JUSTYNA JABŁONKA

Czerwiec 2023
Nr 4/2023

KANCELARIA WYRZYKOWSCY

Newsletter
INSPEKTORA OCHRONY DANYCH
ADW. JUSTYNY JABŁONKI

Drodzy Państwo,
nadszedł czerwiec a wraz z nim przywitało nas piękne, słoneczne lato. Chociaż chętnie oddajemy się już wakacyjnym planom i cieszymy się tymi długimi, ciepłymi dniami, nie możemy zapominać o jednym ważnym aspekcie naszego codziennego życia – ochronie naszych danych. Niech ta piękna pogoda nie zasłoni nam wzroku przed tym, jak ważne jest zachowanie prywatności i jej ochrona. Przygotujcie się na interesujące artykuły i przydatne wskazówki, które pozwolą wam zwiększyć świadomość dotyczącą ochrony danych osobowych.

Przyjemnej lektury.

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

W czerwcu wskazuję na tematy:

I. Kradzież tożsamości, zaciągnięcie kredytu na kogoś innego będzie trudniejsze, czyli jak, gdzie i kiedy będzie można zastrzec swój numer PESEL?

Czym jest numer PESEL?

PESEL (Powszechny Elektroniczny System Ewidencji Ludności) to centralny zbiór danych prowadzony na podstawie ustawy z dnia 24 września 2010 roku o ewidencji ludności.

Numer PESEL to jedenastocyfrowy symbol numeryczny.

Co oznaczają cyfry w numerze PESEL?

Każda z 11 cyfr w numerze PESEL ma swoje znaczenie. Można je podzielić następująco:

RRMMDDPPPPK

RR – to 2 ostanie cyfry roku urodzenia,

MM – to miesiąc urodzenia (zapoznaj się z sekcją „Dlaczego osoby urodzone po 1999 roku mają inne oznaczenie miesiąca urodzenia", która znajduje się poniżej),

DD – to dzień urodzenia,

PPPP – to liczba porządkowa oznaczająca płeć. U kobiety ostatnia cyfra tej liczby jest parzysta (0, 2, 4, 6, 8), a u mężczyzny - nieparzysta (1, 3, 5, 7, 9),

K – to cyfra kontrolna.

Przykład: PESEL 810203PPP6K należy do kobiety, która urodziła się 3 lutego 1981 roku, a PESEL 761115PPP3K - do mężczyzny, który urodził się 15 listopada 1976 roku.

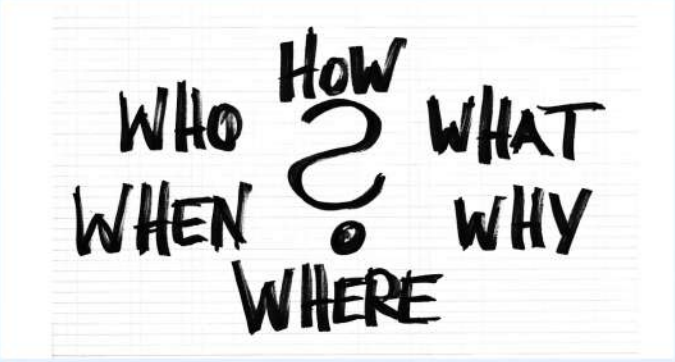
Jak wskazuje ówczesny GIODO: Można więc stwierdzić, że **numer PESEL ex definitione stanowi daną osobową, a jej przetwarzanie podlega wszelkim rygorom przewidzianym w ustawie o ochronie danych osobowych** (https://archiwum.giodo.gov.pl/317/id_art/973/j/pl). Uzyskanie przez osobę trzecią dostępu do naszego numeru PESEL w połączeniu z innymi danymi, jak imię i nazwisko, stwarza **wysokie ryzyko naruszenia praw i wolności osoby fizycznej**. Skutkiem takiej sytuacji może być zaciągnięcie pożyczki na osobę, której numerem PESEL i innymi dodatkowymi danymi dysponuje osoba nieuprawniona.

Zastrzeżenie nr PESEL – od kiedy i w jakim celu?

Z projektu ustawy o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości wynika, że od czerwca 2024 roku każdy będzie mógł zastrzec swój PESEL. Przyjęte założenia mają zapobiegać zaciągnięciom na skradzione dane różnego rodzaju zobowiązań - kredytów i pożyczek oraz otwierania rachunków rozliczeniowych przeznaczonych do wykorzystania w działalności przestępczej. Obecnie to ofiara przestępstwa musi udowodnić, że to nie ona zaciągnęła zobowiązanie. Nowe przepisy zdejmą tę uciążliwość z pokrzywdzonych.

W jaki sposób będzie można zastrzeż nr PESEL?

Elektronicznie: przy wykorzystaniu aplikacji mObywatel
Osobiście: w siedzibie dowolnej gminy, placówce bankowej, SKOK oraz na poczcie.
Rejestr zastrzeżeń prowadzony będzie przez ministra cyfryzacji.



W jaki sposób zastrzeżenie nr PESEL uniemożliwi zaciągnięcie kredytu?

Banki, instytucje kredytowe będą **miały obowiązek weryfikacji zastrzeżenia numeru PESEL** konsumenta przez zawarciem umowy na prowadzenie rachunku bankowego, kredytu, pożyczki i leasingu. Jak wskazał minister cyfryzacji: to na instytucjach finansowych spoczywał będzie obowiązek sprawdzenia, czy dana osoba zastrzegła swój PESEL. Pozwoli to potwierdzić, czy to rzeczywiście ona ubiega się przykładowo o kredyt, czy ktoś się pod nią podszywa. Jeśli numer PESEL będzie zastrzeżony, organ finansowy powinien odmówić dokonania czynności. W przypadku zawarcia takiej umowy, osoba, która zastrzegła numer PESEL, **nie będzie obciążona wynikającymi z niej zobowiązaniami.**
Regulacja ma na celu zablokowanie czynności, co do której posiadacz numeru PESEL nie wyraził zgody poprzez zastrzeżenie swojego numeru PESEL. Jeśli zaś instytucja finansowa nie sprawdzi, czy doszło do zastrzeżenia numeru PESEL a tak faktycznie było - to nie będzie mogła domagać się od konsumenta zaspokojenia roszczenia z tytułu zawarcia takiej umowy, a także zbyć powstałej z niej wierzytelności. Jeśli osoba, której PESEL jest zastrzeżony, faktycznie będzie chciała wziąć kredyt czy pożyczkę, na czas podpisywania umowy będzie musiała cofnąć zastrzeżenie.

Mało tego...

- Notariusze odmówią czynności notarialnej, której przedmiotem będzie nabycie, zbycie lub obciążenie nieruchomości lub udziału w nieruchomości, jeśli numer PESEL strony takiej czynności będzie widniał w rejestrze zastrzeżeń numerów PESEL.
- Operator telekomunikacyjny będzie miał obowiązek zweryfikować zastrzeżenie nr PESEL przed wydaniem duplikatu karty SIM, co ukrócić ma tym samym SIM swapping. **SIM swapping**: duplikowanie kart SIM, w efekcie czego atakujący zyskuje dostęp do powiadomień wysyłanych na telefon ofiary. Skutkuje to ominięciem uwierzytelniania dwuetapowego, realizowanego np. przez kody z wiadomości SMS. Umożliwia to utratę pieniędzy z konta, wyłudzenie danych do logowania do skrzynki mailowej, konta bankowego czy mediów społecznościowych. Metodę **SIM swap** przybliżę w kolejnym wydaniu NEWSLETTERA IOD.

Końcowo, wskazać należy, iż dokonane zastrzeżenie numeru PESEL będzie może zidentyfikować na Gov.pl lub poprzez system zewnętrzny zintegrowany z nowo utworzonym rejestrem zastrzeżeń numerów PESEL.

Autor:
adw. Justyna Jabłonka
Inspektor Ochrony Danych

II. Dane służbowe pracownika. Co wchodzi w ich zakres? Czy można udostępniać takie dane?

W pierwszej kolejności trzeba się zastanowić, **co rozumiemy przez pojęcie „dane osobowe służbowe”?**
Praktyka pokazuje - bo ani kodeks pracy ani też przepisy o ochronie danych osobowych nie wprowadzają kategorii „danych służbowych” - że za **dane osobowe służbowe uznać można: imię i nazwisko, stanowisko, służbowy numer telefonu, służbowy adres email pracownika.**
W zakres danych służbowych nie wchodzi zatem m.in. wizerunek pracownika czy też jego prywatne dane kontaktowe, np. prywatny numer telefonu, adres zamieszkania, prywatny profil na portalu społecznościowym.

Czy służbowe dane pracownika podlegają ochronie?
Tak, tak jak wszystkie inne dane osobowe pracownika.
Dane służbowe, to zwykłe dane osobowe, ale uznaje się, że w związku z faktem, że dane te są ściśle związane z wykonywanymi czynnościami przez pracownika na zajmowanym stanowisku pracy, pracodawca ma uzasadniony interes prawny w tym, aby dane takie przetwarzać, w tym również poprzez ich udostępnienie, np. na stronie internetowej, współpracownikom czy kontrahentom.

PUODO wielokrotnie wskazywał, że przetwarzanie danych służbowych pracownika, a zwłaszcza ich udostępnianie w związku z wykonywanymi przez niego obowiązkami służbowymi, nie wymaga uzyskania uprzedniej zgody tego pracownika. Wykonywanie czynności służbowych przez pracownika, niejednokrotnie wiąże się z koniecznością podejmowania np. kontaktów z osobami trzecimi, instytucjami, urzędami itp. Uniemożliwienie kontaktu z pracownikiem zajmującym określone stanowisko służbowe, mogłoby w niektórych sytuacjach doprowadzić nawet do zagrożenia prawidłowego funkcjonowania pracodawcy.

Jaka jest podstawa prawna przetwarzania przez pracodawcę danych służbowych pracownika?
Podstawą prawną przetwarzania takich danych będzie zatem art. 6 ust. 1 lit f RODO, a więc prawnie uzasadnionym interesie administratora.

Czy współpracownicy mogą udostępniać dane służbowe innych współpracowników?
Jeśli jest to niezbędne do wykonywania zadań służbowych oraz dla zapewnienia prawidłowego funkcjonowania pracodawcy, to tak, mogą.

Często pojawia się również pytanie, co z innymi danymi pracownika, czyli takimi, które nie są danymi służbowymi? Czy takie dane można również udostępniać?
Na gruncie orzeczeń i zaleceń wydawanych przez PUODO, nie ma wątpliwości, że nie znajdujemy podstawy prawnej, która uzasadniałaby powyższe i z dużym prawdopodobieństwem, udostępnienie danych prywatnych pracownika (jego miejsca zamieszkania, prywatnego numeru telefonu, adresu e-mail, numeru PESEL, danych dotyczących zdrowia), może zostać uznane przez PUODO za naruszenie.

A czy współpracownicy mogą między sobą ujawnić dane pracownika, które nie są danymi służbowymi?
W takich sytuacjach, trzeba zachować szczególną ostrożność i podchodzić do każdego zdarzenia indywidualnie.
Czym innym będzie bowiem zwykła rozmowa w gronie znajomych, pomiędzy współpracownikami – i ujawnienie danych osobowych przez osobę (przez pracownika), której dane dotyczą, w celach towarzyskich, a czym innym będzie udostępnienie przez jednego z pracowników danych dotyczących innego pracownika, które posiada w związku z zajmowanym stanowiskiem (np. w związku z pracą w kadrach lub jako przełożony).

Ta druga sytuacja, najczęściej dotyczy danych o zdrowiu i danych o zarobkach. Niejednokrotnie spotykamy się z tym, że pracownicy, w rozmowie między sobą wskazują, dlaczego nie ma kolegi/koleżanki z pracy (jest na L4, ponieważ..., jest nieobecny/nieobecna z powodu sytuacji rodzinnej/choroby członka rodziny ...) bądź ile ktoś zarabia, jaką dostał premię czy podwyżkę.
Takie rozmowy niosą niestety za sobą ryzyko zarzutu nieuprawnionego udostępnienia danych, szczególnie wówczas, kiedy udostępnia je osoba pełniące funkcje kierownicze wobec pracownika, którego dane dotyczą. UODO może uznać, że pracownik ujawniający dane, uzyskał je w związku z pełnieniem funkcji na określonym stanowisku, a skoro tak, jest zobowiązany do zachowania tych danych w poufności.

Ta druga sytuacja, najczęściej dotyczy danych o zdrowiu i danych o zarobkach. Niejednokrotnie spotykamy się z tym, że pracownicy, w rozmowie między sobą wskazują, dlaczego nie ma kolegi/koleżanki z pracy (jest na L4, ponieważ..., jest nieobecny/nieobecna z powodu sytuacji rodzinnej/choroby członka rodziny ...) bądź ile ktoś zarabia, jaką dostał premię czy podwyżkę.

Takie rozmowy **niosą niestety za sobą ryzyko zarzutu nieuprawnionego udostępnienia danych, szczególnie wówczas, kiedy udostępnia je osoba pełniące funkcje kierownicze wobec pracownika, którego dane dotyczą. UODO może uznać, że pracownik ujawniający dane, uzyskał je w związku z pełnieniem funkcji na określonym stanowisku, a skoro tak, jest zobowiązany do zachowania tych danych w poufności.**

Podsumowując.

Dane służbowe pracownika mogą być udostępnianie, albowiem jest to niezbędne dla prawidłowego wykonywania czynności służbowych i prawidłowego funkcjonowania pracodawcy. Do danych tych należą jednak wyłącznie: imię, nazwisko, służbowy numer telefonu oraz służbowy adres e-mail, a także zajmowane stanowisko.

Inne dane pracownika nie są uważane za dane służbowe i co do zasady, powinny zostać zachowane w tajemnicy.

Pracownicy powinni pamiętać, że podejmując zatrudnienie, podpisują zobowiązanie do zachowania danych osobowych w tajemnicy – tj. danych, które uzyskują w związku z pełnieniem zadań służbowych.

Należy zatem z dużą dozą ostrożności ujawniać dane osobowe innych pracowników, nawet wywczas, kiedy dane dotyczą kolegi/koleżanki z pracy, a rozmowa jest zwyczajnie – towarzyska.

Autor:
adw. Justyna Cybulska
Zespół Inspektora Ochrony Danych

III. Osoba zastępująca inspektora ochrony danych. Kim jest osoba zastępująca inspektora ochrony danych i ilu zastępców może mieć inspektor?

Art. 11a ustawy o ochronie danych osobowych przewiduje, że administrator, który wyznaczył IOD, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności. Jej zadaniem jest wykonywanie zadań inspektora w okresie kiedy nie może on wypełniać swoich obowiązków. W czasie nieobecności inspektora do osoby go zastępującej stosuje się odpowiednio przepisy dotyczące inspektora, co oznacza, że w tym czasie osoba ta ma te same obowiązki i uprawnienia, które przysługują inspektorowi.

O ile wyznaczenie inspektora może być obowiązkiem administratora (np. w przypadku administratorów będących pomiotami publicznymi), to decyzja o wyznaczeniu jego zastępcy zawsze należy do administratora. Nawet wtedy, gdy administrator ma obowiązek wyznaczyć inspektora, to nie musi wyznaczać osoby, która będzie go zastępowała. W konkretnych sytuacjach wyznaczenie osoby zastępującej może być jednak wymuszone względami praktycznymi, związanymi z trwającym przez dłuższy czas brakiem możliwości wykonywania obowiązków przez inspektora (np. z uwagi na stan jego zdrowia lub planowany urlop).

Prezes UODO wskazuje, że o ile dany administrator może wyznaczyć tylko jednego inspektora ochrony danych, to dopuszczalne jest, by administrator wyznaczył dwie osoby zastępujące inspektora ochrony danych. W takim przypadku jedna realizowałaby zadania IOD podczas jego nieobecności, a druga wówczas, gdyby w pracy nie było zarówno IOD, jak i tej pierwszej zastępującej go osoby. Wydaje się, że nie ma przeszkód aby administrator wyznaczył nawet większą liczbę osób zastępujących inspektora ochrony danych.

Zastępstwo tylko na czas nieobecności czy na stałe?

Treść art. 11a ustawy o ochronie danych osobowych sugeruje, że zastępcę wyznacza się wyłącznie na czas nieobecności inspektora i że wykonuje on swoje obowiązki wyłącznie w czasie tej nieobecności. Prezes UODO wskazuje jednak, że nie ma przeszkód, aby wyznaczyć stałego zastępcę inspektora, a decyzja czy wyznaczyć stałego zastępcę (bez konieczności wyznaczania i odwoływania podczas poszczególnych nieobecności IOD) czy wyznaczać go doraźnie, jedynie na czas faktycznej nieobecności inspektora, należy do administratora. Jednocześnie Prezes UODO wskazuje, że wyznaczenie osoby zastępującej inspektora na stałe pozwala zapewnić ciągłość wykonywania zadań IOD oraz, że takie rozwiązanie może stanowić realne i ciągłe wsparcie administratora i obsługującego go inspektora. Zgodnie ze stanowiskiem Prezesa UODO osoba zastępująca inspektora może wchodzić w skład zespołu inspektora ochrony danych, którego powołanie może być przydatne z uwagi na rozmiar i strukturę organizacyjną administratora.

W przypadku wyznaczenia osoby zastępującej inspektora ochrony danych na stałe przejmuje ona zadania inspektora w czasie jego nieobecności. Takie przejęcie obowiązków następuje każdorazowo, gdy inspektor ochrony danych nie może wykonywać ich samodzielnie. Nie mają przy tym znaczenia ani przyczyny, ani czas trwania takiej sytuacji. W takim przypadku nie ma potrzeby każdorazowego zawiadamiania Prezesa UODO o przejęciu obowiązków przez osobę zastępującą inspektora czy też o ponownym podjęciu tych obowiązków przez inspektora osobiście.

Jakie wymogi musi spełniać osoba zastępująca inspektora ochrony danych?

Osoba zastępująca musi spełniać takie same wymagania w zakresie kwalifikacji zawodowych, jak inspektor ochrony danych. Oznacza to w szczególności konieczność posiadania przez tę osobę fachowej wiedzy na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań określonych przepisami prawa inspektora ochrony danych. Należy przy tym podkreślić, że o ile przepisy RODO bardzo mocno akcentują wymóg wiedzy i fachowości inspektora i osoby go zastępującej, to nie określają one zasad czy trybu weryfikacji spełnienia tego wymogu.

Co za tym idzie nie ma wymogu posiadania przez osobę zastępującą inspektora ochrony danych określonego wykształcenia, ukończenia kursów czy posiadania konkretnych uprawnień. Z drugiej strony wszelkie certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie danej osoby mogą być ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej przez administratora do pełnienia tej funkcji.

Jak wyznaczyć osobę zastępująca inspektora ochrony danych?

Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. Zasadę tę należy odnieść także do osoby zastępującej inspektora. Nie ma przy tym wymogu aby inspektor ochrony danych i osoba go zastępująca należały do tej samej organizacji.

Również procedura i wymogi formalne związane z wyznaczeniem osoby zastępującej są analogiczne jak w przypadku wyznaczenia inspektora ochrony danych. Wyznaczenie osoby zastępującej inspektora musi nastąpić w sposób formalny. W praktyce oznacza to konieczność wydania odpowiedniego zarządzenia albo podjęcia uchwały w tej sprawie (praktyką jest np. powoływanie inspektora ochrony danych w drodze uchwały przez rady gmin).

W przypadku jednostek samorządu terytorialnego występuje sytuacja wielości administratorów danych. W odniesieniu do różnych kategorii danych osobowych rolę administratora może pełnić jednostka samorządu terytorialnego, jej organ wykonawczy, urząd stanowiący jego aparat pomocniczy i organ uchwałodawczy. W przypadku gmin w roli odrębnych administratorów mogą występować także kierownik urzędu stanu cywilnego i komendant straży gminnej, a w powiecie rzecznik praw konsumentów i powiatowy lekarz weterynarii. Zgodnie ze stanowiskiem prezentowanym przez Prezesa UODO w roli odrębnego administratora danych osobowych może występować także radny, który wykonuje swoje autonomiczne uprawnienia kontrolne, o których mowa w art. 24 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym. Każdy z wymienionych administratorów ma obowiązek wyznaczenia inspektora ochrony danych i ma możliwość wyznaczenia dla niego osoby zastępującej. Wyznaczenie osoby zastępującej inspektora wymaga zgłoszenia Prezesowi UODO. Konieczne jest także dopełnienie obowiązku związanego z opublikowaniem danych kontaktowych

Co za tym idzie nie ma wymogu posiadania przez osobę zastępującą inspektora ochrony danych określonego wykształcenia, ukończenia kursów czy posiadania konkretnych uprawnień. Z drugiej strony wszelkie certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie danej osoby mogą być ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej przez administratora do pełnienia tej funkcji.

Jak wyznaczyć osobę zastępująca inspektora ochrony danych?

Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. Zasadę tę należy odnieść także do osoby zastępującej inspektora. Nie ma przy tym wymogu aby inspektor ochrony danych i osoba go zastępująca należały do tej samej organizacji.

Również procedura i wymogi formalne związane z wyznaczeniem osoby zastępującej są analogiczne jak w przypadku wyznaczenia inspektora ochrony danych. Wyznaczenie osoby zastępującej inspektora musi nastąpić w sposób formalny. W praktyce oznacza to konieczność wydania odpowiedniego zarządzenia albo podjęcia uchwały w tej sprawie (praktyką jest np. powoływanie inspektora ochrony danych w drodze uchwały przez rady gmin).

W przypadku jednostek samorządu terytorialnego występuje sytuacja wielości administratorów danych. W odniesieniu do różnych kategorii danych osobowych rolę administratora może pełnić jednostka samorządu terytorialnego, jej organ wykonawczy, urząd stanowiący jego aparat pomocniczy i organ uchwałodawczy. W przypadku gmin w roli odrębnych administratorów mogą występować także kierownik urzędu stanu cywilnego i komendant straży gminnej, a w powiecie rzecznik praw konsumentów i powiatowy lekarz weterynarii. Zgodnie ze stanowiskiem prezentowanym przez Prezesa UODO w roli odrębnego administratora danych osobowych może występować także radny, który wykonuje swoje autonomiczne uprawnienia kontrolne, o których mowa w art. 24 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym. Każdy z wymienionych administratorów ma obowiązek wyznaczenia inspektora ochrony danych i ma możliwość wyznaczenia dla niego osoby zastępującej. Wyznaczenie osoby zastępującej inspektora wymaga zgłoszenia Prezesowi UODO. Konieczne jest także dopełnienie obowiązku związanego z opublikowaniem danych kontaktowych

osoby zastępującej inspektora ochrony danych. Obowiązek ten można zrealizować zamieszczając imię i nazwisko oraz dane kontaktowe (w szczególności adres poczty elektronicznej lub numer telefonu) osoby zastępującej inspektora na stronie internetowej administratora. Podmioty zobowiązane do prowadzenia własnych stron Biuletynu Informacji Publicznej powinny zamieścić wskazane informacje na stronie Biuletynu. Jeżeli administrator nie prowadzi własnej strony, powinien udostępnić wskazane informacje w sposób ogólnie dostępny w miejscu prowadzenia działalności. Do osoby zastępującej powinny też znaleźć zastosowanie wytyczne Grupy Roboczej art. 29, które zalecają, aby w ramach dobrej praktyki poinformować o imieniu, nazwisku i danych kontaktowych inspektora pracowników administratora. Dane te mogą zostać udostępnione wewnętrznie np. poprzez intranet, w wewnętrznej książce telefonicznej albo w ramach rozpisanej struktury organizacyjnej.

Obowiązki i niezależność zastępcy inspektora ochrony danych

W czasie nieobecności inspektora ochrony danych osoba zastępująca wykonuje wszystkie jego obowiązki. Do jej zadań należy wówczas w szczególności: informowanie o obowiązkach związanych z przetwarzaniem danych osobowych i doradzanie co do sposobu ich wypełniania; monitorowanie przestrzegania przepisów o ochronie danych; działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania; prowadzenie audytów; współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych.

Przy wykonywaniu swoich obowiązków osoba zastępująca inspektora danych osobowych korzysta z tych samych gwarancji niezależności, które przepisy RODO przyznają inspektorowi.

Oznacza to m.in., że w strukturze organizacyjnej administratora osoba zastępująca inspektora może podlegać tylko najwyższemu kierownictwu administratora i powinna mieć zapewnione instrumenty niezbędne do wykonywanie swoich obowiązków. W szczególności istotne jest zapewnienie jej dostępu do informacji i dokumentów pozwalających na monitorowanie prawidłowości procesów przetwarzania danych.

Przepisy o ochronie danych osobowych nie rozstrzygają relacji pomiędzy inspektorem ochrony danych a osobą go zastępującą, niemniej wydaje się, że w naturalny sposób musi tu występować podporządkowanie, tak by zapewnić spójność wykonywania określonych prawem obowiązków inspektora.

Autor:
dr r. pr. Grzegorz Lubeńczuk
Zespół Inspektora Ochrony Danych

IV. Czy zawarcie umowy powierzenia to za mało aby wykazać, iż administrator sprawdził czy Procesor działa zgodnie z RODO? Praktyczne zastosowanie Ankiety oceny spełnienia wymagań dotyczących ochrony danych osobowych.

Aby odpowiedzieć na to pytanie, wskazać należy na art. 28 ust. 1 RODO, z którego wynika:
Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, **korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.**

Istotą tej konstrukcji jest zlecenie przez administratora **wybranemu podmiotowi** dokonania określonych czynności przetwarzania, w imieniu i na rzecz administratora. Podkreślić jednak należy, iż administrator w celu powierzenia danych musi dokonać **wyboru właściwego podmiotu przetwarzającego.**

W piśmiennictwie przedmiotu wskazuje się, że badanie, czy podmiot przetwarzający spełnia wymogi określone w art. 28 ust. 1 rozporządzenia 2016/679, może w praktyce być realizowane **poprzez uzyskanie odpowiedzi na kwestionariusz pytań**, dotyczących kwestii stosowania odpowiednich środków technicznych i organizacyjnych zapewniających zgodność działań podmiotu przetwarzającego z przepisami, przekazywany przez administratora, natomiast na etapie zawierania z podmiotem przetwarzającym umowy powierzenia nie ma obowiązku prowadzenia audytu stosowanych przez procesora środków (por. P. Barta, M. Kawecki, P. Litwiński, Komentarz do art. 28, teza 1 [w:] Ogólne rozporządzenie o ochronie danych..., red. P. Litwiński, s. 314).
Obowiązki podmiotu przetwarzającego w zakresie odpowiednich środków technicznych i organizacyjnych zostały uregulowane w art. 32 rozporządzenia, w którym to przepisie wskazano, że środki te powinny zapewnić stopień bezpieczeństwa odpowiadający ryzyku, jakie wiąże się z przetwarzaniem danych.

Czy weryfikacja podmiotu przetwarzającego powinna zostać przeprowadzona przez administratora przed rozpoczęciem współpracy z podmiotem przetwarzającym, w jej trakcie czy może samo podpisanie umowy powierzenia jest wystarczające aby podmiot ten zweryfikować?

Prezes UODO zwrócił uwagę, iż weryfikacja podmiotu, tj. sprawdzenie czy daje on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO powinno odbyć się **przed rozpoczęciem z tym podmiotem współpracy.**

Jakimi narzędziami może posłużyć się administrator do przeprowadzenia weryfikacji podmiotu przetwarzającego?

Pierwszym elementem procesu weryfikacji podmiotów, którym mamy zamiar powierzyć dane może być ankieta, w której administrator skieruje do podmiotu przetwarzającego zestaw pytań dotyczących stosowanych zabezpieczeń.
Kiedy administrator powinien przesłać ankietę/zestaw pytań do podmiotu przetwarzającego?
Dobrą praktyką jest dołączenie ankiety do dokumentów, które są wymagane od oferentów w związku z przeprowadzaniem postępowania w trybie zamówień publicznych czy zapytań ofertowych bądź po prostu przesłanie jej do wypełnienia przed podpisaniem umowy głównej, umowy powierzenia danych.

Przykładowy zestaw pytań do wykorzystania przez administratora w ankiecie oceny spełnienia wymagań dotyczących ochrony danych osobowych:

1. Czy w organizacji została wdrożona dokumentacja dotycząca ochrony danych osobowych? Jeżeli tak, proszę wskazać jaka konkretnie?
2. Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?
3. Czy każdy z pracowników dopuszczonych do przetwarzania danych osobowych ma obowiązek zapoznać się z polityką ochrony danych i z innymi procedurami wdrożonymi w organizacji z zakresu ochrony danych, przed przekazaniem mu dostępu do danych?
4. Czy w organizacji są przeprowadzane cykliczne szkolenia dla pracowników z zakresu prawidłowego przetwarzania danych osobowych?
5. Czy podmiot przetwarzający prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania?
6. Czy podmiot przetwarzający dokonuje systematycznej analizy ryzyka?
7. Czy podmiot przetwarzający powołał Inspektora Ochrony Danych, a jeśli nie, to czy posiada w swoich strukturach stanowisko, które odpowiada za nadzór nad obszarem ochrony danych osobowych?
8. Czy podmiot przetwarzający wdrożył procedurę dotyczące sposobu działania w przypadku wystąpienia incydentu naruszenia danych osobowych oraz umożliwiające realizację praw osób, których dane osobowe dotyczą?
9. Czy podmiot przetwarzający nadaje pracownikom upoważnienia do przetwarzania danych osobowych?
10. Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych zostali zobowiązani do zachowania ich w tajemnicy?
11. Czy podmiot przetwarzający wprowadził pracę zdalną w swoje organizacji? Jeśli tak, czy wprowadził również Regulamin ochrony danych w pracy zdalnej, do którego stosowania zobowiązują się pracownicy?
12. Czy podmiot przetwarzający sprawdza stan zabezpieczeń pod względem ochrony danych osobowych innych podmiotów/podwykonawców, z którymi podejmuje współpracę?
13. Czy podmiot przetwarzający zadbał, aby dostęp do danych osobowych miały tylko osoby ku temu upoważnione, tym samym czy zastosowane zostały zabezpieczenia przez dostępem osób trzecich? Jeśli tak, jakie zabezpieczenia zostały zastosowane?
14. Czy podmiot przetwarzający wykonuje kopie zapasowe? Jeśli tak, to z jaka częstotliwością oraz gdzie są one przechowywane?
15. Czy podmiot przetwarzający dopuścił do użytkowania przez pracowników służbowe nośniki zewnętrzne i czy są one szyfrowane?

Wskazać należy, iż w/w pytania są pytaniami przykładowymi. Warto, aby każdorazowo ankieta i zawarte w niej pytania korespondowały ze sposobem, w jaki dany podmiot przetwarzający zamierza przetwarzać przekazane przez administratora dane i w jaki sposób usługa będzie wykonywana.

Należy pamiętać, że podmiot przetwarzający udzielający odpowiedzi na pytania nie tylko powinien odpowiadać zgodnie ze stanem faktycznym, ale powinien również posiadać dokumentację, która pozwoli mu wykazać, iż faktycznie jest tak, jak twierdzi.

Wymóg określony art. 28 ust. 1 rozporządzenia 2016/679 bezwzględnie obowiązuje bowiem każdego administratora danych, który w ramach prowadzonej działalności korzysta z zasobów lub usług podmiotu przetwarzającego podczas przetwarzania danych osobowych. **Samo podpisanie umowy powierzenia przetwarzania danych osobowych bez dokonania odpowiedniej oceny podmiotu przetwarzającego nie może być uznane jako realizacja obowiązku przeprowadzenia postępowania weryfikującego podmiot przetwarzający pod kątem spełnienia przez niego wymogów rozporządzenia 2016/679.** Z obowiązku przeprowadzenia takiej oceny nie zwalnia również fakt wieloletniej współpracy i korzystania z usług danego podmiotu przetwarzającego przed dniem 25 maja 2018 r., tj. przed rozpoczęciem stosowania rozporządzenia 2016/679. (Decyzja PUODO z 19.01.2022 r., DKN.5130.2215.2020, LEX nr 3313623).

Autor:
adw. Justyna Jabłonka
Inspektor Ochrony Danych

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