Biblioteka ODOeksperta

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

PRAKTYCZNY PORADNIK DLA ADMINISTRATORÓW DANYCH

TOMASZ SIEŃKOWSKI

Stan prawny: grudzień 2019

Autor: Tomasz Sieńkowski, prawnik w zespole kancelarii „ODOekspert".

Wydawca: „ODOekspert" Kancelaria Radcy Prawnego Jakub Wezgraj, siedziba główna: ul. Prosta 69, 00-838 Warszawa

Niniejsza książka stanowi materiał promocyjny „ODOekspert" Kancelarii Radcy Prawnego Jakuba Wezgraja.

Wydanie 1

Spis treści

I. Poufność oraz przetwarzanie danych osobowych na polecenie administratora

Powszechnie obowiązujące przepisy o ochronie danych osobowych bardzo silnie akcentują zasadę poufności danych. Oznacza to między innymi, że każdy administrator danych powinien stać na straży tego, by do przetwarzania danych osobowych dopuszczone były wyłącznie osoby przez niego upoważnione. Każda bowiem inna osoba uzyskująca dostęp do danych osobowych jako nieupoważniona naruszałaby przymiot poufności danych.

Czym jest jednak to upoważnienie? Jaką powinno mieć formę? Jak powinien wyglądać sam proces jego nadawania?

Na te oraz inne pytania odpowiedź znajdziesz w niniejszym poradniku.

Jedną z podstawowych zasad przetwarzania danych osobowych jest zasada poufności danych. Reguła ta jest interpretowana szeroko, jednak samo pojęcie „poufności" można rozumieć intuicyjnie – jako przymiot gwarantujący, że dane osobowe nie dostaną się w „niepowołane ręce". Zgodnie ze znaczeniem językowym zamieszczonym w Słowniku Języka Polskiego, termin „poufny" oznacza „udostępniany tylko niewielu osobom, wymagający dyskrecji". Natomiast według standardów ISO poufność to właściwość polegająca na tym, że informacja nie jest udostępniania ani ujawniana nieautoryzowanym osobom lub procesom.

Analizując znaczenie poufności dla przetwarzania danych osobowych warto przypomnieć, że w rozumieniu przepisów RODO naruszeniem ochrony danych jest między innymi każde przypadkowe lub niezgodne z prawem ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

PRZYKŁAD

Naruszeniem poufności danych może być między innymi:

- dostęp do zasobów zapisanych na dyskach twardych laptopów w wyniku kradzieży laptopa, bądź jego utraty w innych okolicznościach (np. zgubienia, pozostawienia w miejscu publicznym);
- przesłanie na błędny adres e-mail wiadomości z załącznikiem stanowiącym plik z zestawieniem danych osobowych.

Jedną z zasadniczych właściwości, która stanowi środek bezpieczeństwa natury organizacyjnej jest dopuszczanie do przetwarzania danych osobowych wyłącznie osób uprzednio upoważnionych przez administratora danych.

Co na ten temat mówią przepisy? Porównajmy regulacje aktualnie obowiązujące, a także te które obowiązywały wcześniej.

RODO	**Dyrektywa 95/46/WE** *(nieobowiązująca)*	**Ustawa o ochronie danych osobowych z 1997 r.** *(nieobowiązująca)*
Artykuł 29	Artykuł 16	Artykuł 37
Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.	Żadna osoba działająca z upoważnienia administratora danych lub przetwarzającego, włączając samego przetwarzającego, który ma dostęp do danych osobowych, nie może przetwarzać ich bez polecenia administratora danych, chyba że wymaga tego prawo.	Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Jeszcze przed rozpoczęciem stosowania RODO (tj. przed 25 maja 2018 r.) istniały precyzyjne regulacje odnoszące się do przedmiotowej kwestii. W art. 37 nieobowiązującej już ustawy o ochronie danych osobowych z 1997 r. znajdowało się postanowienie stanowiące, że: *„do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych"*. Na gruncie RODO nie ma natomiast analogicznego przepisu, który bezpośrednio wskazywałby na konieczność nadawania upoważnień przez administratora, jednak obowiązek taki wyprowadzany jest m. in. z art. 29, który wskazuje na możliwość przetwarzania danych przez podmiot przetwarzający lub osobę działającą, z upoważnienia administratora (mających dostęp do danych osobowych) wyłącznie na polecenie administratora, chyba że wymagają tego przepisy prawa. W dalszej części RODO znajdziemy zapis, który pozostaje w ścisłym związku z art. 29. Treść art. 32 ust. 4 RODO mówi, iż administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu

przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymagają tego właściwe przepisy prawa. Zatem treść art. 32 ust. 4 rozumieć należy jako obowiązek podjęcia działań w celu realizacji obowiązku, o którym mowa w art. 29 RODO.

Dlatego mówiąc o osobach działających z upoważnienia administratora - nieodłącznym elementem staje się konieczność uprzedniego udzielenia tym osobom upoważnienia do przetwarzania danych, które precyzyjnie wskazywałoby zakres uprawnień do przetwarzania danych – dokonywanych na polecenie administratora.

WNIOSKI

Warto pamiętać, że:

- zgodnie z zasadą rozliczalności administrator powinien umieć wykazać, iż zapewnił odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa przetwarzanych danych, w tym w zakresie ich poufności;
- przed dopuszczeniem osoby do wykonywania obowiązków związanych z przetwarzaniem danych osobowych, administrator lub podmiot przetwarzający (np. pracodawca) upoważnia poszczególne osoby do przetwarzania danych osobowych zgodnie z jego instrukcjami (na jego polecenie).

II. Co z ewidencją osób upoważnionych?

Na gruncie nieobowiązującej już ustawy o ochronie danych osobowych w art. 39 administrator danych zobowiązany był do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, która zawierała: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych; a także identyfikator (jeżeli dane przetwarzane były w systemie informatycznym). Czy można zatem przyjąć, że w związku z wejściem w życie RODO obowiązek jej prowadzenia ustał?

Wśród obligatoryjnych elementów dokumentacji przetwarzania danych przewidzianych w RODO (wśród których można znaleźć m. in. rejestr czynności przetwarzania danych czy rejestr naruszeń ochrony danych) nie znajdziemy ewidencji nadanych upoważnień. Jednak Prezes Urzędu Ochrony Danych w wytycznych dotyczących dokumentacji przetwarzania danych wskazał, że przygotowując dokumentację, której celem jest wykazanie zgodności przetwarzania danych z wymaganiami określonymi w RODO, należy zweryfikować dotychczasowe elementy stosowanej dokumentacji w tym m. in. ewidencji prowadzonych upoważnień do przetwarzania danych, czy uprawnień do poszczególnych funkcji użytkowanych systemów informatycznych.

WNIOSKI

Przyjąć zatem należy, że prowadzenie ewidencji jest całkowicie fakultatywne, natomiast może ona stanowić pomocne narzędzie w wymiarze organizacyjnym.

Nowelizacja poprzedniej ustawy o ochronie danych osobowych obowiązująca od dnia 1 stycznia 2015 r. wprowadziła zasadnicze zmiany w zakresie wymagań wobec osób zainteresowanych pełnieniem funkcji Administratora Bezpieczeństwa Informacji (ABI). Jednakże w obowiązujących przed nowelą przepisach ustawy była ona uregulowana w sposób wyjątkowo lakoniczny. Jedynie treść obowiązującego wówczas art. 36 ust. 3 wskazywała, że administrator danych wyznacza Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony danych osobowych, o których mowa w art. 36 ust. 1 Ustawy, chyba że sam zamierza wykonywać te czynności.

III. Jakie elementy powinno uwzględniać upoważnienie do przetwarzania danych osobowych?

Obecnie nie ma konkretnych regulacji co do tego jakie elementy powinno obejmować upoważnienie. Mając na względzie obligatoryjne elementy ewidencji osób upoważnionych do przetwarzania danych przewidzianej w art. 39 nieobowiązującej ustawy o ochronie danych osobowych, na zasadzie analogii można wywnioskować, że przed wejściem w życie przepisów RODO zakres upoważnienia wyznaczały informacje z przedmiotowej regulacji (przytoczone w punkcie 2 powyżej).

Zasadnym wydaje się jednak rozszerzenie zakresu wydanego upoważnienia m. in. poprzez zawarcie informacji o:

- konkretnym zbiorze danych osobowych lub zakresie danych osobowych, do którego dostęp ma uzyskać osoba (np. jeśli osoba ma być odpowiedzialna wyłącznie za telefoniczny kontakt z klientami: dane klientów danego podmiotu);
- nazwie systemu informatycznego (oraz zakresu uprawnień), do którego ma uzyskać dostęp osoba (jeżeli przetwarzanie odbywać się będzie elektronicznie z wykorzystaniem poszczególnych systemów informatycznych);
- osobie wydającej upoważnienie.

WZÓR UPOWAŻNIENIA

Przykładowy wzór upoważnienia może wyglądać następująco:

[*data nadania upoważnienia*]

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

w [*pełna nazwa podmiotu*]

Osoba, której nadawane jest upoważnienie do przetwarzania danych osobowych:

.....

[*imię i nazwisko / stanowisko lub funkcja*]

Dane osobowe objęte zbiorem o nazwie / Dane osobowe w zakresie:

Przetwarzane w formie elektronicznej:

[ ] TAK [ ] NIE

z wykorzystaniem systemów informatycznych:

nazwa systemu	zakres uprawnień systemowych

Uzasadnienie/uwagi: [*wszelkie potencjalne uwagi lub informacje*]

Okres na jaki nadano upoważnienie: [*konkretny okres, bądź ramy czasowe*]

Osoba wydająca upoważnienie (bezpośredni przełożony)

[*podpis*]

IV. Procedura nadawania upoważnień – o czym warto pamiętać?

Szczególnie w dużych organizacjach niezwykle przydatna może okazać spójna i przejrzysta procedura postępowania w zakresie nadawania upoważnień, która może regulować poszczególne czynności i kroki jakie należy podjąć np. w przypadku nowozatrudnionego pracownika. Warto przewidzieć wszelkie okoliczności, które mogą być charakterystyczne dla danego podmiotu związane m. in. ze strukturą organizacyjną, zakresem odpowiedzialności, infrastrukturą informatyczną czy właściwością kanałów komunikacji, aby jak najbardziej zminimalizować ryzyko przetwarzania danych osobowych przez osoby do tego nieupoważnione.

1. Kto nadaje upoważnienie?

To administrator danych jest podmiotem praw i obowiązków wynikających z przepisów RODO. W przypadku spółek prawa handlowego to organ zarządzający (jako całość) będzie odpowiadał z tytułu ewentualnych naruszeń (zgodnie z charakterystyką danej spółki). Kompetencje w zakresie nadawania upoważnień mogą zostać nadane umocowanym osobom działającym w imieniu administratora m. in. członkowie zarządu, kierownicy działu kadr itp.

W procedurze warto także uwzględnić osoby przełożone lub osoby na stanowiskach kierowniczych poszczególnych komórek organizacyjnych, które odpowiedzialne będą za wnioskowanie o nadanie lub zmianę zakresu upoważnienia do przetwarzania danych osobowych.

2. Upoważnienie indywidualne czy zbiorcze?

Musimy pamiętać o tym, że aktualnie nie obowiązują żadne regulacje jak również wytyczne polskiego organu nadzoru w zakresie tego czy upoważnienia do przetwarzania danych mogą być udzielane „zbiorczo" (np. wszystkim osobom zatrudnionym na danym stanowisku – w analogicznym zakresie) czy też każdorazowo - indywidualnie. Jest to zagadnienie dyskusyjne, często zależne od struktury danej organizacji. Jednakże indywidualne przydzielanie upoważnień do przetwarzania danych osobowych może mieć zasadnicze znaczenie dla celów dowodowych wobec zasady rozliczalności przetwarzania danych, a także wymogów

art. 29 RODO (który odnosi się do działania „z upoważnienia administratora"), związanych m.in. z koniecznością wykazania precyzyjnego zakresu upoważnienia czy wskazania okresu przez które obowiązywało. Bez wątpienia jednym z podstawowych standardów związanych z zapewnieniem poufności danych osobowych oraz rozliczalności prowadzonych na nich operacji jest zapewnienie dostępu do danych osobowych na poziomie indywidualnym. Z tego też względu nadawanie upoważnień indywidualnych („imiennych") ze wskazaniem konkretnego zakresu danych osobowych, do którego osoba upoważniania uzyskuje prawo dostępu, jest rozwiązaniem zdecydowanie zalecanym.

3. W jakim momencie należy nadać upoważnienie?

Niezwykle istotne jest to, by osoba, która przystępuje do wykonywania obowiązków służbowych, które wiążą się z przetwarzaniem danych osobowych miała już wydane upoważnienie. Tym samym upoważnienie do przetwarzania danych osobowych należy wydawać **przed rozpoczęciem wykonywania czynności związanych z ich przetwarzaniem**.

Zatem konieczne jest wcześniejsze ustalenie i skonkretyzowanie:

- do jakich danych osobowych (zbiorów danych) powinna mieć dostęp osoba zatrudniona na danym stanowisku?
- obsługa jakich systemów informatycznych (służących do przetwarzania danych osobowych) będzie niezbędna do wykonywania obowiązków służbowych na danym stanowisku?

Dopiero wówczas będzie można sprawnie określić zakres konkretnego upoważnienia do przetwarzania danych osobowych.

4. Jak określić okres na jaki ma zostać udzielone upoważnienie?

Również i w tym zakresie nie ma konkretnych regulacji czy wytycznych. Zatem wskazane mogą być konkretne okresy czasu liczone, np. w miesiącach, jednakże pamiętać należy, że w przypadku wygaśnięcia upoważnienia uzyskiwanie dalszego dostępu do danych osobowych stanowi faktycznie naruszenie ochrony danych osobowych, ponieważ osobę, której

wygasło upoważnienie należałoby traktować jako nieuprawnioną do dostępu do danych osobowych.

Zalecanym jest zatem rozwiązanie oparte na zasadzie nadawania upoważnień na czas zatrudnienia / współpracy na danym stanowisku lub na czas realizacji zleconych czynności.

5. W jaki sposób następuje odwołanie udzielonego upoważnienia?

Sposób odwoływania upoważnień do przetwarzania danych osobowych powinien być określony przez administratora danych w postaci wewnętrznej procedury (jako element procedury nadawania, aktualizacji i odbierania upoważnień). W tego typu procedurze można na przykład przyjąć, że w przypadku potrzeby odwołania upoważnienia przed upływem okresu, na jaki zostało wydane, działająca w imieniu administratora osoba (umocowana do udzielania upoważnień) odwołuje upoważnienie na wniosek przełożonego osoby, której upoważnienie podlega odwołaniu, wskazując jednocześnie powód wymagający odwołania (np. brak dalszej potrzeby uzyskiwania dostępu do danych osobowych przez pracownika).

W przypadku odwołania upoważnienia należy dopilnować, by osobie, której odwołuje się upoważnienie, faktycznie odebrano dostępy do dokumentacji papierowej, na której zapisane są dane osobowe, ale również do systemów informatycznych oraz zasobów IT (np. dysków sieciowych), które służą do przetwarzania danych osobowych.

6. Forma nadawanych upoważnień w świetle ustawy nowelizującej przepisy sektorowe

Przepisy RODO w żadnym miejscu nie wskazują konkretnej formy w jakiej upoważnienie ma być wydane. Motyw 15 RODO wskazuje ponadto, że ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik. Regulacja ta pozostawia zatem administratorowi swobodę co do wyboru środków i metod, które zostaną zastosowane do realizacji poszczególnych celów i wymagań związanych z zapewnieniem należytego bezpieczeństwa przetwarzanych danych.

Czy można więc uznać, że upoważnienie może być wydawane zarówno w formie tradycyjnej (tj. papierowej) jak i elektronicznej? W tym miejscu warto przyjrzeć się treści ustawy dostosowującej polskie ustawodawstwo do wymagań RODO z dnia 21 lutego 2019 r.[1] Dokonała ona wielu zmian w przepisach sektorowych w zakresie zasad przetwarzania danych osobowych. Co jednak istotne z punktu widzenia omawianego tematu – dokonała nowelizacji kilkudziesięciu ustaw poprzez zobowiązanie administratora do pisemnego upoważnienia osób dopuszczonych do przetwarzania danych.

Zmiany objęły m. in. przepisy prawa pracy (w tym zagadnień związanych z ZFŚS):

Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy	Art. 22[1]b § 3	Do przetwarzania danych osobowych, o których mowa w § 1 (danych wrażliwych z art. 9 ust. 1 RODO), mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.
Ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych	art. 8 ust. 1b	Do przetwarzania danych osobowych dotyczących zdrowia, o których mowa w art. 9 ust. 1 RODO, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

Wątpliwość jednak budzi użyte sformułowanie „pisemnego upoważnienia". Zarówno w treści RODO, jak i ustawy o ochronie danych osobowych z 2018 r., a także w ustawach, w których sformułowanie to ostatecznie zostało wprowadzone, nie znajdziemy definicji „formy pisemnej". Wobec tego można sięgnąć do orzeczenia Sądu Najwyższego, który w wyroku z dn. 29 września 2004. (sygn. II CK 527/03) uzasadnił, że dokumentem wykazującym iż czynność została dokonana, **może być każdy dokument**, którego treść bezpośrednio lub pośrednio wskazuje na fakt dokonania czynności. Mając na uwadze brak innych wytycznych ustawodawcy, na ten moment przyjąć można, iż dopuszczalną formą wydawania upoważnień jest taka, która

[1] Właściwy tytuł ustawy to: ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. z 2019 r. poz. 730.

przyjmuje formę dokumentu („papierowego" lub elektronicznego), co do której nie można mieć wątpliwości, że jest wyrazem woli udzielającego upoważnienia w stosunku do osoby upoważnianej[2].

Innymi słowy należy przyjąć, że upoważnienia do przetwarzania danych osobowych **mogą być wydawane zarówno w formie papierowej jak i elektronicznej**, ponieważ w obu przypadkach formę tą należy uznać za „pisemną" (treść upoważnienia zostanie udokumentowana na piśmie).

WNIOSKI

Istotne jest aby faktyczna czynność udzielenia upoważniania (zmaterializowana w formie „papierowej" lub w formie elektronicznej) pozwalała wykazać: kogo ono dotyczy, jaki zakres danych osobowych obejmuje, na jaki okres i przez kogo zostało wydane. Zgodnie z zasadą rozliczalności administrator powinien umieć wykazać, iż:

- zapewnił odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa przetwarzanych danych, w tym w zakresie ich poufności, oraz że
- wypełnił nałożony na niego obowiązek upoważnienia osoby przetwarzającej dane osobowe na jego polecenie.

7. Zobowiązanie do zachowania danych w tajemnicy

Niektóre akty prawne, które zostały znowelizowane w związku z wejściem w życie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO, znalazło się między innymi postanowienie: „*Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy*". Poza upoważnieniem, o którym mowa wcześniej zmiana generuje kolejny bezwzględny obowiązek, którego forma nie została bezpośrednio wskazana. Również i w tym przypadku posłużyć się należy względami praktycznymi w perspektywie ciążącej na administratorze zasady rozliczalności – poprzez

[2] Niniejsze stanowisko zostało także potwierdzone w wystąpieniu UODO z dn. 29 listopada 2019 r., w którym wskazano, że: *„nadawanie upoważnień w postaci elektronicznej należy uznać za wykonanie obowiązku nadania upoważnień w formie pisemnej"*.

takie odebranie oświadczenia od upoważnianej osoby, które nie będzie budziło żadnych wątpliwości co do jego treści.

Nie ma przeciwskazań co do tego, by takim samym obostrzeniem objąć wszystkie osoby, które administrator upoważnił do przetwarzania danych osobowych. Również i w tym miejscu sięgnąć można do treści ustawy o ochronie danych osobowych z 1997 r., która w art. 39 ust. 2 zawierała zbliżoną regulację o następującej treści: „*Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia*". Zwłaszcza należy mieć na uwadze art. 28 RODO, który w ust. 3 lit. b) zobowiązuje podmiot przetwarzający dane osobowe do zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.

WZÓR OŚWIADCZENIA

Przykładowy wzór oświadczenia rozszerzony o dodatkowy element - zapoznania się z obowiązującymi w danej organizacji regulacjami wewnętrznymi, może wyglądać następująco:

.....
[*imię i nazwisko*]

.....
[*stanowisko lub funkcja*]

OŚWIADCZENIE

Oświadczam, że zapoznałem/am się z obowiązującymi w zakresie ochrony danych osobowych regulacjami wewnętrznymi w [*pełna nazwa organizacji*], a także wymaganiami wynikającymi z obowiązujących w tym zakresie przepisów prawa oraz zobowiązuję się do ich stosowania.

Jestem świadomy/a obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu lub wygaśnięciu upoważnienia do przetwarzania danych osobowych.

.....
[*miejscowość i data*]

.....
[*czytelny podpis*]

odoekspert

Kancelaria Radcy Prawnego Jakub Wezgraj

Siedziba główna:

ul. Prosta 69, 00-838 Warszawa

www.odoekspert.pl

ISBN 978-83-946339-1-2