przepisy wewnętrzne w twojej instytucji stanowią inaczej. Wniosek o informacje, sprostowanie czy usunięcie danych możesz złożyć ustnie, elektronicznie lub pisemnie. Najlepiej byłoby, gdyby fakt wpłynięcia wniosku był udokumentowany lub gdyby wniosek został wysłany pocztą elektroniczną. Jednocześnie powinieneś przechowywać kopię wysłania wniosku dla późniejszych celów dowodowych.

W jaki sposób powinienem sformułować wniosek o informacje lub sprostowanie? Czy powinienem w nim odwoływać się do przepisów prawa?

Zgłaszając wniosek o informacje lub sprostowanie nie musisz używać języka prawnego. Twój pracodawca musi ocenić zawartość tego wniosku. Oprócz informacji umożliwiających twoją identyfikację konieczne jest podanie we wniosku, że zwracasz się z prośbą o informacje o przetwarzaniu twoich danych osobowych lub wnioskujesz o sprostowanie jednej lub kilku danych osobowych będących w posiadaniu twojego pracodawcy.

Co mogę zrobić w sytuacji, gdy informacje dostarczone przez pracodawcę są niewystarczające, są niekompletne lub pracodawca odmawia mi udzielenia odpowiedzi? Co mogę zrobić, jeśli pracodawca odmawia sprostowania lub usunięcia nieprawidłowych danych, które posiada na mój temat?

W tej sytuacji możesz ponownie złożyć wniosek, tym razem adresując go do wyższej instancji niż poprzednio (np. do zarządu instytucji zamiast do przełożonego). Dochodząc swoich praw, jeśli to możliwe możesz również zwrócić się do prawnika lub związków zawodowych. Co więcej, możesz szukać pomocy u organów administracji publicznej. W tym przypadku, kiedy przedmiotem sprawy są dane osobowe i prywatność, najbardziej odpowiednią instytucją publiczną będzie organ ochrony danych osobowych w twoim kraju.

Czy mam takie same prawa w stosunku do mojego poprzedniego pracodawcy?

Twój poprzedni pracodawca zobowiązany jest do przetwarzania twoich danych osobowych nawet po zakończeniu stosunku pracy (np. dla potrzeb podatkowych lub systemu ubezpieczenia społecznego). W związku z tym twój poprzedni pracodawca, podobnie jak obecny, zobowiązany jest do udzielenia ci odpowiedniej informacji związanej z przetwarzaniem twoich danych osobowych.

5.2. Wsparcie organów nadzorczych.

W sytuacji, kiedy wydaje ci się, że twój pracodawca narusza prawa do prywatności lub przetwarza twoje dane osobowe niezgodnie z prawem, możesz zwrócić się do odpowiedniego organu ochrony danych osobowych w kraju, w którym aktualnie pracujesz. Organy ochrony danych dysponują szeregiem instrumentów prawnych, które służą ochronie twojej prywatności i mogą przewidywać środki zaradcze wobec niezgodnego z prawem przetwarzania danych.

W jaki sposób mogę złożyć skargę?

Możesz złożyć skargę na piśmie, za pośrednictwem poczty elektronicznej lub osobiście. Niezbędne jest dokładne opisanie wszystkich faktów potwierdzających twoje podejrzenia o naruszeniu twoich praw. Jednocześnie w miarę możliwości powinieneś udokumentować te fakty konkretnymi dowodami (jeśli dokumenty lub inne wymierne dowody potwierdzające naruszenie twoich praw są w twoim posiadaniu), a także powinieneś pamiętać o podaniu twoich danych kontaktowych.

Czy muszę dokonać opłaty za złożenie skargi?

Złożenie skargi jest zazwyczaj nieodpłatne. Jednakże mogą pojawić się wyjątki, np. w Polsce, składając skargę, zobowiązany jesteś do dokonania opłaty administracyjnej.

Czy mogę złożyć skargę anonimowo?

Skarga anonimowa, czyli skarga nie zawierająca informacji umożliwiającej bezpośredniej identyfikacji autora tej skargi, nie może zostać uznana jako skarga oficjalna. Co więcej, organ ochrony danych osobowych nie będzie miał możliwości zwrócenia się do ciebie o dostarczenie dodatkowych informacji, jeśli będzie to konieczne przy ocenie twojego wniosku, oraz pozbawisz się możliwości uzyskania informacji dotyczącej rezultatów rozpatrzenia wniosku. Z drugiej strony, jeśli anonimowe skargi zawierać będą uzasadnione podejrzenia systematycznego łamania prawa, odpowiedni organ może poważnie potraktować takie sygnały i podejmie się próby przeanalizowania tego problemu.

Co się dzieje z moją skargą po zgłoszeniu jej do organu ochrony danych osobowych?

Organ ochrony danych osobowych po otrzymaniu skargi analizuje ją i, jeśli zaistnieje konieczność, zwraca się z prośbą o uzupełnienie informacji. Jednocześnie powinieneś zostać poinformowany o kolejnych czynnościach związanych z rozpatrywaniem skargi. Organ ochrony danych może rozpocząć postępowanie administracyjne w stosunku do pracodawcy lub wszcząć u niego kontrolę. Twoja skarga również może zostać przekazana do innego kompetentnego organu. Jednakże może się zdarzyć, że twoja skarga zostanie uznana za bezpodstawną i w związku z tym organ ochrony danych osobowych może ją zawiesić, o czym zostaniesz poinformowany.

Czy powinienem współpracować z organem ochrony danych osobowych po uznaniu przez niego zasadności skargi?

W większości przypadków nie ma konieczności aktywnej współpracy z organem ochrony danych osobowych w procesie rozpatrywania skargi. Wyjątkowo możesz być poproszony o pomoc polegającą na złożeniu wyjaśnień na potrzeby postępowania dowodowego. Poza tym nie masz innych obowiązków związanych z rozpatrywaniem skargi.

Jakie są wyniki postępowania administracyjnego lub kontroli?

W przypadku potwierdzenia w wyniku kontroli przetwarzania przez pracodawcę danych osobowych pracownika niezgodnie z prawem, organ ochrony danych osobowych może nakazać wprowadzenie środków zaradczych w postaci zablokowania lub zniszczenia danych. Jeśli w wyniku postępowania ad-

ministracyjnego udowodnione zostanie łamanie prawa przez pracodawcę podczas przetwarzania Twoich danych osobowych, w przypadku niektórych państw członkowskich Unii Europejskiej możliwe jest nałożenie kary finansowej na pracodawcę w granicach przewidzianych prawem (takie działanie możliwe jest np. w Bułgarii lub Republice Czeskiej). W innych krajach, np. w Polsce lub Chorwacji, instytucja będąca podmiotem kontroli może zostać ukarana finansowo wyłącznie wówczas, jeśli nie wprowadziła środków zaradczych zgodnie z decyzją organu ochrony danych osobowych.

Czy powinienem być poinformowany o wynikach postępowania administracyjnego? W jakim czasie?

Organ ochrony danych osobowych powinien poinformować cię o wyniku postępowania administracyjnego jak tylko ostateczna decyzja wejdzie w życie. Okres rozpatrywania konkretnej sprawy może różnić się w zależności od przepisów prawnych obowiązujących w poszczególnych krajach członkowskich Unii Europejskiej, jak i od podjętych przez pracodawcę działań zmierzających do odwołania się od decyzji. W przypadku Republiki Czeskiej postępowanie administracyjne trwa średnio około 3 miesięcy.

Co mogę zrobić w przypadku, gdy decyzja podjęta przez organ ochrony danych osobowych nie satysfakcjonuje mnie? Czy mogę odwołać się od tej decyzji?

Jeżeli nie jesteś zadowolony z wyników działań organu ochrony danych osobowych zajmującego się rozpatrzeniem twojej skargi (nie zgadzasz się z wynikami kontroli lub postępowania administracyjnego), możesz wnieść odwołanie od tej decyzji do sądu. W niektórych systemach prawnych, np. w systemie prawnym obowiązującym w Republice Czeskiej, ty – jako skarżący – nie jesteś uwzględniony jako strona w postępowaniu prowadzonym przez organ ochrony danych osobowych, w związku z czym nie masz żadnych podstaw prawnych do podejmowania żadnych działań prawnych. Jednakże w tej sytuacji możesz skorzystać z niektórych nadzwyczajnych środków zaradczych w postaci ogólnej skargi na działanie administracji publicznej zgodnie z prawem administracyjnym lub możesz skierować swoją sprawę do rozpatrzenia przez Rzecznika Praw Obywatelskich.

Jakie inne instytucje, oprócz organu ochrony danych osobowych, są uprawnione do rozpatrywania tego typu spraw?

Możesz zgłosić się również do inspekcji pracy, która posiada kompetencje nadzorcze w obszarze dotyczącym prywatności w miejscu pracy. Inspekcja pracy może przeprowadzić inspekcje w miejscu pracy, nakazać wprowadzenie środków zaradczych lub nałożyć kary finansowe za naruszenie prawa.

Co powinienem zrobić jeśli niezgodne z prawem działania mojego pracodawcy doprowadziły do wyrządzenia mi szkody i chciałbym uzyskać z tego tytułu rekompensatę finansową od pracodawcy?

Sprawy związane z przyznaniem odszkodowania lub rekompensaty są prowadzone przez sądy powszechne, nie zaś przez organy ochrony danych osobowych. W związku z tym, jeżeli żądasz rekompensaty finansowej od twojego pracodawcy ze względu na fakt, że bezprawnie naruszył twoją prywatność, a pracodawca nie zgadza się na wypłatę rekompensaty, powinieneś złożyć wniosek do sądu powszechnego.

Gdzie powinienem złożyć skargę w sytuacji, gdy instytucja Unii Europejskiej, dla której pracuję, narusza moje prawa do ochrony danych osobowych?

Kontrolą przetwarzania danych osobowych w instytucjach Unii Europejskiej zajmuje się Europejski Inspektor Ochrony Danych (European Data Protection Supervisor). W sytuacji, gdy pracujesz w jednej z instytucji Unii Europejskiej i masz uzasadnione podejrzenia, że twój pracodawca nie przetwarza twoich danych osobowych właściwie, zgodnie z obowiązującym prawem możesz złożyć skargę bezpośrednio do Europejskiego Inspektora Ochrony Danych[13].

Zalecenia

1. Zwracaj uwagę na przetwarzanie twoich danych osobowych przez pracodawcę, ich prawidłowość i zakres.
2. Zawsze możesz zapytać swojego pracodawcę (lub innego administratora danych, np. agencję zatrudnienia) o to, w jaki sposób postępuje z twoimi danymi osobowymi.
3. Masz prawo do złożenia skargi do organu ochrony danych osobowych, jeżeli podejrzewasz, że twoje dane osobowe nie są przetwarzane zgodnie z prawem.

13 Więcej informacji na temat działalności Europejskiego Inspektora Ochrony Danych znajduje się na stronie internetowej EDPS http:// edps.europa.eu.

Słownik

Dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą); osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; przykład danych osobowych stanowią imię, nazwisko, data urodzenia, adres, numer konta bankowego, informacje o wykształceniu, doświadczeniu zawodowym, numer telefonu, adres e-mail, nagrania wideomonitoringu itp.;
Dane szczególnie chronione	zalicza się co nich co do zasady dane ujawniające pochodzenie narodowe, rasowe lub etniczne, poglądy polityczne, przynależność związkową, przekonania religijne lub filozoficzne, jak również dane o stanie zdrowia, życiu seksualnym oraz dane dotyczące skazań;
Osoba, której dane dotyczą	osoba fizyczna, której dane dotyczą, po prostu „ty";
Przetwarzanie danych osobowych	każda operacja lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie; wystarczy jedna z ww. operacji (np. gromadzenie), aby doszło do przetwarzania danych osobowych;
Administrator danych	podmiot (osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ), który decyduje o celach i środkach przetwarzania danych osobowych i ponosi odpowiedzialność za przetwarzanie tych danych, w tym podmiot, który jest zobowiązany do przetwarzania danych osobowych na podstawie przepisów prawa (np. pracodawca ma obowiązek przetwarzać pewne dane pracowników z uwagi na przepisy o ubezpieczeniu społecznym i zdrowotnym oraz kontroli podatkowej);
Przetwarzający dane	podmiot (osoba fizyczna lub prawną, władza publiczną, agencja lub inny organ) przetwarzający dane osobowe w imieniu administratora danych, np. agencja poszukująca konkretnego pracownika na zlecenie określonego pracodawcy, firma zewnętrzna prowadząca rachunkowość pracodawcy itp.;

Zgoda	dobrowolne, konkretne i świadome oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie;
Transgraniczne przekazywanie danych	swobodny przepływ danych osobowych pomiędzy krajami UE, EOG lub przekazywanie danych do państw trzecich. W obrębie państw należących do UE, EOG przepływ danych nie podlega ograniczeniom i nie wymaga zgody krajowych organów ochrony danych osobowych. Natomiast przekazywanie danych do państw trzecich może mieć miejsce jedynie po spełnieniu określonych warunków wynikających z przepisów o ochronie danych osobowych.
Organ ochrony danych osobowych	jest niezależnym krajowym organem sprawującym nadzór nad stosowaniem przepisów o ochronie danych osobowych, w szczególności przyjmuje skargi na przetwarzanie danych osobowych i informuje o sposobie ich rozpatrzenia.

Organy ochrony danych zaangażowane w projekt

POLSKA

Biuro Generalnego Inspektora Ochrony Danych Osobowych

Generalny Inspektor Ochrony Danych Osobowych, powołany w roku 1998, jest niezależnym organem nadzorczym, którego uprawnienia obejmują szeroko pojęty obszar ochrony danych. Do obowiązków Generalnego Inspektora Ochrony Danych Osobowych należą: nadzorowanie zgodności przetwarzania danych z ustawą o ochronie danych osobowych, wydawanie decyzji administracyjnych i rozpatrywanie skarg związanych z zastosowaniem przepisów o ochronie danych osobowych, prowadzenie publicznego rejestru zbiorów danych, wydawanie opinii o projektach ustaw i przepisów, uczestnictwo w pracach organizacji i instytucji międzynarodowych zaangażowanych w ochronę danych osobowych, a także inicjowanie i podejmowanie działań mających na celu poprawę ochrony danych osobowych poprzez publikację ulotek i innego rodzaju działalność edukacyjną. Generalny Inspektor Ochrony Danych Osobowych posiada uprawnienia do wydawania decyzji administracyjnych i rozpatrywania skarg związanych z zastosowaniem przepisów o ochronie
danych osobowych.

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Kontakt
ul. Stawki 2
00-193 Warszawa
Tel. (+48 22) 860 70 81
Fax: (+48 22) 860 70 90
E-mail: kancelaria@giodo.gov.pl
www.giodo.gov.pl
Godziny pracy: 8.00 - 16.00 od poniedziałku do piątku

REPUBLIKA CZESKA

Biuro Ochrony Danych Osobowych

Utworzone w czerwcu 2000 roku Biuro Ochrony Danych Osobowych jest niezależnym organem nadzorczym obdarzonym licznymi uprawnieniami. Jego misją jest zapewnienie przestrzegania zasad ochrony danych przez przedsiębiorstwa i władze oraz uświadamianie obywatelom ich praw wynikających z ustawy o ochronie danych. Biuro prowadzi różnorodną działalność, od rozpatrywania skarg i prowadzenia dochodzeń, przez konsultacje i promocje, po prowadzenie rejestru zgłoszonych operacji przetwarzania, wydawanie zezwoleń na przekazywanie danych za granicę czy przygotowywanie stanowisk w określonych sprawach. Działalność Biura reguluje czeska ustawa o ochronie danych.
Biuro jest szanowanym uczestnikiem procesu ustawodawczego, w którym uczestniczy jako konsultant, zawsze starając się promować przestrzeganie zasad ochrony danych w projektach ustaw przedkładanych przez rząd.
Biuro służy poradnictwem i wsparciem osobom fizycznym i profesjonalistom i rozprowadza wiele cennych publikacji. Poza ukazującymi się regularnie Dziennikiem Oficjalnym, Biuletynem i Sprawozdaniem Rocznym, czytelnicy mają do dyspozycji różne ulotki i broszury koncentrujące się na interesujących tematach.

úřad pro ochranu
osobních údajů
the office for personal
data protection

Kontakt
Pplk. Sochora 27
170 00 Prague 7
Tel. +420 234 665 111
Fax: +420 234 665 444
E-mail: posta@uoou.cz
www.uoou.cz
Godziny pracy: 7.30 - 16.15 od poniedziałku do czwartku
7.30 - 15.00 piątek

CHORWACJA

Agencja Ochrony Danych Osobowych

Chorwacka Agencja Ochrony Danych Osobowych (CAPPD) jest niezależnym podmiotem prawnym, któremu powierzono wykonywanie zadań publicznych. Agencja jest niezależna w realizacji swoich działań w ramach kompetencji przyznanych jej przez ustawę o ochronie danych osobowych (Dziennik Urzędowy, Nr 103/03).

Agencja składa się z 5 departamentów:
Biuro Dyrektora,
Departament Ochrony Danych Osobowych,
Departament Współpracy Międzynarodowej, UE i Spraw Prawnych,
Departament Nadzoru i Rejestru Centralnego,
Departament do Spraw Ogólnych.

Działalność Agencji obejmuje wykonywanie zadań administracyjnych i zawodowych dotyczących ochrony danych osobowych. W ramach zadań publicznych Agencja:

- nadzoruje egzekwowanie przepisów dotyczących ochrony danych osobowych,
- wskazuje na naruszenia wykryte przy gromadzeniu danych osobowych,
- prowadzi listę krajów i organizacji międzynarodowych, które odpowiednio uregulowały ochronę danych osobowych,
- rozpatruje wnioski o ustalenie możliwych naruszeń praw zagwarantowanych w ustawie,
- prowadzi Rejestr Centralny.

Agencja utworzyła dział pomocy, do którego obywatele i organizacje mogą zgłaszać naruszenia prawa w zakresie gromadzenia i przetwarzania danych osobowych, jeżeli chodzi o następujące kwestie:

- wykorzystywanie numerów identyfikacyjnych obywateli jako danych osobowych (przez banki, administrację, w handlu detalicznym, etc.);
- kopiowanie i skanowanie dokumentów tożsamości;
- stosowanie biometrii przy przetwarzaniu danych osobowych;
- udostępnianie danych osobowych studentów w miejscach publicznych.

Współpraca z innymi krajami i organizacjami partnerskim pozwala Agencji być na bieżąco z ostatnimi tendencjami i wydarzeniami w dziedzinie ochrony danych.

CAPPD uczestniczyła do tej pory w szeregu krajowych i unijnych projektów związanych z ochroną danych osobowych obywateli, w szczególności dzieci i młodzieży.

W ostatnich latach AZOP koncentruje się w szczególności na podejmowaniu proaktywnych kroków na rzecz informowania opinii publicznej na temat pojawiających się kwestii ochrony prywatności dotyczących mediów cyfrowych, Internetu i portali społecznościowych. Internet zapewnia bardzo szybką wymianę informacji, ale z drugiej strony oferuje mnóstwo możliwości naruszenia prywatności, toteż Agencja będzie usilnie pracowała nad podniesieniem świadomości publicznej na temat tej kwestii. Staje się to pilną potrzebą, gdy praktyka dziennikarska niektórych mediów ignoruje ich zobowiązania etyczne, moralne i prawne.

Kontakt
Fra Grge Martića 14
HR - 10 000 Zagreb
Tel.: 00385 (0)1 4609-000
Fax: 00385 (0)1 4609-099
E-mail: azop@azop.hr
http://www.azop.hr
Godziny pracy: 07:30 - 16:30 od poniedziałku do piątku

BUŁGARIA

Komisja Ochrony Danych Osobowych

Bułgarska Komisja Ochrony Danych Osobowych jest organem nadzorczym ds. ochrony danych w Bułgarii. Jest niezależnym organem publicznym utworzonym w 2002 r. wraz z uchwaleniem ustawy o ochronie danych osobowych. Komisja jest organem kolegialnym, składającym się z przewodniczącego i czterech członków. Kandydatury przewodniczącego i członków proponowane są przez Radę Ministrów, zaś ich wyboru dokonuje Zgromadzenie Narodowe. Ich kadencja trwa 5 lat.

Działając jako organ ochrony danych w Bułgarii, Komisja rozpatruje skargi i prowadzi przesłuchania, wydaje pozwolenia na przekazywanie danych oraz opinie prawne w kwestiach dotyczących ochrony danych i prywatności, wykonuje kontrole dotyczące administratorów danych celem zweryfikowania, czy przestrzegają prawa, określa minimalne środki techniczne i organizacyjne ochrony danych, które muszą być wdrożone przez administratorów danych, wydaje obowiązkowe instrukcje, itp.

Jednym z kluczowym kierunków pracy Komisji jest prowadzenie skutecznej międzynarodowej współpracy oraz programów szkoleniowych dotyczących różnych aspektów wśród określonych grup docelowych społeczeństwa. W tym względzie bardzo ważnym instytucjonalnym uprawnieniem Komisji jest możliwość zawierania międzynarodowych porozumień o współpracy z podobnymi organami nadzorczymi ds. ochrony danych.

Komisji działa przy wsparciu struktury administracyjnej podzielonej na 4 dyrektoriaty (1 ogólny i 3 wyspecjalizowane). Łączna liczba pracowników, w tym członków Komisji, wynosi 87 osób.

Kontakt
№ 2 Prof. Tsvetan Lazarov Blvd.,
Sofia 1592
Tel.: 3592/91-53-518
Fax: 3592/91-53-525
E-mail: kzld@cpdp.bg
www.cpdp.bg