JUSTYNA JABŁONKA

Październik 2023
Nr 8/2023

KANCELARIA WYRZYKOWSCY

Newsletter
INSPEKTORA OCHRONY DANYCH
ADW. JUSTYNY JABŁONKI

Drodzy Czytelnicy,

w najnowszym wydaniu naszego Newslettera omówimy związek między danymi osobowymi a sztuczną inteligencją, w szczególności skupiając się na ChatGPT i jego zgodności z zasadami ochrony danych osobowych. Zbadamy również, jakie dokumenty swoich pracowników pracodawcy mogą przechowywać, a które powinny być dostępne jedynie do wglądu, jak również wskażemy na problematykę udostępniania kontrahentom przez pracodawcę danych pracownika. Wreszcie przyjrzymy się obowiązkowi informowania o pozyskiwaniu danych osobowych z rejestrów publicznych. Zachęcam do uważnej lektury, aby pozostać na bieżąco z kluczowymi kwestiami dotyczącymi ochrony danych osobowych.

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

W październikowych News'ach znajdziecie Państwo tematy:

I. Dane osobowe a sztuczna inteligencja, czyli kilka słów o ChatGPT i jego zgodności z RODO.

Kto z nas w ostatnim czasie nie słyszał o sztucznej inteligencji i ChatGPT? UODO zwrócił uwagę na bezpieczeństwo danych osobowych przetwarzanych w ramach sztucznej inteligencji i o tym chciałabym dzisiaj Państwu krótko wspomnieć.

Czym jest Chat GPT?

ChatGPT („Generative Pre-trained Transformer" czat) to narzędzie w formie aplikacji on-line, służące do rozmowy z wykorzystaniem sztucznej inteligencji. Zadając pytanie, udzielamy mu tzw. „podpowiedzi", wymuszając jego odpowiedź, powstałą na bazie relacji słów, zapamiętanych w procesie wyuczania. Jest to model, w którym algorytm został wytrenowany na bardzo dużej ilości danych tekstowych, pochodzących z Internetu. ChatGPT niewątpliwie imponuje umiejętnością generowania ogromnego zakresu przekonujących treści w wielu językach. Ma jednak kilka wad, a szczególności taką, że może się mylić i podawać nieprawidłowe/nieprawdziwe fakty.

ChatGPT a dane osobowe.

Każde zapytanie użytkownika ChatGPT, jest widoczne dla jego twórcy. Wobec powyższego należy bardzo ostrożnie formułować zapytania pod kątem zawartych w nich informacji, w szczególności należy zadbać o to, aby w zapytaniach do ChatGPT nie podawać informacji o charakterze danych osobowych bądź informacji poufnych. W związku z powyższym ważne jest, aby twórcy takich narzędzi, jaka ChatGPT, wykonywali obowiązki wynikające z przepisów o ochronie danych osobowych oraz zapewniali ochronę danych w związku z korzystaniem z narzędzi przez nich proponowanych. Zgodnie z najnowszym stanowiskiem UODO „przetwarzanie danych osobowych z wykorzystaniem AI nie jest wykluczone, niemniej jednak algorytmy i systemy sztucznej inteligencji muszą zapewniać odpowiednio wysoki poziom bezpieczeństwa danych osobowych". AI – sztuczna inteligencja, nie może godzić w prywatność i ochronę danych osobowych.

Komisja Europejska już od 2020 r. pracuje nad „Aktem w sprawie sztucznej inteligencji" (AI Act). Ten unijny dokument, który został ogłoszony w formie Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii będzie pierwszym na świecie aktem prawnym, kompleksowo regulującym kwestie związane ze sztuczną inteligencją. Zwraca się w nim uwagę na sposoby ochrony danych osobowych przetwarzanych w związku z pojawieniem się i rozwojem sztucznej inteligencji.

Według wytycznych wskazanych przez nie tylko polski, ale też zagraniczne organy nadzorcze, twórcy sztucznej inteligencji muszą zwrócić szczególną uwagę na:

1. Ustalenia i wskazanie użytkownikowi podstawy prawnej do przetwarzania danych osobowych,
2. Wskazania administratora, współadministratora, podmiotów przetwarzających,
3. Konieczność przeprowadzenia DPIA,
4. Zapewnienia obowiązków informacyjnych,
5. Zabezpieczenia przetwarzania danych,
6. Realizację praw osób, których dane dotyczą,
7. Zautomatyzowane przetwarzanie danych i obowiązki z tym związane, ponieważ szczególnie w tym zakresie pojawiają się braki.

Czy ChatGPT może stanowić zagrożenie dla bezpieczeństwa danych osobowych?

Przeprowadzono dotychczas kilka badań na temat tego, czy ChatGPT może napisać złośliwe oprogramowanie. Pojawiły się bowiem obawy, że ChatGPT może zostać wykorzystany przez kogoś mającego złe zamiary, ale nie posiadającego wystarczającej wiedzy, aby wygenerować kod złośliwego oprogramowania. Na ten moment, ChatGPT jest dobrą opcją dla ekspertów, którzy mogą potwierdzić, czy dane przekazane przez narzędzie są prawidłowe i prawdziwe, i nadaje się bardziej do rozwiązywania prostych zadań niż złożonych. Niewykluczone jednak, że ekspert będzie w stanie nakłonić ChatGPT do napisania, czy może bardziej korekty, złośliwego oprogramowania.

ChatGPT może być również pytany o doradztwo w zakresie problemów technicznych. Istnieje zatem ryzyko, że przestępcy będą wykorzystywać ChatGPT do pomocy w cyberatakach w zakresie przekraczającym ich możliwości.

Ponadto, pojawiło się zagrożenie, że przestępcy wykorzystają go do napisania przekonujących maili phishingowych, w tym w wielu językach. Może to skutkować tym, że osoba mająca możliwości techniczne, stworzy przekonujące treści – maile phishingowe, a następnie będzie za pomocą ChatGPT rozpowszechnić je w dużo większej mierze, niż bez tego narzędzia, albowiem wykorzysta go do tłumaczenia treści i przesłania ich do

większej liczby odbiorców, również zagranicznych.

Jako że sztuczna inteligencja dopiero się rozwija, nie są znane wszystkie zagrożenia jakie może powodować dla danych osobowych. Niemniej jednak, już na ten moment, organy nadzorcze przyglądają się jej działaniu i podejmują pewne kroki.
Pierwszą odpowiedzią w zakresie stosowania sztucznej inteligencji i ChatGPT jest działanie włoskiego organu nadzorczego, który nakazał ograniczenie przetwarzania danych dotyczących użytkowników tej usługi we Włoszech, po ujawnieniu wycieku rozmów oraz informacji o płatnościach subskrybentów ChatGPT. Organ zwrócił uwagę, że użytkownicy ChatGPT nie otrzymują żadnej informacji w przedmiocie obowiązków informacyjnych RODO, oraz wskazał, że trudno wręcz jest wskazać podstawę prawną do gromadzenia danych osobowych dla samego trenowania ChatGPT.

Podsumowanie:
Korzystanie ze sztucznej inteligencji daje wiele możliwości i może być pomocne, zarówno w tworzeniu nowego biznesu, rozwijaniu tego, który istnieje, ale także i przy wykonywaniu pracy przez pracownika. Należy jednak korzystać z takich narzędzi z zachowaniem ostrożności, ponieważ kwestia ochrony danych osobowych w związku ze sztuczną inteligencją ma duże braki, a wiele wątków związanych z prawami osób, które z niej korzystają, pozostaje nieuregulowanych. Twórcy sztucznej inteligencji nie zadbali dotychczas o to, aby wprowadzić odpowiednie, tj. spełniające wymogi m. in. RODO, rozwiązania gwarantujące ochronę danych osobowych.

Trzeba zatem zachować rozwagę w podawaniu swoich lub innej osoby danych osobowych np. w trakcie rozmowy z ChatGPT, ponieważ na ten moment nie mamy kontroli nad tym, co się dzieje z naszymi danymi i do czego mogą być wykorzystane.

Autor:
Justyna Jabłonka
Inspektor Ochrony Danych
adwokat

II. Jakie dokumenty pracownika pracodawca może przechowywać, a jakie powinien otrzymać jedynie do wglądu bez możliwości ich utrwalania zgodnie z brzmieniem RODO?

W dzisiejszym wpisie, kontynuując rozpoczęty w poprzednim miesiącu temat RODO w HR, chciałabym zwrócić uwagę na kolejną ważną kwestię, tj. tą dotyczącą dokumentów przechowywanych w szczególności w aktach pracowniczych.

Dokumentacja pracownika – analiza ogólna.

Na wstępie spójrzmy na art. 94 pkt 9a Kodeksu pracy, który wskazuje, że jednym z obowiązków pracodawcy jest prowadzenie i przechowywanie w postaci papierowej lub elektronicznej dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników (dokumentacja pracownicza). Jak wynika z powyższego, dokumentację pracowniczą dzieli się na dwie części, tj. akta osobowe oraz dokumentację w sprawach związanych ze stosunkiem pracy.

Jeżeli chodzi o akta osobowe, składają się one z czterech części:

- **część A akt osobowych,** w których powinny znaleźć się oświadczenia lub dokumenty zgromadzone w związku z ubieganiem się o zatrudnienie oraz skierowania na badania lekarskie i orzeczenia lekarskie dotyczące wstępnych, okresowych i kontrolnych badań lekarskich z poprzednich okresów zatrudnienia;
- **część B akt osobowych,** w których powinny znaleźć dokumenty dotyczące nawiązania stosunku pracy oraz przebiegu zatrudnienia;
- **część C akt osobowych,** w których powinny znaleźć się dokumenty związane z ustaniem zatrudnienia danej osoby;
- **część D akt osobowych,** w których powinny znaleźć się odpis zawiadomienia o ukaraniu oraz inne dokumenty związane z ponoszeniem przez pracownika odpowiedzialności porządkowej lub odpowiedzialności określonej w odrębnych przepisach, które przewidują zatarcie kary po upływie określonego czasu.

Ponadto, oddzielnie od akt osobowych pracodawca prowadzi również dokumentację w sprawach związanych ze stosunkiem pracy, na którą składają się m. in. dokumenty dotyczące ewidencjonowania czasu pracy, korzystania z urlopów, listy płac, karty ewidencji przydziału odzieży roboczej.

Wszystkie dokumenty i oświadczenia, które znajdują się w poszczególnych częściach akt osobowych, należy przechowywać z zachowaniem porządku chronologicznego i z zachowaniem bezpieczeństwa danych.

Co oczywiste, dokumentacja pracownicza obejmuje szereg dokumentów, a tym samym wiele danych osobowych pracownika. Pracodawca powinien więc zachować szczególną ostrożność i gromadząc dokumentację postępować w zgodzie z zasadą minimalizacji danych wyrażoną w art. 5 lit. c RODO. Jak pamiętamy, zasada minimalizacji wymaga od administratora – tutaj od pracodawcy, aby przetwarzał dane które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Jakie błędy popełniają najczęściej pracodawcy?

Zgodnie z zasadą minimalizmu, pracodawca powinien pozyskiwać i przetwarzać wyłącznie takie dane, jakie jest zobligowany posiadać zgodnie z przepisami prawa. Będą to zatem wszelkie dokumenty składające się na dokumentację pracowniczą i wskazane wprost w treści Rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej w sprawie dokumentacji pracowniczej. Trzeba jednak pamiętać, że katalog dokumentów wymienionych w wyżej wskazanym rozporządzeniu jest otwarty, więc praktyka może wymagać od pracodawcy przechowywania także innych, nie wymienionych tam wprost dokumentów.

W aktach osobowych pracowników prowadzonych w postaci papierowej, powinny być gromadzone jedynie kopie dokumentów, które są dostarczane przez pracownika, chyba że konieczność pozyskiwania oryginałów wynika bezpośrednio z przepisów prawa. Pracodawca ma prawo dokonywać kopii i przechowywać takie dokumenty jak np. **świadectwo pracy czy dyplom ukończenia szkoły lub certyfikaty** - dla potwierdzenia **kwalifikacji pracownika**. Oryginałów takich dokumentów pracodawca może żądać jedynie do wglądu.

A co w przypadku, kiedy pracodawca chce potwierdzić dane pracownika? Niejednokrotnie pracodawcy – wciąż, mimo tak długiego już okresu obowiązywania RODO, pytają mnie, czy mogą kopiować dowód osobisty, paszport, akty stanu cywilnego (np. w związku z udzieleniem urlopu okolicznościowego) lub prawo jazdy. A wszystko to, aby potwierdzić dane pracownika lub okoliczności, na które się powołuje. Ale czy jest to dozwolone? W moim przekonaniu nie. Kopiowanie i przechowywanie takich dokumentów, które nierzadko przecież wskazują dużo więcej danych osobowych niż te, które pracodawca może przetwarzać, stanowi działanie niezgodnie z zasadą minimalizacji danych. W związku z powyższym osobiście rekomenduję pracodawcom, aby żądali jedynie okazania dokumentów takich jak dowód osobisty, paszport czy akty stanu cywilnego, a z okazania sporządził np. notatkę (bez spisywania niepotrzebnie danych osobowych).

Odpowiedź nie jest tak jednoznaczna w przypadku prawa jazdy pracownika. Analizę problemu tego dokumentu trzeba zacząć od wskazania, że prawo jazdy nie jest dokumentem tożsamości, a dokumentem poświadczającym posiadane uprawnienia do prowadzenia pojazdów wskazanej kategorii. Rozróżnienie to jest niezwykle ważne, ponieważ pracodawcy często uważają prawo jazdy za dokument wręcz tożsamy z dowodem osobistym.

Pracodawca będzie miał prawo do posiadania kopii prawa jazdy w przypadku, gdy dokument ten będzie niezbędny pracownikowi do wykonywania obowiązków wiążących się z koniecznością prowadzenia pojazdów, a celem jego udostępnienia przez pracownika jest potwierdzenie posiadanych uprawnień. Niemniej jednak, nic nie stoi na przeszkodzie, aby pracodawca bazował jedynie na oświadczeniu pracownika, okazaniu tego dokumentu oraz sporządzonej z okazania notatki. To rozwiązanie należy uznać za lepsze z punktu widzenia ochrony danych osobowych (chociaż jak wskazano, nie jest jedyne poprawne). W przypadku zawodowych kierowców natomiast, pracodawca może przechowywać kopię prawa jazdy jako dokument potwierdzający kwalifikacje do wykonywania powierzonej pracy. Wątpliwości mogą pojawić się jednak w przypadku, gdy pracownik otrzymuje samochód służbowy jako dodatek w pracy, ale nie jest zatrudniony na stanowisku kierowcy. Według ugruntowanego już stanowiska, jeśli służbowe auto ma być narzędziem pracy pracownika, to prawo jazdy będzie niezbędną kwalifikacją do wykonywania pracy. Jeśli zaś służbowe auto ma być dodatkiem, to prawo jazdy może być pracodawcy okazane za zgodą pracownika.

Czy pracownik może wyrazić zgodę na przechowywanie kopii dokumentów i przetwarzanie jego danych w sposób szerszy od tego, co zostało uregulowane w przepisach prawa?

Według wypracowanej praktyki – tak, pracownik może wyrazić zgodę na przetwarzanie jego danych poprzez przechowywanie określonych dokumentów. Pozostaje jednakże pytanie, czy w takim przypadku, bądź - czy w każdym takim przypadku, pracodawca będzie w stanie odpowiednio uargumentować potrzebę przetwarzania tych danych, a tym samym wykazać, że nie narusza zasady minimalizmu.

Reasumując: przechowując dane pracowników, działy HR powinny zawsze mieć bacznie na uwadze brzmienie przepisów prawa w tym zakresie (w szczególności kodeks pracy oraz rozporządzenie, o którym mowa na wstępie), a także zasadę minimalizmu danych. Nie jest bowiem trudnością skopiować wszystkie dokumenty, które ułatwią niejako pracodawcy działalność, ale trudnością jest niejednokrotnie wykazać, że te dokumenty i dane w nich zawarte, były pracodawcy niezbędne i są zgodne z przepisami.

Autor:
Justyna Cybulska
zespół Inspektora Ochrony Danych
adwokat

III. Obowiązek informowania o pozyskaniu danych osobowych z rejestrów publicznych (art. 14 RODO)

Wyrokiem z dnia 19 września 2023 r. (sygn. akt III OSK 2538/21) Naczelny Sąd Administracyjny podtrzymał pierwszą karę nałożoną przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO) na podstawie przepisów RODO. **Kara w wysokości 943 tys. zł została nałożona za nieinformowanie osób, których dane dotyczą o pozyskaniu ich danych osobowych.** Tym samym NSA potwierdził konieczność informowania osób, których dane dotyczą o pozyskaniu ich danych osobowych, nawet w sytuacji, gdy ich źródłem są ogólnodostępne rejestry publiczne. W ocenie Sądu zasadą jest bowiem transparentność przetwarzania danych osobowych, a wszelkie wyjątki od tej zasady, w tym wyjątek dotyczący zwolnienia z obowiązku informacyjnego, należy interpretować zawężająco i dopuszczać co do zasady tylko przy przetwarzaniu danych dla celów publicznych, w szczególności statystycznych, badawczych, archiwalnych czy historycznych. W praktyce oznacza to konieczność realizacji obowiązku informacyjnego w zasadzie w każdym przypadku pozyskania danych osoby fizycznej ze źródeł takich jak: Centralna Ewidencja i Informacja o Działalności Gospodarczej czy Krajowy Rejestr Sądowy czy Krajowy Rejestr Urzędowy Podmiotów Gospodarki Narodowej (REGON).

Źródła publiczne a obowiązek informacyjny z art. 14 RODO

Źródłem wskazanego obowiązku jest art. 14 RODO, który nakłada na administratora obowiązek podania osobie, której danych nie pozyskano bezpośrednio od niej, szeregu informacji dotyczących przetwarzania jej danych osobowych, w tym źródła z której pozyskano jej dane i przysługujących jej praw. Obowiązek ten pojawia się w każdym przypadku, gdy administrator uzyska dane osobowe z innego źródła niż ta osoba. Źródłem takim mogą być w szczególności inni (zewnętrzni) administratorzy danych; pośrednicy danych, inne osoby, których dane dotyczą oraz źródła dostępne publicznie (Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, 2017). Szczególnie interesująca jest sytuacja, gdy informacje pozyskiwane są ze źródeł dostępnych publicznie, w tym z rejestrów tworzonych na podstawie regulacji ustawowej z założeniem umożliwienia powszechnego dostępu do znajdujących się w nich danych i ich swobodnego przetwarzania.

Określona z góry jawność tych rejestrów każe zakładać osobie, której dane zostały ujawnione w takim rejestrze, że dane te będą dostępne potencjalnie dla każdego zainteresowanego i przetwarzane w zasadzie w niekontrolowany sposób. Z uwagi na ustawowy obowiązek ujawnienia tych danych osoba ta w zasadzie nie ma możliwości uniknięcia takiej sytuacji. Może się zatem wydawać, że informowanie tej osoby o każdym fakcie pozyskania jej danych osobowych jest pozbawione sensu, jednak przepisy RODO zakładają, że osoba, której dane zostały ujawnione w rejestrze publicznym ma prawo uzyskać informację kto i w jakim celu pozyskuje jej dane z tego rejestru. Art. 14 ust. 2 lit. f RODO, wprost stanowi, że administrator podaje osobie, której dane dotyczą, źródło pochodzenia danych osobowych, a gdy ma to zastosowanie także informację czy pochodzą one ze źródeł publicznie dostępnych. Istnienie tego obowiązku potwierdza PUODO, który nakłada wysokie kary pieniężne na administratorów, którzy nie wywiązują się z tego obowiązku. Wskazany na wstępie wyrok NSA ostatecznie przesądza, że pomimo pojawiających się praktyce licznych wątpliwości, obowiązek ten musi być realizowany.

Wyłączenia obowiązku informacyjnego

Art. 14 ust. 5 RODO przewiduje, ze **administrator nie musi realizować obowiązku informacyjnego i tym samym informować o pozyskaniu danych osobowych jeżeli: osoba, której dane dotyczą, dysponuje już odpowiednimi informacjami; udzielenie informacji jest niemożliwe; udzielenie informacji wymagałoby niewspółmiernie dużego wysiłku; realizacja obowiązku informacyjnego mogłoby uniemożliwić lub poważnie utrudnić realizację celów przetwarzania danych osobowych; pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator oraz, gdy dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego.** Ponadto, zgodnie z przepisami ustawy o ochronie danych osobowych z 10 maja 2018 r. art. 14 RODO nie znajduje zastosowania do: działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych oraz do wypowiedzi w ramach działalności literackiej i artystycznej.

Administrator, który chce powołać się na okoliczność, że udzielenie wymaganych informacji jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, powinien przeprowadzić test równowagi, aby porównać wysiłek wkładany w udzielenie informacji osobie, której dane dotyczą, z konsekwencjami i skutkami dla tej osoby w przypadku nieudzielenia tego rodzaju informacji. Administrator powinien udokumentować dokonanie takiego testu zgodnie ze spoczywającymi na nim obowiązkami w zakresie rozliczalności (Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, 2017). Niemożliwość lub niewspółmiernie duży wysiłek muszą wynikać bezpośrednio z faktu, że dane osobowe zebrano w inny sposób niż od osoby, której dane dotyczą. Dokonując oceny czy okoliczności takie zachodzą, należy wziąć pod uwagę m.in. liczbę osób, których dane dotyczą; okres przechowywania danych i przyjęte przez administratora zabezpieczenia. Warto przy tym podkreślić, że zgodnie ze stanowiskiem prezentowanym przez sądy administracyjne, jeżeli administrator posiada dane teleadresowe osoby fizycznej prowadzącej jednoosobową działalność gospodarczą, lub która zawiesiła wykonywanie działalności gospodarczej to wysłanie jej informacji, o których mowa w art. 14 RODO pocztą tradycyjną lub w drodze kontaktu telefonicznego nie może być uznane za czynność niemożliwą lub wymagającą niewspółmiernie dużego wysiłku. W szczególności o potrzebie niewspółmiernie dużego wysiłku w tym zakresie nie może przesądzać sam fakt dużej liczby osób, którym należałoby podać wymagane informacje. Należy jednak zauważyć, że nawet jeśli administrator wykaże, że podanie poszczególnym osobom informacji wymaganych w sytuacji pozyskania danych osobowych jest niemożliwe albo, że wymagałoby niewspółmiernie dużego wysiłku to i tak nie zwalnia go to w całości z obowiązku informacyjnego, bowiem art. 14 ust. 5 lit. b RODO, zobowiązuje go do podania wymaganych informacji publicznie. Oznacza to konieczność opublikowania przez administratora ogłoszeń zawierających niezbędne informacje (np. w mediach lub na własnej stronie internetowej).

W tej sytuacji możliwość odstąpienia od obowiązku informowania o pozyskaniu danych osobowych może być bez zastrzeżeń dopuszczona w zasadzie tylko w sytuacji, gdy dane osobowe zostały pozyskane w wykonaniu obowiązku wynikającego z przepisów prawa powszechnie obowiązującego (co może dotyczyć w szczególności pozyskiwania danych przez organy administracji publicznej, które działają w celu wykonania nałożonych na nie obowiązków ustawowych) lub, gdy fakt ten nie może być ujawniony z uwagi na konieczność zachowania tajemnicy zawodowej.

Termin spełnienia obowiązku informacyjnego

Obowiązek informacyjny określony w art. 14 RODO powinien być zrealizowany w „rozsądnym terminie" po pozyskaniu danych osobowych. Podejmując decyzję o tym, w którym momencie udzielić informacji przewidzianych w art. 14, administrator powinien brać pod uwagę rozsądne oczekiwania osób, których dane dotyczą, potencjalny wpływ przetwarzania na te osoby i ich zdolność do wykonywania praw w związku z tym przetwarzaniem (Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, 2017).

W każdym jednak przypadku obowiązek informacyjny z art. 14 RODO należy zrealizować w czasie pierwszego kontaktu z osobą, której dane dotyczą, a gdyby kontakt taki nie miał miejsca, nie później niż w ciągu miesiąca od pozyskania danych.

Informacje muszą być „podane"

Art. 14 RODO przewiduje, że wskazane w jego treści informacje, muszą być „podane" osobie, której dane dotyczą. Obowiązek podania informacji oznacza, że administrator musi podjąć czynne działania w celu udzielenia osobie, której dane dotyczą, niezbędnych informacji lub czynnie skierować ją do miejsca, w którym te informacje się znajdują. Miejsce i sposób udostępnienia informacji powinny być oczywiste, co można zapewnić np. dzięki bezpośredniemu udzieleniu informacji, podaniu linków, wyraźnemu oznakowaniu takich informacji lub podaniu ich w formie odpowiedzi na konkretnie sformułowane pytanie. Obowiązek podania informacji nie będzie natomiast zrealizowany, jeżeli osoba, której dane dotyczą, będzie musiała samodzielnie szukać informacji, które powinien podać jej administrator.

Sposób podania informacji

RODO nie określa formy ani sposobu realizacji obowiązku informacyjnego z art. 14, niemniej zgodnie z treścią art. 12 ust. 1 RODO należy przyjąć, że co do zasady niezbędne informacje powinny być udzielane na piśmie. W stosownych przypadkach, tj. w sytuacjach determinowanych sposobem utrzymywania kontaktów z osobą, której dane dotyczą, mogą one być udostępnione w inny sposób, w tym w formie elektronicznej. Grupa Robocza Art. 29 zaleca przy tym, by wszystkie informacje skierowane do osoby, której dane dotyczą, były dla niej dostępne w jednym miejscu lub w ramach jednego dokumentu, który powinien być łatwo dostępny na wypadek, gdyby osoba ta chciała zapoznać się z całością informacji, a jednocześnie, by informacje dotyczące przetwarzania danych osobowych były wyraźnie wyodrębnione od innych informacji niezwiązanych z prywatnością, np. postanowień umownych lub ogólnych warunków korzystania (Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, 2017). W każdym przypadku administrator musi dążyć do tego, by informacje były przekazywane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

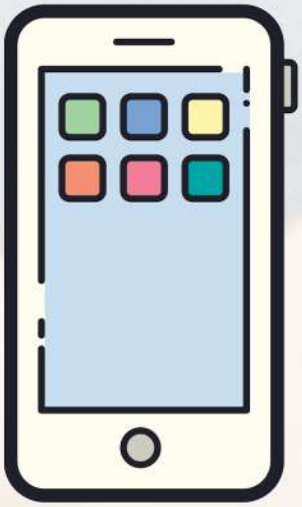
Autor:
Grzegorz Lubeńczuk
zespół Inspektora Ochrony Danych
doktor, radca prawny

IV. Czy pracodawca może udostępnić kontrahentom dane dotyczące pracownika?

W najnowszym Biuletynie UODO pojawiła się informacja na temat tego, że w wyniku wniesionej przez pracownika skargi, pracodawca **otrzymał karę od UODO w związku z udostępnieniem danych tego pracownika kontrahentowi.**

Pracodawca chciał w ten sposób zachować dobre relacje z kontrahentem, natomiast pracownik z powodu nieobecności w pracy spowodowanej dłuższą choroba, nie podejmował z nim kontaktu. Kontrahent zażądał wyjaśnień, a pracodawca wskazał, że pracownik pozostaje na zwolnieniu chorobowym i udostępnił kontrahentowi jego **prywatny numer telefonu.**
Pracownik wniósł skargę zarzucając, że doszło do naruszenia nie tylko RODO, ale także i jego prywatności, a UODO skargę ta uwzględnił.

Prywatny numer telefonu pracownika.
Pracodawca, w pierwszej kolejności, nie miał podstawy prawnej do udostępnienia kontrahentowi prywatnego numery telefonu pracownika. Naruszony został zatem art. 6 ust. 1 RODO. **Prywatny numer telefonu pracownika może być przetwarzany tylko za jego zgodą.** W opisywanej sprawie, pracownik takiej zgody nie wyraził, a co więcej, swojego prywatnego numeru nie udostępnił pracodawcy (a jedynie współpracownikom). Poza tym, kontakt był możliwy za pośrednictwem służbowego adresu e-mail albo służbowego numeru telefonu, ale nie zadbano o stosowne rozwiązania na czas nieobecności pracownika, np. automatyczne powiadomienie o tymczasowym przejęciu obowiązków pracownika przez inna osobę.
Pracodawca może zatem przetwarzać dane osobowe pracownika w postaci prywatnego numeru telefonu, ale nie może czynić tego w sposób dowolny, bez podstawy prawnej. Taką podstawą może być zgoda pracownika. W razie jej braku pracodawca narusza RODO.



Dane dotyczące zdrowia pracownika.

Ale idąc dalej, pracodawca udostępnił także dane wrażliwe, bo dotyczące zdrowia pracownika, co powoduje naruszenie art. 9 ust. 1 RODO.

Pracodawca tłumaczył, że udostępnienie tych danych było skutkiem braku kontaktu pracownika z kontrahentem, tj., że pracownik nie odpowiadał na maile, a pracodawcy zależało na długiej współpracy biznesowej. Dodatkowo, w związku z przedłużającym się zwolnieniem pracownika, konieczna była reorganizacja pracy i rozdzielenie jego obowiązków innym pracownikom.

UODO uznał jednak, że te powody nie stanowią żadnej z przesłanek wymienionych w art. 9 ust. 2 RODO, które umożliwiałyby udostępnienie danych o zdrowiu pracownika osobom trzecim.

Dane osobowe o zwolnieniu lekarskim pracownika to dane szczególnej kategorii. Danymi szczególnej kategorii o stanie zdrowia są m.in. dane o

- chorobie,
- ryzyku choroby,
- historii medycznej,
- stanie fizjologicznym,
- stanie biomedycznym.

Podsumowanie: pracodawca powinien pamiętać, że nawet wydające się błahym udostępnienie danych osobowych, musi mieć swoją podstawę prawną, a prywatność i ochrona danych pracownika jest ważniejsza, niż działalność pracodawcy.

Udostępnienie danych osobowych pracownika osobom trzecim, w tym kontrahentom, dotyczyć może imienia, nazwiska, stanowiska oraz służbowego numeru telefonu i adresu e-mail, o czym pisaliśmy w poprzednich miesiącach.

Autor:
Justyna Jabłonka
Inspektor Ochrony Danych
adwokat

JUSTYNA JABŁONKA

KANCELARIA WYRZYKOWSCY

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

www.justynajablonka.pl
www. kancelariawyrzykowscy.pl

BLOG dla JST:
https://kancelariawyrzykowscy.pl/pl/blog-jst/
FB:
https://www.facebook.com/kancelariawyrzykowscy