SPIS TREŚCI

Aktualności

Ochrona danych osobowych

Dostęp do informacji publicznej

Tajemnice ustawowo chronione

Rada Programowa:

dr *Mariusz Bidziński* – Uniwersytet SWPS w Warszawie
Maciej Byczkowski – Prezes firmy ENSI, Prezes Zarządu Stowarzyszenia Administratorów Bezpieczeństwa Informacji
dr hab. *Paweł Fajgielski* – prof. Katolickiego Uniwersytetu Lubelskiego Jana Pawła II
prof. dr hab. *Stanisław Hoc* – Uniwersytet Opolski
dr hab. *Mariusz Krzysztofek* – Director, Privacy Counsel – EMEA, Herbalife
dr *Paweł Litwiński* – Instytut Allerhanda
doc. dr *Arwid Mednis* – Wydział Prawa i Administracji Uniwersytetu Warszawskiego
prof. nadzw. dr hab. *Maciej Rogalski* – Uczelnia Łazarskiego w Warszawie
dr *Grzegorz Sibiga* – Instytut Nauk Prawnych Polskiej Akademii Nauk
dr *Piotr Sitniewski* – Prezes Fundacji JAWNOSC.PL, prowadzący portal jawnosc.pl i www.jawnoscsamorzadu.pl, Krajowa Szkoła Administracji Publicznej
dr hab. *Przemysław Szustakiewicz* – Prof. Uczelni Łazarskiego w Warszawie
dr hab. *Sławomir Zalewski* – Prof. Wyższej Szkoły Policji w Szczytnie
dr hab. inż. *Janusz Zawiła-Niedźwiecki*, prof. PW, dziekan Wydziału Zarządzania Politechniki Warszawskiej

Redakcja:

Redaktor naczelna:
r. pr. Marcin Lewoszewski
Redaktor prowadząca:
Julia Augustynowicz
Wydawca:
Patryk Janiak

Skład i łamanie: DTP Service
Druk i oprawa: Interdruk, Warszawa

Cena: 110 zł w tym 5% VAT

informacja W ADMINISTRACJI PUBLICZNEJ

Wydawnictwo C.H.Beck
00-203 Warszawa, ul. Bonifraterska 17
e-mail: informacjawadministracji@beck.pl
www.czasopisma.beck.pl

UWAGA: Opinie zawarte w niniejszym kwartalniku wyrażają osobisty punkt widzenia Autorów. Wydawnictwo C.H.Beck nie ponosi odpowiedzialności za zawarte w nim informacje.

Kamila Kędzierska
Redaktor naczelna

Szanowni Państwo,

W nowym numerze kwartalnika „Informacja w Administracji Publicznej" ponownie podejmujemy temat reformy ochrony danych osobowych związanych z Ogólnym rozporządzeniem o ochronie danych osobowych (RODO), starając się odpowiedzieć na liczne pytania, które pojawiły się w pierwszych miesiącach stosowania nowych przepisów. W pierwszej kolejności prezentujemy artykuł szczegółowo omawiający problematykę realizacji obowiązku informacyjnego, o którym mowa w art. 13 RODO. Nasi Autorzy przedstawiają także najważniejsze informacje dotyczące wprowadzenia i funkcjonowania monitoringu wizyjnego w szkole i urzędzie, z punktu widzenia przepisów o ochronie danych osobowych. W zakresie ochrony danych osobowych w ramach funkcjonowania placówek oświatowych prezentujemy również omówienie odnoszące się do publikowania zdjęć uczniów na stronach internetowych, natomiast w odniesieniu do funkcjonowania wszystkich jednostek sektora finansów publicznych – wpływ przepisów RODO na prowadzenie postępowań o udzielenie zamówienia publicznego. W celu ułatwienia stosowania omawianych przepisów nasi Autorzy przygotowali dla Państwa przydatne wzory dokumentów, wraz z praktycznym omówieniem – w zakresie dokumentacji ochrony danych osobowych według RODO.

Omawiając problematykę dostępu do informacji publicznej prezentujemy informacje dotyczące projektu nowej dyrektywy unijnej o ponownym wykorzystaniu informacji sektora publicznego, standardów, które należy zachować przy otwieraniu danych publicznych, a także zakresu stosowania przepisów Kodeksu postępowania administracyjnego w ramach udostępniania informacji. Aby ułatwić praktyczne zastosowanie przepisów, przekazujemy wskazówki dotyczące wzywania do podpisania wniosku o udostępnienie informacji publicznej, jak również schemat wspomagający udzielenie odpowiedzi na pytanie o przypadki, kiedy dokument wewnętrzny nie podlega udostępnieniu.

Prezentujemy ponadto obszerne uwagi dotyczące coraz częściej pojawiającego się problemu – zastrzeżenia informacji jako tajemnicy przedsiębiorstwa w ramach postępowania o udzielenie zamówienia publicznego, szczególnie w kontekście dyrektywy 2016/943. Podmioty zainteresowane uruchomieniem systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych międzynarodowych znajdą natomiast schemat obrazujący niezbędne czynności przygotowawcze wraz z przystępnym komentarzem.

Tradycyjnie publikujemy odpowiedzi na pytania Czytelników, odnoszące się m.in. do prawidłowego sposobu prowadzenia listy obecności po rozpoczęciu stosowania RODO, udostępniania informacji o wynagrodzeniach pracowników powiatowych urzędów pracy oraz stosowania urządzeń teleinformatycznych w kontekście sporządzania i przechowywania informacji niejawnych.

Mając nadzieję na zainteresowanie omawianą problematyką zachęcam do przesyłania do redakcji pytań odnoszących się do nurtujących Państwa kwestii.

Kamila Kędzierska

Wywiad przeprowadzony z dr *Maciejem Kaweckim* – Dyrektorem w Departamencie Zarządzania Danymi w Ministerstwie Cyfryzacji

Panie Dyrektorze, proszę powiedzieć, na jakim etapie legislacyjnym jesteśmy, jeżeli chodzi o przygotowanie przepisów, mających na celu dostosowanie polskiego porządku prawnego do RODO? Jakie kroki przed nami i kiedy możemy się spodziewać zakończenia procesu legislacyjnego?

dr Maciej Kawecki: Projekt czeka na posiedzenie Rady Ministrów. Po przyjęciu przez Komitet Stały Rady Ministrów będziemy chcieli, żeby został jak najszybciej przyjęty przez Radę Ministrów. Realnym terminem jest listopad b.r. Grudzień i pierwsza połowa stycznia to czas na prace parlamentarne, w związku z tym koniec lutego będzie terminem na wejście w życie wszystkich przepisów. Ostatnia wersja projektu ustaw pochodzi z 22.10.2018 r., zawiera ona względem wcześniejszego projektu trzy najważniejsze zmiany. Pierwsza z nich dotyczy ustawy o ochronie danych osobowych i wprowadzenia instytucji zastępcy inspektora ochrony danych, której dzisiaj nie ma, natomiast przed 25 maja ustawa przewidywała zastępcę. Druga zmiana dotyczy art. 28 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta i przyznaje pacjentom nieodpłatny dostęp do pierwszej kopii dokumentacji medycznej – dziś za to pobierana jest opłata. Jest to istotna zmiana, czyli zrównanie prawa do kopii wynikającego z art. 15 RODO z art. 28 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Trzecia zmiana dotyczy Kodeksu pracy w zakresie monitoringu wizyjnego i przesądzenia, że obszary związków zawodowych nie mogą podlegać bezwzględnie monitoringowi. Są to zmiany, których nie było we wcześniejszej wersji, a teraz zostały wprowadzone.

Czy Ministerstwo Cyfryzacji planuje jakieś działania nakierowane na edukowanie i wsparcie dla administracji publicznej w związku z tymi nowymi przepisami? Czego możemy spodziewać się w końcówce 2018 r.?

M.K.: Po pierwsze planujemy wydanie poradnika związanego z RODO dla administracji publicznej, jego wydanie przewidziane jest na koniec listopada, początek grudnia. Po drugie razem z pełnomocnikiem rządu ds. małych i średnich przedsiębiorstw planujemy pomiędzy 15 listopada a 15 grudnia zorganizowanie cyklu spotkań głównie, ale nie tylko, dla administracji skarbowej oraz dla innych przedsiębiorców. Minister Cyfryzacji rozważa wydanie objaśnień na podstawie art. 33 Prawa przedsiębiorców, dotyczącego najbardziej wrażliwych tematów. W dniu 25 listopada została uruchomiona dla przedsiębiorców zakładka na stronie internetowej Ministerstwa Cyfryzacji, która w jednym miejscu skupia wszystkie informacje na temat RODO www. www.www .

Z pańskiego punku widzenia i na podstawie obserwacji poczynionych w ramach prowadzonych spotkań z Panem i administracją publiczną, jakie obowiązki wynikające z RODO sprawiły administracji publicznej największe problemy i dlaczego?

M.K.: Największy problem sprawia odpowiednie zlokalizowanie Inspektora Ochrony Danych. Za przykład niech posłuży mała jednostka budżetowa, gdzie pracuje jeden informatyk, bardzo często ten informatyk pełni funkcję IOD i wtedy rzeczywiście w jakimś zakresie ocenia, kontroluje sam siebie. Z jednej strony odpowiada za zabezpieczenia, a z drugiej strony odpowiada za nadzór nad tymi zabezpieczeniami. Cały czas wyzwaniem jest odpowiednia lokalizacja IOD.

Drugą rzeczą są zgody. W administracji publicznej pokutuje przekonanie, że tą najważniejszą przesłanką przetwarzania danych osobowych jest zgoda, spotykamy się z różnymi przypadkami, gdzie na np. przetwarzanie danych osobowych pracowników zbierana jest zgoda. Czyli nadmiarowość w zbieraniu zgód.

Ponadto, choć nie są to przypadki nagminne, administracja publiczna

trochę boi się, z powodu RODO, rozmawiania z obywatelami przez telefon, nie chcąc udostępniać im żadnych informacji. Zaczęto się obawiać, że droga telefoniczna w ogóle nie może służyć jakimkolwiek kontaktom. Tak nie jest, administracja powinna, w zależności od tego, co się przez telefon mówi, starać się weryfikować tożsamość dzwoniącego przez tzw. pytanie identyfikujące.

Z perspektywy czasu, czy w oparciu o zdobyte doświadczenie pracy Ministerstwa Cyfryzacji, zmieniłby Pan coś w przyjętej koncepcji przygotowania nowej ustawy o ochronie danych osobowych i pakietu ustaw zmieniających? Czy coś można było zrobić inaczej?

M.K.: Można się zastanowić, czy ta regulacja nie jest nadmiarowa dla MŚP. Za przykład niech posłuży nam mały przedsiębiorca, który rozpoczyna działalność, mały start-up, który nie jest prawnikiem, którego nie stać na prawników, ma ogrom regulacji prawnych i jeszcze tematykę RODO, a jego głównym celem jest prowadzenie działalności gospodarczej i jej rozwój. Dlatego, aby ułatwiać im wdrażanie RODO warto wydawać różnego rodzaje poradniki i dokumenty.

Na pewnym etapie prac legislacyjnych wprowadziliśmy zmiany związane z ułatwieniem stosowania RODO dla MŚP. Tych przepisów mogłoby być więcej, np. mogłyby dotyczyć analizy ryzyka, która na etapie pogłębionym powinna dotyczyć makroprzedsiębiorców, a na etapie podstawowym mikroprzedsiębiorców, czyli tych, którzy zatrudniają do 10 pracowników. To są te uwagi, które, jeżeli moglibyśmy, to rozważylibyśmy, czy nie powinny być wprowadzone.

W pozostałym zakresie uważam, że ustawa się sprawdza.

Bardzo dobrym rozwiązaniem jest uprawnienie UODO do wydawania dokumentów, jak np. wytyczne dotyczące spraw kadrowych – choć te są kontrowersyjne, dotyczące monitoringu wizyjnego, czy dotyczące wyborów, wszystkie zostały wydane na podstawie ustawy o ochronie danych osobowych.

Jak przebiegają prace grup roboczych działających przy Ministerstwie Cyfryzacji, których celem jest wyjaśnienie zasad stosowania RODO w praktyce? Na czym te prace są skoncentrowane? Kiedy możemy spodziewać się wyników tych prac?

M.K.: Pierwszy rezultat prac jest już dostępny i obublikowany na stronach internetowych ministerstwa. Jest to poradnik „RODO w służbie zdrowia". Do końca roku będą wydane wszystkie lub prawie wszystkie poradniki. W tym momencie prace trwają w czterech grupach:

1) grupa dotycząca sektora finansowego, telekomunikacyjnego i ubezpieczeniowego;
2) grupa ds. edukacji, która przygotowała poradnik „RODO w systemie oświaty i wychowania";
3) grupa ds. administracji publicznej, która zajmuje się tematami związanymi z przetwarzaniem danych w sektorze publicznym oraz
4) grupa ds. ogólnych, która odpowiada na różne pytania od bardzo skomplikowanych do bardzo prostych.

Pierwsze spotkanie grupy miało charakter plenarny, teraz prace odbywają się w zespołach.

W pracach biorą udział m.in.: przedstawiciele Ministerstwa Edukacji Narodowej, Ministerstwa Zdrowia, Kancelarii Prezesa Rady Ministrów, Ministerstwa Spraw Wewnętrznych i Administracji, Ministerstwa Finansów, Ministerstwa Przedsiębiorczości i Technologii, Ministerstwa Inwestycji i Rozwoju, Ministerstwa Obrony Narodowej.

Grupa korzysta też z doświadczeń przedstawicieli Rzeczników: Praw Obywatelskich i Praw Pacjenta.

Dbamy o to aby poradniki były wydawane szybko. Za każdym razem, przynajmniej tak było przy poradniku „RODO w służbie zdrowia", staramy się uzyskać opinię Prezesa Urzędu Ochrony Danych. Dzięki temu poradniki są bardziej wartościowe dla tych, którzy będą z nich korzystać.

legalis administracja

Inicjatywy Ministerstwa Cyfryzacji związane z wyjaśnianiem przepisów RODO i innych przepisów

Rozpoczęcie stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1; dalej: RODO) przyniosło wiele błędnych interpretacji przepisów nowego prawa. Pytania do Ministra Cyfryzacji w zakresie problemów z wdrożeniem RODO kierowane są nadal. Ministerstwo wspiera administratorów danych osobowych w administracji publicznej (ale też poza nią) w wyjaśnianiu sensu tych przepisów oraz rozwiązywaniu najważniejszych problemów związanych z wdrożeniem nowego prawa unijnego.

Ministerstwo Cyfryzacji włączyło się w kampanię przygotowań do wejścia w życie RODO. Dyrektor Departamentu Zarządzania Danymi w Ministerstwie Cyfryzacji dr *Maciej Kawecki* (DZD), jako koordynator wdrożenia RODO, uczestniczył w spotkaniach na terenie całej Polski i nadal bierze w nich udział. Ministerstwo prowadziło kampanie informacyjne i włączało się we wszystkie możliwe inicjatywy w tym zakresie. Już po wejściu w życie unijnego rozporządzenia podstawowym problemem stała się nadinterpretacja przepisów, a czasem ich całkowicie błędne rozumienie.

Z tego względu Minister Cyfryzacji zdecydował się powołać Grupę Roboczą ds. Ochrony Danych Osobowych. Zamiar jej powołania został zgłoszony przez Ministra Cyfryzacji na posiedzeniu Rady Ministrów 5.6.2018 r.

Cele prac Grupy są następujące:

1) opracowanie klucza postępowania w najczęstszych sytuacjach problemowych, które wynikają z nadinterpretacji przepisów RODO, oraz mogących budzić wątpliwości przepisów ustawy z 10.5.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.; dalej: OchrDanychU);
2) wydanie serii „Poradników RODO dla branżowych praktyków" – zbiorów odpowiedzi na najczęściej zadawane w poszczególnych branżach pytania. Zalecenia – wypracowane przez Grupę w ścisłej współpracy z Prezesem Urzędu Ochrony Danych Osobowych – będą pomocne dla osób odpowiadających za zgodność z zapisami RODO w firmach, urzędach i organizacjach;
3) wypracowanie Kodeksu Postępowania dla Administracji Publicznej;
4) zidentyfikowanie luk w prawie krajowym w zakresie bezpośredniego stosowania RODO i opracowania ścieżki do ich usunięcia.

Grupa to interdyscyplinarne robocze forum wymiany doświadczeń. W skład Grupy wchodzą eksperci z sektora prywatnego i publicznego, uczestniczą reprezentanci członków Rady Ministrów, przedstawiciele administracji publicznej, biznesu, izb i stowarzyszeń branżowych, środowisk naukowych i organizacji pozarządowych. W pracach biorą udział przedstawiciele Ministerstwa Edukacji Narodowej, Ministerstwa Zdrowia, Kancelarii Prezesa Rady Ministrów, Ministerstwa Spraw Wewnętrznych i Administracji, Ministerstwa Finansów, Ministerstwa Przedsiębiorczości i Technologii, Ministerstwa Inwestycji i Rozwoju, Ministerstwa Obrony Narodowej. Grupa korzysta też z doświadczeń przedstawicieli Rzeczników: Praw Obywatelskich i Praw Pacjenta. Liderem Grupy jest dr *M. Kawecki*, Ministerstwa Cyfryzacji i koordynator wdrożenia RODO. Pełny skład Grupy, zaakceptowany przez Ministra Cyfryzacji, dostępny jest na stronie: https://www.gov.pl/cyfryzacja/ruszyly-prace-grupy-ds-ochrony-danych-osobowych.

W ramach Grupy pracują następujące zespoły tematyczne:

1. Zespół ds. Systemu Ochrony Zdrowia – pracujący pod kierownictwem dr *M. Kaweckiego*;
2. Zespół ds. Administracji – pod kierownictwem *S. Szczepaniaka*, Zastępcy Dyrektora Departamentu Prawnego MC;
3. Zespół ds. Telekomunikacji i Finansów – pod kierownictwem *K. Prusak-Górniak*, Dyrektora Departamentu Prawnego MC;

4. Zespół ds. Edukacji – prowadzi *J. Noga-Bogomilska*, radca prawny w Ministerstwie Cyfryzacji;
5. Zespół ds. Ogólnych (niemieszczących się w powyższych zakresach) – *J. Pisarczyk-Jagielska*, Inspektor Ochrony Danych.

W efekcie kolejnych posiedzeń zespołów oraz przyjętej formuły roboczego dopracowywania tekstów zaleceń, przygotowano do publikacji (i przekazano do zaopiniowania PUODO) dwa poradniki: „RODO w służbie zdrowia" oraz „RODO w systemie oświaty i wychowania". Pierwszy poradnik jest już dostępny na stronach internetowych ministerstwa.

W przygotowaniu są następujące poradniki:

1) „RODO w urzędzie/w administracji publicznej";
2) „RODO w telekomunikacji i finansach";
3) Zespół ds. ogólnych … „A w ogóle to… RODO – czyli, co zrobić, by nie zbłądzić?".

Ważne

Ministerstwo Cyfryzacji przygotowało „RODO Informator" i „RODO dla obywatela" zamieszczone na stronach urzędu. Te publikacje powstały znacznie wcześniej i pomogły wielu podmiotom we wdrożeniu i zrozumieniu nowego prawa unijnego.

Zagadnienia omawiane w ramach zespołów

Zagadnienia omawiane na posiedzeniach Zespołu ds. Systemu Ochrony Zdrowia omówiono już w poradniku dostępnym na wspomnianych stronach Ministerstwa Cyfryzacji.

Zespół zajmujący się zagadnieniami dot. telekomunikacji i finansów omawiał problemy, które dotyczyły podmiotów prywatnych, tj. banków i firm telekomunikacyjnych. Jednak wiele spraw dotyczy także administracji. Eksperci z Grupy Roboczej wielokrotnie zajmowali się wątpliwościami zgłaszanymi w zakresie spełnienia obowiązku informacyjnego względem osób, których dane zostały zebrane przed 25.5.2018 r. Wiele pytań dotyczyło sposobu realizacji obowiązku informacyjnego podczas komunikacji telefonicznej. To zagadnienie będzie także opisane w publikacji. Znajdzie się tu również rozwiązanie problemu, jak należy rozumieć „dane kontaktowe osoby prawnej" z motywu 14 RODO. Podjęto próbę odpowiedzi na pytanie, czy sam fakt zeskanowania dokumentu papierowego, na którym znajdują się dane osobowe i przechowywania go w systemach informatycznych (np. w postaci pliku PDF) jest podstawą do uznania, że dane te są przetwarzane w sposób zautomatyzowany w rozumieniu RODO. W administracji zdarzają się takie sytuacje, gdy dane zostały przekazane administratorowi z własnej inicjatywy podmiotu danych, tj. bez uprzedniej wiedzy oraz sygnalizowanej przez administratora potrzeby przekazania takich danych. Próbowano odpowiedzieć na pytanie, jak należy postępować w takiej sytuacji. Opisano stanowisko Grupy w sprawie kopii zapasowych. Istotny w tym przypadku jest termin powstania obowiązku usunięcia danych osobowych z kopii zapasowych systemów informatycznych. Zaprezentowano stanowisko w zakresie sektorowych przepisów odrębnych – czy przepisy odrębnych ustaw dotyczące działalności podmiotów regulowanych (tzw. regulacje sektorowe) mogą stanowić *lex specialis* wobec przepisów RODO.

Zagadnienia omawiane w ramach Zespołu ds. Edukacji zainteresują pracujących w szkołach i innych placówkach dydaktycznych oraz osoby zajmujące się ochroną danych osobowych. Pojawiło się podstawowe pytanie o to, czy nauczyciel może posługiwać się imieniem i nazwiskiem ucznia w trakcie zajęć lekcyjnych? Co z wyczytywaniem nazwisk na uroczystościach szkolnych i wywieszaniem prac plastycznych z nazwiskiem ucznia? Czy należy w tych przypadkach uzyskać zgodę rodziców? Sposób postępowania w stosunku do danych zawartych w dokumentach ucznia dotyczących zdrowia, np. dysleksji, budził wątpliwości. Publikacja odpowiada na pytania dotyczące postępowania z wizerunkiem ucznia i danymi osobowymi ucznia w szkolnej szatni.

Zespół ds. Administracji zajmował się zagadnieniami takimi jak: przesłanka interesu publicznego z art. 6 ust. 1 lit. e) RODO w stosunku do administracji, problemem związanym z transmisją *online* posiedzeń organów samorządowych, przetwarzaniem danych osobowych w związku z zamówieniami publicznymi, danymi osobowymi w przypadku wystąpień posłów i senatorów, stosowaniem przesłanki legalności – zgody jako podstawy przetwarzania w administracji publicznej, zagadnieniami związanymi z przetwarzaniem danych osobowych przy okazji organizacji imprez i spotkań, stosowaniem przesłanki prawnie uzasadnionych interesów, o których mowa w art. 6 ust. 1 lit. f) RODO, stosowaniem przepisów RODO względem obowiązków wynikających z ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257 ze zm.) w zakresie spraw przekazywanych zgodnie z właściwością miejscową, zagadnieniami ochrony danych osobowych przy organizacji wyborów, dokumentacją ochrony danych osobowych w jednostce samorządowej.

Zespół ds. Ogólnych analizował zagadnienia, które nie znalazły się w zakresie tematycznym pozostałych zespołów. Wśród tematów znalazła się problematyka związana z obowiąz-

kiem informacyjnym wobec przedstawicieli spółki w zakresie zawieranych umów, kontrolami i ich liczbą w zakresie zwieranych umów powierzenia, danymi w fakturach, a także zagadnienie dotyczące administratora danych w firmach w przypadku firm kurierskich, archiwizacji wniosków dotyczących praw osób, których dane dotyczą, przewidzianych w RODO i inne.

Widać już pierwsze efekty prac Grupy. Ministerstwo jest w trakcie uzgodnień dotyczących kolejnych publikacji pomocnych w rozwiązywaniu najistotniejszych problemów. Wielu administratorów uznaje RODO za dodatkowe utrudnienie i zbędne obowiązki, pomimo tego, że unijne rozporządzenie ma działać na rzecz wszystkich osób, których dane są przetwarzane i chronić ich prawa.

Internet rzeczy

W MC podejmowane są również inne inicjatywy. Powstała Grupa Robocza ds. Internetu Rzeczy. Pierwsze jej posiedzenie odbyło się 24.8.2018 r. w siedzibie Urzędu. Wzięli w nim udział: *K. Okoński*, *M. Ociepa*, odpowiednio sekretarz i podsekretarz stanu w MC, przedstawiciele Ministerstwa Przedsiębiorczości i Technologii, wspominany już dr *M. Kawecki* oraz *L. Maśniak*, Wiceprzewodniczący Rady Architektury przy Komitecie Rady Ministrów ds. Cyfryzacji, a także przedsiębiorcy oraz przedstawiciele środowisk naukowych i administracji.

„Internet rzeczy" (*Internet of things – IoT)* to stosunkowo nowe zagadnienie pojawiające się w prasie i mediach, także w kontekście ochrony danych osobowych. Celem prac Grupy jest opracowanie raportu, który będzie wskazywał realny wpływ rozwoju *IoT* na rozwój gospodarczy kraju, wskaże potencjał i zagrożenia w tym zakresie. Konkluzje ze wspólnej pracy dotrą do wszystkich resortów, odpowiedzialnych za obszary interwencji wskazane w raporcie wypracowanym przez Grupę. Opracowano katalog zagadnień, którymi członkowie Grupy chcą się zajmować. Uczestnicy spotkania najczęściej wskazywali na potrzebę implementacji rozwiązań *IoT* w poszczególnych sektorach. Najczęściej wymieniano: ochronę zdrowia, pojazdy autonomiczne, ochronę środowiska, finanse, *smart city* czy energetykę.

Podgrupy działające w ramach Grupy to:

1. Ogólna – część wstępna raportu, zapewnienie spójności i kompletności raportu końcowego.
2. Opomiarowanie – woda, gaz, prąd, ścieki – liczniki, standardy, analiza danych.
3. Ochrona Zdrowia – telemedycyna, ubezpieczenia zdrowotne, *wearable devices* i inne.
4. Rolnictwo i ochrona środowiska.
5. Pojazdy autonomiczne – logistyka, transport, drogi.
6. Przemysł.
7. Telekomunikacja – 5G, lokalizacja, wykorzystanie danych.
8. Bezpieczeństwo i Certyfikacje – ogólne zagadnienia bezpieczeństwa, certyfikacji urządzeń i dostawców.
9. Inteligentne Miasta i Budynki.

Podczas spotkania uczestnicy wskazali dodatkowe sektory zastosowań *IoT*, tj. rolnictwo, gospodarkę żywnościową, farmację. Podczas wystąpień sygnalizowano potrzebę rozmowy o *IoT* w kontekście: ochrony praw konsumenta, działań dydaktycznych, zwiększania świadomości obywateli, standaryzacji platform dla *smart city*, sieci 5G, obowiązków producentów i operatorów związanych z *IoT*, cyberbezpieczeństwa, zastosowania nowoczesnych bezprzewodowych technologii sieciowych w komunikacji z energooszczędnymi urządzeniami *IoT*, wykorzystania chmury publicznej w ramach aplikacji *IoT*. Równie ważną kwestią będzie zdefiniowanie barier technologicznych, legislacyjnych i ekonomicznych oraz praca nad ich zniesieniem.

Sztuczna inteligencja

Kolejna ważna inicjatywa to zajęcie się problematyką sztucznej inteligencji (SI). Tu także powstała Grupa robocza. **Sztuczna inteligencja jest tym zjawiskiem, w którym upatruje się wielu korzyści dla gospodarek i społeczeństw, ale jednocześnie budzi ono najwięcej obaw.** Staje się obszarem olbrzymich wysiłków inwestycyjnych i rozwojowych w wielu krajach. To wyzwanie dla przedsiębiorców, korporacji a nawet start-upów, których celem jest zdobycie przewagi konkurencyjnej.

Zwieńczeniem prac Grupy była zorganizowana 9.11.2018 r. konferencja, podczas której przedstawione zostały wyniki prac. Pierwsze spotkanie podgrup roboczych w sprawie SI odbyło się 6.7.2018 r. w Ministerstwie Cyfryzacji. Członkowie Grupy zgłaszali się po zamieszczeniu informacji na stronie internetowej urzędu.

W ramach Grupy powstały 4 podgrupy obejmujące wybrane tematy dotyczące sztucznej inteligencji:

1. **Gospodarka oparta na danych** (w tym wsparcie dla wdrożenia SI przez firmy)

   Przedmiotem prac grupy są zagadnienia związane z rosnącym wolumenem danych cyfrowych w gospodarce i administracji. Tylko dostęp do wysokiej jakości cyfrowych danych umożliwi tworzenie, testowanie i wykorzystywanie rozwiązań z zakresu sztucznej inteligencji. Celem grupy jest wypracowanie narzędzi, które umożliwią firmom przygotowanie do szerokiego wykorzystania danych w swojej aktywności oraz w perspektywie wykorzystanie sztucznej inteligencji w swojej działalności.

2. **Finansowanie badań i rozwoju**

   Celem działań grupy jest zmapowanie i ocena istniejących mechanizmów finansowych i poszukiwanie nowych, a także zaproponowanie optymalnych modeli absorpcji tych środków, w tym ekosystemu współpracy nauki, administracji i biznesu.
3. **Edukacja**

   Przedmiotem prac grupy jest m.in. diagnoza problemów w systemie polskiej edukacji oraz przedstawienie konkretnych propozycji rozwiązań. Synteza wszystkich etapów edukacji oraz odniesienie się do potrzeby kształcenia ustawicznego.
4. **Etyka i prawa człowieka** (w tym kwestie prawne) – prace nad kwestiami: odpowiedzialności za działania robotów/sztucznej inteligencji, możliwości nadania osobowości prawnej robotom. Jest to problematyka odpowiedzialności za produkt oraz odpowiedzialności z tytułu ryzyka operatora SI. Zagwarantowanie wolności człowieka i praw podstawowych, na których opiera się UE – nowe technologie nie powinny bowiem oznaczać nowych wartości, ale również nie powinny być przyczyną protekcjonistycznego ograniczania wolności gospodarczej ani warunków uczciwej konkurencji.

Celem prac poszczególnych grup będzie wypracowanie krótkiego raportu zawierającego: opis stanu aktualnego, identyfikację barier, przedstawienie propozycji konkretnych rozwiązań. Opracowany wspólnie materiał posłuży jako podstawa do wypracowania założeń dla strategii sztucznej inteligencji dla Polski.

Otwieranie danych i ponowne wykorzystywanie informacji sektora publicznego

Ministerstwo dostrzega potrzebę współpracy w zakresie otwierania danych i ponownego wykorzystywania informacji sektora publicznego w dowolnych celach – komercyjnych lub niekomercyjnych.

W dniu 11.7.2018 r. odbyło się pierwsze posiedzenie Grupy Roboczej ds. Otwartych Danych. Członkami Grupy są przedstawiciele Ministerstwa Cyfryzacji zajmujący się tą tematyką, organizacji pozarządowych, środowisk naukowych, biznesu oraz administracji samorządowej i rządowej. Celem prac Grupy jest włączenie podmiotów zewnętrznych do kreowania polityki otwartości danych oraz promocja ponownego wykorzystywania danych przez różne podmioty.

Warto przypomnieć, że Rada Ministrów we wrześniu 2016 r. przyjęła Program Otwierania Danych Publicznych i wyznaczyła tym samym cele strategiczne w obszarze otwierania danych do 2020 r. Ponadto 25.4.2018 r. Komisja Europejska opublikowała projekt nowej dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego (tzw. dyrektywa *reuse*), która poszerza zakres danych przekazywanych do dalszej eksploatacji i wprowadza nowe rozwiązania, które mają ułatwić ponowne wykorzystywanie informacji. Inicjatywa ta jest częścią strategii Jednolitego Rynku Cyfrowego. Jej celem jest usunięcie barier dla rozwoju gospodarki opartej na danych. Zaproponowano nowe rozwiązania, które mają zapewnić m.in. zwiększenie dostępu do tzw. danych dynamicznych w czasie rzeczywistym poprzez interfejs programistyczny aplikacji API oraz bezpłatny dostęp do poszczególnych kategorii danych o wysokiej wartości dla ponownego wykorzystywania przez API, które będą wymienione w przyszłym akcie wykonawczym.

Grupa postawiła sobie ambitne zadania. Wśród tematów zgłoszonych przez członków Grupy do dyskusji pojawiła się także problematyka standardów tworzenia nowych rozwiązań bazodanowych w zakresie rejestrów, które uwzględnią potrzeby związane z otwieraniem danych (w tym kwestie anonimizacji danych w przypadku danych osobowych, wrażliwych itp.), inny to zaangażowanie doświadczonych placówek do działań szkoleniowych oraz włączenie w plan zajęć szkół lekcji z zakresu korzystania z otwartych danych przy współpracy z MEN.

Przede wszystkim chodzi jednak o zachęcanie instytucji dysponujących danymi do ich udostępniania, dbania o ich jakość, a także wypracowania *business case* dla administracji w tym zakresie.

To tylko kilka przykładów inicjatyw MC. Warto podkreślić, że wiele projektów o skali ogólnokrajowej nabrało tempa. Ministerstwo liczy na współpracę z Czytelnikami pisma w zakresie nowych inicjatyw.

Joanna Pisarczyk-Jagielska
Inspektor Ochrony Danych

Sylwia Bielińska
Główny Specjalista

Podstawa prawna

- art. 6 ust. 1 lit. e) lit. f) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1)

Prawo do otrzymania kopii danych a prawo do przenoszenia danych – kluczowe zagadnienia dla sektora publicznego

Michał Czerniawski
Doktor nauk prawnych, urzędnik państwowy, jeden z negocjatorów RODO

Pomimo że rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1; dalej: RODO) jest bezpośrednio stosowane we wszystkich państwach członkowskich – w tym w Polsce – już od kilku miesięcy, jego praktyczna implementacja wciąż nastręcza problemów. Zagadnieniem o dużej doniosłości praktycznej dla administracji publicznej jest kwestia dostępu do danych przez osoby, których one dotyczą.

Administracja publiczna przetwarza niezwykle duże ilości danych. W tym kontekście szczególnie istotne są dwa uprawnienia osób fizycznych: prawo do żądania kopii danych (art. 15 ust. 3 RODO) oraz prawo do żądania przeniesienia danych osobowych (art. 20 RODO). Uprawnienia te skonstruowano w celu umożliwienia osobie, której dane dotyczą, sprawowania jak najpełniejszej kontroli nad tym, co dzieje się z dotyczącymi jej informacjami. Potencjalnie wiążą się one jednak ze sporymi obciążeniami dla administratora danych. Stąd też ustawodawca, tak unijny, jak i krajowy[1], zdecydował się ograniczyć możliwość skorzystania z obu ww. praw w stosunku do sektora publicznego.

Prawo do otrzymania kopii danych

Artykuł 15 ust. 3 RODO stanowi, że „administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu". Dostarczenie następuje na żądanie osoby, której dane dotyczą. Co istotne, przepis ten, inaczej niż omówiony poniżej art. 20 RODO, nie reguluje kwestii formatu otrzymywanych danych, kopia więc może być dostarczona w formacie nienadającym się do odczytu maszynowego, np. PDF. Z kolei za

[1] Należy jednocześnie odnotować, że w stosunku do części rozwiązań krajowych wciąż toczą się prace legislacyjne. Zob. Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, http://legislacja.rcl.gov.pl/projekt/12302951.

formaty „nadające się do odczytu maszynowego", co jest szczególnie istotne w kontekście przenoszalności, uznaje się m.in. otwarte formaty takie jak XML, JSON, CSV[2]. Kwestia formatu, w którym następuje udostępnienie danych jest jedną z podstawowych różnic pomiędzy prawem do uzyskania kopii danych, a uprawnieniem do ich przeniesienia, tylko bowiem w tym pierwszym przypadku unijny prawodawca nie stawia wobec administratora danych szczególnych wymogów. Jednocześnie, zgodnie z omawianym przepisem, jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Ograniczenie postanowień art. 15 ust. 3 stanowi art. 15 ust. 4 RODO, zgodnie z którym prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych. Motyw 63 RODO w odniesieniu do takich praw i wolności wskazuje wprost na ochronę tajemnicy handlowej lub własności intelektualnej, w szczególności na prawa autorskie chroniące oprogramowanie. Jeżeli więc kopia danych ujawniałaby tego typu informacje, np. *know-how* co do tego jak działa konkretny system administratora danych, administrator może nie uczynić zadość żądaniom osoby, której dane dotyczą.

W świetle art. 15 RODO niezwykle istotna jest kwestia odpłatności. Wykonanie prawa do uzyskania kopii danych osobowych, co do zasady, nie powinno wiązać się z koniecznością ponoszenia opłat. Dotyczy to jednak wyłącznie pierwszej kopii. W przypadku kolejnych kopii, administrator danych może pobrać opłatę „w rozsądnej wysokości wynikającej z kosztów administracyjnych". Takie rozwiązanie ma na celu ograniczenie nadużywania analizowanego uprawnienia. Jednocześnie, w motywie 63 RODO unijny prawodawca zachęca do umożliwiania bezpośredniego dostępu do systemu, w którym przetwarzane są dane, co już jest w Polsce niekiedy możliwe, także w sektorze publicznym, przykładem może być tu wgląd do rejestru PESEL za pośrednictwem portalu obywatel.gov.pl.

W kontekście prawa do otrzymania kopii danych w polskim porządku prawnym kluczowy wydaje się art. 5 ustawy z 10.5.2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2018 r. poz. 1000 ze zm.; dalej: OchrDanychU). Opiera się on na przewidzianej w art. 23 ust. 1 RODO możliwości ograniczenia zakresu obowiązków i praw przewidzianych w RODO, przez prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, o ile ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, art. 5 OchrDanychU uzupełnia ją jednak jeszcze o dodatkowe, niewynikające z postanowień RODO, wymogi. Przepis ten stanowi, że administrator wykonujący zadanie publiczne, nie przekazuje informacji, o których mowa w art. 15 ust. 1–3 RODO, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązków, o których mowa w art. 15 ust. 1–3 RODO, jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 RODO oraz jeżeli ma miejsce jedna z następujących sytuacji:

1) wykonywanie tych obowiązków uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
2) wykonywanie tych obowiązków naruszy ochronę informacji niejawnych.

Postanowienie to stosuje się wobec „administratorów wykonujących zadania publiczne", obejmuje więc także podmioty prywatne wykonujące tego typu zadania. Sformułowanie „nie przekazuje" należy interpretować w ten sposób, że organ nie ma tu swobody decyzyjnej, i jeżeli zachodzą wyżej wymienione przesłanki, kopii danych po prostu przekazać nie może. Ponadto, zgodnie z art. 5 ust. 2 OchrDanychU, jeżeli dostarczenie kopii danych osobowych wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, administrator wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Odpowiednio stosuje się przy tym art. 64 ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257 ze zm.), który pozwala na wezwanie wnoszącego do usunięcia braków w wyznaczonym terminie i w przypadku ich nieusunięcia, pozostawienie sprawy bez rozpoznania. Poprzez to postanowienie polski ustawodawca wydaje się brać pod uwagę skalę danych osobowych przetwarzanych przez sektor publiczny i mogące z tego wynikać problemy praktyczne. Należy jednak wskazać, że powoływanie się na przywołany przepis wymaga rozwagi, ponieważ niemożność wyszukania danych może stanowić dla osoby, której dane dotyczą, podstawę do skargi do organu nadzorczego na naruszenie przez administratora danych zasad dotyczących przetwarzania danych osobowych, o których mowa w art. 5 RODO. Z kolei art. 5 ust. 3 OchrDanychU wskazuje, że administrator w przypadkach, o których mowa w ust. 1 i 2 tego artykułu, zapewnia odpowiednie środku służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą. Polski ustawodawca decyzję co do tego, czym są „odpowiednie" środki, które należy zapewnić, pozostawia jednak admini-

[2] Grupa Robocza Art. 29, Wytyczne dotyczące prawa do przenoszenia danych, przyjęte 13.12.2016 r., ostatnio zmienione i przyjęte 5.4.2017 r., dokument WP 242 rew.01 w tłumaczeniu GIODO, s. 19.

stratorowi danych. Co istotne, zgodnie z art. 5 ust. 4 OchrDanychU, administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niedostarczenia kopii danych osobowych podlegających przetwarzaniu.

Warto także odnotować, że w chwili oddania niniejszego tekstu do druku, wciąż procedowany jest „Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679", który jeszcze bardziej ogranicza stosowanie art. 15 ust. 3 RODO, choćby w stosunku do danych osobowych objętych różnego rodzaju tajemnicami zawodowymi, w szczególności radcy prawnego lub adwokata, a także zasobów archiwalnych i archiwów czy też w kontekście Prawa zamówień publicznych bądź umów koncesji na roboty budowlane lub usługi. W praktyce, prawo krajowe w szeregu sytuacji pozwala administratorom z sektora publicznego na odmowę dostarczenia kopii danych, stawiając ich w tym zakresie w znacznie lepszej sytuacji niż administratorów danych z sektora prywatnego.

Prawo do przenoszenia danych

O ile art. 15 RODO (prawo do uzyskania kopii danych) jest uprawnieniem bezwarunkowym i doznaje ograniczenia dopiero, w związku z art. 23 RODO, na podstawie przepisów prawa krajowego, o tyle ograniczenia możliwości żądania przenoszenia danych osobowych (art. 20 RODO) od administratorów danych z sektora publicznego wprowadza już samo RODO. W mojej ocenie, samo prawo do przenoszenia danych jest uprawnieniem prokonsumenckim i prokonkurencyjnym, a więc od samego początku projektowanym z myślą o administratorach danych spoza tego sektora. Wydaje się, że miało ono przeciwdziałać zjawisku tzw. *lock-in*, w przypadku którego, ze względu na brak interoperacyjności pomiędzy usługodawcami, usługobiorca, z przyczyn technicznych bądź ze względu na wiążące się z tym koszty, nie jest w stanie zmienić dotychczasowego usługodawcy (może tu chodzić np. o przenoszenie kont pomiędzy portalami społecznościowymi czy historii zakupów pomiędzy sklepami internetowymi). Problem ten ze swojej natury nie dotyczy jednak ani administracji publicznej, ani podmiotów prywatnych wykonujących zadania realizowane w interesie publicznym.

Zgodnie z art. 20 RODO, na prawo żądania przeniesienia danych składają się trzy uprawnienia osoby, której dane dotyczą:

1) prawo do otrzymania danych;
2) prawo do przesłania otrzymanych danych bez utrudnień ze strony administratora;
3) prawo do przesłania danych bezpośrednio pomiędzy administratorami (o ile jest to technicznie możliwe)[3].

Prawo do przenoszenia danych jest znacząco ograniczone w samym RODO, i tak:

1) przysługuje tylko w ściśle określonych sytuacjach, tj. gdy podstawą prawną przetwarzania jest zgoda bądź umowa;
2) przysługuje tylko wtedy, gdy dane przetwarzane są w sposób zautomatyzowany;
3) obejmuje wyłącznie dane dostarczone administratorowi przez osobę, której one dotyczą (a nie całość przetwarzanych danych, jak w przypadku art. 15 ust. 3 RODO);
4) nakazuje udostępnienie danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego;
5) nie znajdzie zastosowania w przypadku przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, o czym wprost stanowi art. 20 ust. 3 RODO.

Wydawałoby się, że art. 20 ust. 3 RODO całkowicie eliminuje możliwość żądania przeniesienia danych osobowych od administratorów danych z sektora publicznego (zwłaszcza, jeżeli weźmiemy dodatkowo pod uwagę, że uprawnienie to przysługuje wyłącznie gdy podstawą przetwarzania jest zgoda bądź umowa). Nie jest to jednak do końca prawda. Należy pamiętać, że są sytuacje, w których sektor publiczny przetwarza dane, choć nie jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Administracja publiczna wykonuje np. też zadania organizatorskie, tytułem przykładu – szereg organów prowadzi i rozsyła listy mailingowe, do których zapisanie się jest dla obywatela dobrowolne i wymaga wyrażenia zgody. Dane zbierane w tego typu celach, jako niespełniające przesłanek z art. 20 ust. 3 RODO, będą podlegać prawu do przenoszenia danych. Stąd też należy pamiętać, że w określonych sytuacjach osoba fizyczna może żądać od administratora danych z sektora publicznego przeniesienia jej danych.

Dalsze obowiązki

Tak prawo do otrzymania kopii danych, jak i prawo do przenoszenia danych podlegają nie tylko opisanym wyżej ograniczeniom, ale także zasadom wynikającym z przepisów ogólnych. Należy w szczególności pamiętać, że wszelkie działania podejmowane przez administratora danych w ich kontekście powinny być zgodne z art. 12 RODO i spełniać wskazane w tym przepisie wymogi w zakresie informacji, komunikacji oraz ułatwiania wyko-

[3] Szerzej na ten temat: *M. Czerniawski*, Obowiązki administratora danych wynikające z prawa do przenoszenia danych, [w:] Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych, Biblioteka Monitora Prawniczego, Warszawa 2017.

nywania praw. Zgodnie z art. 12 ust. 5 RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
b) odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa jednak na administratorze. Natomiast, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie na podstawie art. 12 ust. 6 RODO, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Jeśli chodzi o kwestię terminów realizacji analizowanych uprawnień, to określa je art. 12 ust. 3 RODO, zgodnie z którym administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem (bądź o przedłużeniu terminu na odpowiedź, z podaniem przyczyn opóźnienia). Przepis ten, w przypadku żądania kopii danych, należy czytać razem z art. 5 ust. 4 OchrDanychU.

Podstawa prawna

- art. 12 ust. 3, 5 i 6, art. 15 ust. 3 i 4, art. 20, art. 23 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1)
- art. 5 ustawy z 10.5.2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2018 r. poz. 1000 ze zm.)

Podsumowanie

Zróżnicowanie przez ustawodawcę traktowania sektora prywatnego i publicznego wydaje się być, w określonych sytuacjach, działaniem usprawiedliwionym. Przede wszystkim uzasadnia je charakter zadań wykonywanych przez ten drugi i skala przetwarzanych przez ten sektor danych osobowych. Wykonywanie prawa do otrzymania kopii danych osobowych podlegających przetwarzaniu oraz prawa do przenoszenia danych stanowi potencjalnie bardzo poważne obciążenie dla sektora publicznego, które w skrajnych przypadkach mogłoby zakłócić prawidłowe funkcjonowanie poszczególnych administratorów danych działających w tym obszarze. Nie powinno więc dziwić, że tak unijny, jak i polski ustawodawca, zdecydowali się ograniczyć możliwość korzystania z obu ww. uprawnień. W przypadku prawa do przenoszenia danych, odpowiednie ograniczenia ustanowiono bezpośrednio na poziomie unijnym. Z kolei w odniesieniu do prawa do otrzymania kopii danych, kluczowe są wymogi wskazane w art. 5 OchrDanychU, a także wciąż procedowane zmiany w przepisach sektorowych. Takie rozwiązania z jednej strony pozwalają na uniknięcie możliwego paraliżu działania administracji publicznej, który mógłby wyniknąć w przypadku zbyt dużej liczy żądań, z drugiej strony ograniczają uprawnienia osób, których dane dotyczą. Dlatego też wydaje się że, przede wszystkim w kontekście ograniczeń prawa do otrzymania kopii danych, należy je stosować z rozwagą, upewniwszy się, że spełnione są wszystkie wymagane przepisami prawa przesłanki. Pełnej jasności co do praktyki stosowania nowych przepisów dostarczy zapewne dopiero orzecznictwo sądów.

legalis administracja

Transmitowanie i nagrywanie obrad rady gminy a ochrona danych osobowych

dr hab. Paweł Fajgielski, prof. KUL
Kierownik Katedry Prawa Technologii Informacyjnych i Komunikacyjnych na Wydziale Prawa, Prawa Kanonicznego i Administracji KUL Jana Pawła II

Nowelizacją ustaw samorządowych – dokonaną 11.1.2018 r. – nałożono na jednostki samorządu terytorialnego (od nowej kadencji) obowiązek transmitowania i nagrywania obrad organów kolegialnych JST (rady gminy, rady powiatu oraz sejmiku województwa). Wprowadzenie tego obowiązku pociąga za sobą wiele problemów praktycznych. W niniejszym artykule omówione zostaną problematyczne zagadnienia dotyczące ochrony prywatności i ochrony danych osobowych w związku z transmisją i nagrywaniem obrad, przy czym kwestie te zostaną ukazane na przykładzie rady gminy – odpowiednio odnoszą się one również do organów kolegialnych pozostałych JST.

Zagwarantowanie jawności

Jawność działań organów publicznych, realizowana w postaci dostępu do informacji publicznych, obejmuje m.in. możliwość wstępu obywateli na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu (zagwarantowaną w art. 61 ust. 1 Konstytucji Rzeczypospolitej Polskiej z 2.4.1997 r.. Uszczegółowieniem przepisu Konstytucji RP jest art. 7 ust. 1 pkt 3 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.; dalej: DostInfPubU), w którym obok wstępu na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, przewidziano również udostępnianie materiałów, w tym audiowizualnych i teleinformatycznych, dokumentujących te posiedzenia, natomiast w art. 18 ust. 3 DostInfPubU wskazano, że w miarę potrzeby zapewnia się transmisję audiowizualną lub teleinformatyczną z posiedzeń.

Na szczeblu gminy jawność jest gwarantowana w art. 11b ustawy z 8.3.1990 r. o samorządzie gminnym (t.j. Dz.U. z 2018 r. poz. 994 ze zm.; dalej: SamGminU), który przewiduje m.in. prawo wstępu obywateli na sesje rady gminy. Jednak względy lokalowe (ograniczona liczba miejsc dla publiczności w salach, w których odbywają się sesje) sprawiają, że ze wskazanego uprawnienia korzystać może jedynie niewielka liczba osób. Aby zapewnić powszechną możliwość obserwowania przebiegu obrad rady gminy, w wielu gminach wprowadzono internetowe transmisje audiowizualne z sesji rad oraz publikację na stronach internetowych nagrań przebiegu sesji. Podstawą prawną podejmowania takich działań

były dotąd wspomniane powyżej przepisy DostInfPubU. W niektórych gminach nagrywanie przebiegu sesji rady było wykonywane w odmiennym celu – dla ułatwienia sporządzenia protokołu, bez udostępniania nagrań na stronach internetowych. W praktyce kwestia statusu nagrań i ich udostępniania była problematyczna, czego dowodem są niejednolite orzeczenia sądów administracyjnych w tym zakresie[1]. Jednak przepisy DostInfPubU nie nakładają bezwzględnego obowiązku transmitowania czy nagrywania posiedzeń rady gminy, przewidują jedynie taką możliwość.

Na mocy art. 1 pkt 6 ustawy z 11.1.2018 r. o zmianie niektórych ustaw w celu zwiększenia udziału obywateli w procesie wybierania, funkcjonowania i kontrolowania niektórych organów publicznych (Dz.U. z 2018 r. poz. 130 ze zm.; dalej: ZwUdzObywU), w dodanym wskutek nowelizacji art. 20 ust. 1b SamGminU, wprowadzony został obowiązek transmitowania i rejestracji obrad rad gmin. Zgodnie ze wskazanym powyżej przepisem: „Obrady rady gminy są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk. Nagrania obrad są udostępniane w Biuletynie Informacji Publicznej i na stronie internetowej gminy oraz w inny sposób zwyczajowo przyjęty". Analogiczny obowiązek wprowadzono również w odniesieniu do rad powiatów (art. 15 ust. 1a ustawy z 5.6.1998 r. o samorządzie powiatowym, t.j. Dz.U. z 2018 r. poz. 995 ze zm.) oraz sejmików samorządowych (art. 21 ust. 1a ustawy z 5.6.1998 r. o samorządzie województwa, t.j. Dz.U. z 2018 r. poz. 913 ze zm.). Zgodnie z przepisem art. 15 nowelizacji, obowiązek transmitowania i rejestracji obrad będzie miał zastosowanie do kadencji organów jednostek samorządu terytorialnego następujących po kadencji, w czasie której ustawa ta weszła w życie, a więc do kadencji organów wybranych w wyborach samorządowych jesienią 2018 r. Pociąga to za sobą konieczność przygotowania się do realizacji nałożonych na JST obowiązków i nasuwa wiele wątpliwości oraz problemów.

Jawność obrad a ochrona prywatności i ochrona danych osobowych

Jedną z kwestii problematycznych, związanych z transmitowaniem i udostępnianiem nagrań sesji rady gminy jest relacja między jawnością obrad a koniecznością ochrony prywatności osób niepełniących funkcji publicznych, których wizerunek i inne dane osobowe mogą być ujawniane. *Prima facie* wydawać by się mogło, że wprowadzenie obowiązku transmitowania przebiegu obrad oraz udostępniania nagrań rozstrzyga ten problem, ponieważ przepis przewidujący wskazany obowiązek może być odczytywany jako podstawa dopuszczalności przetwarzania danych osobowych (zgodnie z art. 6 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1–88; dalej: RODO), gdyż można uznać, że przetwarzanie danych w tym przypadku jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Jednak szczegółowa analiza przepisów dotyczących ochrony wizerunku i ochrony prawa do prywatności w kontekście udostępniania informacji publicznej wskazuje, że kwestia ta jest znacznie bardziej złożona i problematyczna. Nie ulega wątpliwości, że dane osobowe (w tym również wizerunki) osób pełniących funkcje publiczne, mające związek z pełnioną funkcją, objęte są jawnością i podlegają udostępnieniu na zasadach określonych w przepisach o dostępie do informacji publicznej. Nie można jednak niejako automatycznie rozciągać jawności na dane osobowe osób prywatnych, tylko dlatego, że są one uczestnikami sesji rady gminy. Istotę problemu można ukazać na następującym przykładzie praktycznym: w sesji rady gminy uczestniczy osoba fizyczna niepełniąca funkcji publicznej, która złożyła skargę na działania wójta – osoba ta przedstawia się podając imię, nazwisko, adres zamieszkania, a opisując szczegóły podaje także informacje na temat stanu swojego zdrowia. Wizerunek tej osoby również zostaje zarejestrowany. Pociąga to za sobą wątpliwość natury zasadniczej: czy informacje, które dotyczą sfery prywatnej tej osoby, mogą być publikowane, czy też nie powinny być ujawnianie, gdyż podlegają ochronie prawnej?

Argumentem, który zazwyczaj podnoszony jest na korzyść jawności, a zatem również możliwości publikowania tego rodzaju informacji, jest przyjęcie założenia, że skoro osoba uczestniczy w sesji rady gminy i wypowiada się publicznie, to poprzez swoje działania rezygnuje z przysługującego jej prawa do ochrony prywatności. Jednak tego rodzaju założenie jest wadliwe, gdyż prawo do udziału w sesji rady gminy stanowi przejaw realizacji prawa dostępu do informacji publicznej i nie wiąże się z obowiązkiem ujawniania danych osobowych czy też informacji ze sfery prywatności, natomiast przepis art. 5 ust. 2 DostInfPubU wyraźnie przewiduje ograniczenie dostępu do informacji publicznej ze względu na prywatność osoby fizycznej. Przyjęcie wskazanego powyżej wniosku o konieczności rezygnacji z prawa do prywatności mogłoby prowadzić

[1] Por. *T. Szewc*, Glosa do wyroku NSA z 15.6.2016 r., I OSK 3162/14; Udostępnienie fonogramu sesji rady, Orzecznictwo w Sprawach Samorządowych 2018, Nr 1, s. 132–136 i wskazane tam orzeczenia.

do istotnego ograniczenia czynnego udziału obywateli w życiu publicznym (np. do powstrzymywania się od składania skarg w obawie przed ujawnieniem informacji ze sfery ich życia prywatnego).

Podobny wniosek na rzecz jawności jest formułowany, gdy chodzi o możliwość wykorzystywania wizerunku – skoro osoba uczestniczy w sesji rady, to wizerunek osoby nie jest chroniony, ponieważ sesja rady odbywa się w miejscu publicznym i jest jawna. Jednak szczegółowa analiza przepisów określających zasady wykorzystania wizerunku nie potwierdza takiej interpretacji. Zgodnie z art. 81 ust. 2 ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2018 r. poz. 1191 ze zm.) zezwolenia nie wymaga rozpowszechnianie wizerunku:

1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Oznacza to, że można bez zezwolenia publikować wykonane podczas sesji rady zdjęcia (oraz filmy) ukazujące wizerunki osób pełniących funkcje publiczne, natomiast w przypadku osób, które funkcji takich nie pełnią, o ile prawnie dopuszczalne jest opublikowanie wizerunku osoby obecnej na sesji rady, widocznej w otoczeniu innych osób uczestniczących w posiedzeniu (grupowe zdjęcie, nagranie przedstawiające grupę osób obecnych na sali obrad), to już publikacja wizerunku w postaci zdjęcia bądź nagrania, na którym widoczna jest tylko jedna osoba (zbliżenie ukazujące twarz tej osoby), wymaga uzyskania zezwolenia (zgody) tej osoby na rozpowszechnianie jej wizerunku, gdyż w tym przypadku osoba ta nie stanowi „szczegółu całości", co jest przesłanką dopuszczalności wykorzystania wizerunku określoną przepisami.

Dostęp do informacji publicznej a ochrona prywatności w orzecznictwie sądów

Obowiązek transmisji i udostępniania nagrań posiedzeń rady gminy stanowi nowe rozwiązanie w porządku prawnym, jednak problem ochrony prywatności w kontekście udostępniania informacji publicznej pojawiał się już wcześniej i był przedmiotem rozstrzygnięć judykatury. Problem ten uwidocznił się przy publikowaniu na stronach internetowych uchwał rady gminy oraz udostępnianiu tych dokumentów w Biuletynie Informacji Publicznej. Publikowanie i udostępnianie dokumentów w niezmienionej postaci (zawierających dane osobowe) uznawane jest w orzecznictwie za praktykę naruszającą art. 5 ust. 2 DostInfPubU, gdyż może prowadzić do naruszenia prawa do prywatności osób niepełniących funkcji publicznych, których dane są w ten sposób ujawniane.

W wyroku z 14.3.2013 r. (I OSK 620/12, Legalis) Naczelny Sąd Administracyjny stwierdził, że w sprawie, „w której udostępnieniu w BIP podlegała informacja o sposobie załatwienia przez Radę Gminy skargi osoby fizycznej, niepełniącej funkcji publicznej, na działalność Wójta Gminy, wzgląd na ochronę prawa do prywatności tej osoby uzasadniał pominięcie w informacji zamieszczonej w Biuletynie danych personalnych tej osoby". Naczelny Sąd Administracyjny podzielił argumentację przedstawioną w I instancji przez WSA, który dokonał odróżnienia jawności posiedzenia rady od udostępniania informacji publicznej w BIP. O ile w trakcie posiedzenia dane zostały ujawnione, to – w ocenie sądu – nie oznacza, że powinny one zostać udostępnione w BIP. Jeżeli chodzi o rejestrację obrad, o której mowa w art. 19 SamGminU, NSA wskazał, że „w przepisie tym jest mowa o sporządzeniu i udostępnieniu informacji. Nie oznacza to jednak, że w przypadku rejestracji obejmującej całość obrad organ jest zwolniony z respektowania zasad chroniących dane osobowe ze względu na prywatność osoby fizycznej (art. 5 ust. 2). Jeżeli udostępnienie tych treści naruszałoby prywatność osoby fizycznej, wówczas, mimo sporządzenia materiałów audiowizualnych rejestrujących w pełni obrady, nie będą one udostępniane w takim zakresie, w jakim godziłyby w dobra podlegające ochronie. Szczególnie regulacja zawarta w art. 19 dotycząca środków technicznych służących do utrwalania przebiegu obrad nie zwalnia organów ze stosowania zasad ogólnych regulujących prawo dostępu do informacji, a w szczególności przepisów ograniczających ten dostęp ze względów, o których mowa w art. 5 ust. 1 i 2 ustawy". Argumenty te są aktualne również na gruncie art. 20 ust. 1b SamGminU.

Zasadność anonimizacji danych osobowych w treści uchwał była kwestionowana przez organy jst m.in. dlatego, że może to prowadzić do braku czytelności uchwały. Jednak kwestionując ten argument, sąd administracyjny uznał w jednym z orzeczeń, że „usunięcie personaliów osób prywatnych, czy też ich zanonimizowanie w ogłoszonej w BIP uchwale organu gminnego, nie wpływa na czytelność dokonanego w ten sposób przekazu. W tym przypadku treść aktu administracyjnego nie traci waloru informacyjnego, albowiem wynika z niej kto, kiedy i w jakiej sprawie publicznej zajął określone stanowisko" (wyr. WSA w Warszawie z 18.11.2008 r., II SA/Wa 1177/08, Legalis).

Warto również zwrócić uwagę na to, że naruszenie prawa do prywatności poprzez ujawnienie danych osobowych na stronie internetowej gminy,

może być podstawą do roszczeń dochodzonych przed sądem cywilnym. W jednym z wyroków z 8.5.2014 r. w sprawie (XXIV C 1183/13, Legalis) sąd okręgowy w Warszawie zasądził od pozwanej gminy na rzecz powódki kwotę 15 000 zł wraz z odsetkami, tytułem zadośćuczynienia za naruszenie jej dóbr osobistych m.in. poprzez bezprawne zamieszczenie na stronie internetowej gminy oraz w BIP urzędu gminy danych osobowych powódki, m.in. w opublikowanej tam uchwale rady gminy. Sąd okręgowy stwierdził, że: „W odniesieniu zaś do publikacji danych osobowych powódki wskazano dodatkowo, że zgodnie z art. 5 ust. 2 cytowanej wyżej ustawy [red. DostInfPubU] prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej, chyba że osoba ta pełni funkcje publiczne lub zrezygnowała z przysługującego jej prawa. Z powyższego wynikało, że jakkolwiek art. 8 ust. 3 w zw. z art. 6 ust. 1 pkt 4 lit. a) [ustawy] o dostępie do informacji publicznej zobowiązuje organ gminy do udostępnienia informacji w postaci uchwał rady gminy w Biuletynie Informacji Publicznej, to nakaz ten nie obejmuje publikacji danych osobowych prywatnej osoby fizycznej. Niewątpliwie zatem publikacja danych osobowych powódki miała w przedmiotowej sprawie charakter bezprawny". Sąd apelacyjny w Warszawie, oddalając apelację w dniu 13.5.2015 r. (I ACa 1753/14, Legalis), uznał rozstrzygnięcie sądu niższej instancji za prawidłowe oraz wskazał na to, że: „W sprawie, w której udostępnieniu w BIP podlegała informacja o sposobie załatwienia przez Radę Gminy skargi osoby fizycznej, niepełniącej funkcji publicznej, na działalność Wójta Gminy, wzgląd na ochronę prawa do prywatności tej osoby uzasadniał pominięcie w informacji zamieszczonej w Biuletynie danych personalnych tej osoby. Ograniczenie to znajduje w pełni uzasadnienie w omawianym przepisie art. 5 ust. 2 ustawy [DostInfPubU] oraz art. 61 ust. 3 Konstytucji. Z przepisów tych wynika, że ustawodawca kreując prawo obywateli do uzyskiwania informacji o działalności organów władzy publicznej, jako dobro nadrzędne nad prawem dostępu do informacji, usytuował ochronę prywatności osób fizycznych".

Transmitowanie i nagrywanie obrad – możliwe interpretacje i sposoby postępowania

Jak wskazano powyżej, sformułowanie przepisów nakładających obowiązek transmitowania i nagrywania obrad sesji rady gminy oraz ich relacja do przepisów dotyczących ochrony prywatności są niejasne i mogą być różnie interpretowane, a co za tym idzie – mogą prowadzić do różnych sposobów postępowania podmiotów, które będą realizować transmisje oraz publikować nagrania na stronach internetowych.

Najprostszym sposobem wykładni omawianych przepisów jest przyjęcie, że przepisy nakładające obowiązek transmisji i nagrywania obrad, będące podstawą przetwarzania danych osobowych, stanowią wystarczającą podstawę do udostępniania zawartych tam informacji, bez względu na to, czy informacje te dotyczą osób pełniących funkcje publiczne, czy też nie. Przyjęcie takiej interpretacji prowadzić może w praktyce do transmitowania obrad i udostępniania nagrań bez dokonywania jakichkolwiek działań mających na celu ochronę informacji dotyczących osób niepełniących funkcji publicznych. Podejście takie nie wydaje się jednak właściwe, z uwagi na przedstawione powyżej przepisy dotyczące ochrony wizerunku oraz wyłączenia jawności w zakresie ochrony prywatności, a także sposób ich wykładni prezentowany w orzecznictwie sądowym. Jeżeli organ gminy chciałby oprzeć się na takim stanowisku, to powinien mieć świadomość ryzyka prawnego, jakie wiąże się z zarzutem naruszenia prawa do prywatności oraz prawa do ochrony wizerunku i konsekwencjami, jakie z tego mogą wyniknąć.

Wydaje się, że prawidłowym sposobem interpretacji omawianych przepisów jest przyjęcie, że obowiązek transmisji i nagrywania (udostępniania nagrań) obrad podlega ograniczeniom wynikającym z konieczności poszanowania prawa do wizerunku oraz uwzględnienia wyłączeń jawności w stosunku do osób, które nie pełnią funkcji publicznych. Taka wykładnia pozwala realizować postulat jawności przy jednoczesnym ograniczeniu ryzyka prawnego, o którym mowa powyżej. W praktyce przyjęcie zaproponowanej interpretacji prowadzi jednak do trudności natury technicznej i organizacyjnej, związanych z koniecznością anonimizacji danych osób prywatnych, w tym ograniczenia ujawniania ich wizerunku.

Ważne

Anonimizacja może być dokonywana podczas trwania sesji rady – już na etapie transmisji (nagrywania), bądź w terminie późniejszym – poprzez edycję sporządzonego wcześniej nagrania.

Anonimizacja dokonywana w trakcie sesji może polegać m.in. na takim ustawieniu kamery, które uniemożliwia ukazanie wizerunku jednej osoby niepełniącej funkcji publicznej (pokazuje wiele osób uczestniczących w sesji w charakterze publiczności) i wyciszaniu dźwięku w czasie, gdy osoba niepełniąca funkcji publicznej podaje swoje dane, natomiast anonimizacja dokonywana w terminie późniejszym może polegać na zamazywaniu obrazu i przekształcania dźwięku, tak aby uczynić nieczytelnymi wizerunek i inne dane osobowe osób, które funk-

cji publicznych nie pełnią (analogicznie do praktyki zaczerniania danych zawartych w dokumentach publikowanych na stronach internetowych). Zarówno działania zmierzające do anonimizacji uprzedniej, jak i następczej mogą być uciążliwe dla osób, które będą je realizowały, jednak pozwalają one pogodzić jawność obrad z koniecznością ochrony prywatności oraz wizerunku osób niepełniących funkcji publicznych.

Wartym rozważenia rozwiązaniem jest uzyskiwanie od osób niepełniących funkcji publicznych zezwolenia (zgody) na rozpowszechnianie wizerunku i ujawnienie danych osobowych. Praktyka taka nie powinna jednak prowadzić do wymuszania zgody ani też ograniczania prawa udziału w sesjach rady osobom, które takiej zgody nie wyraziły (za niedopuszczalne uznać należy uzależnienie uczestnictwa w obradach od wyrażenia zgody). Odbieranie zgody od wszystkich osób uczestniczących w sesji rady w charakterze publiczności nie wydaje się rozwiązaniem właściwym, ponieważ sam fakt udziału w sesji rady nie stanowi ingerencji w prywatność tych osób (nie wiąże się – co do zasady – z koniecznością ujawniania danych osobowych, zwłaszcza szczególnych kategorii danych), a rozpowszechnianie wizerunku osób stanowiących element większej całości, takiej jak sesja rady, jest prawnie dopuszczalne i nie wymaga zgody. Przyjmowanie założenia, że udział osoby w sesji rady oznacza jej zgodę na udostępnianie danych i rozpowszechnianie wizerunku jest zbyt daleko idące, ponieważ uczestnictwo w obradach stanowi uprawnienie, które nie jest zależne od zgody na przetwarzanie danych (osoba może uczestniczyć w sesji rady, a jednocześnie może nie godzić się na publikowanie jej wizerunku i ujawnianie danych). Przepisy RODO nawet w przypadku, gdyby zgoda miała być wywodzona z „wyraźnego działania potwierdzającego" wymagają, aby zgoda była dobrowolna, konkretna, świadoma i jednoznaczna[4]. Możliwa do przyjęcia jest praktyka pytania o zgodę na rozpowszechnianie wizerunku i ujawnianie danych osoby, która funkcji publicznej nie pełni, a zamierza zabrać głos na sesji, przed udzieleniem jej głosu, a w przypadku niewyrażenia przez tę osobę zgody – dokonywanie anonimizacji jej danych.

Na kanwie omawianych przepisów można zastanawiać się, czy nie należałoby przyjąć odmiennych reguł odnośnie do transmisji, a odmiennych w stosunku do udostępniania nagrań. Wątpliwość taka powodowana jest okolicznościami faktycznymi związanymi z udziałem w posiedzeniu rady gminy. Skoro każdy ma prawo uczestnictwa w obradach, a także możliwość rejestracji obrazu i dźwięku, to transmisja w czasie rzeczywistym (*on-line*) stanowiąca realizację tego uprawnienia powinna stwarzać tej osobie takie same możliwości, jakie ma osoba fizycznie obecna na sesji rady, natomiast inaczej należałoby traktować nagrania udostępniane na stronach internetowych, w przypadku których można dopatrywać się analogii do zasad udostępniania dokumentów na stronach internetowych organów publicznych. Jednak prawodawca nie uregulował tych kwestii w sposób szczegółowy, co powinno skłaniać organy do ostrożności i przyjmowania wykładni oraz rozwiązań praktycznych pozwalających ograniczyć ryzyko prawne związane z formułowaniem zarzutów naruszenia prywatności i bezprawnego rozpowszechniania wizerunku.

Podstawa prawna

- art. 61 ust. 1 ustawy z 2.4.1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. Nr 78, poz. 483 ze zm.)
- art. 5 ust. 2, art. 7 ust. 1 pkt 3, art. 18 ust. 3 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.)
- art. 11b, art. 20 ust. 1b ustawy z 8.3.1990 r. o samorządzie gminnym (t.j. Dz.U. z 2018 r. poz. 994 ze zm.)
- art. 15 ust. 1a ustawy z 5.6.1998 r. o samorządzie powiatowym (t.j. Dz.U. z 2018 r. poz. 995 ze zm.)
- art. 21 ust. 1a ustawy z 5.6.1998 r. o samorządzie województwa (t.j. Dz.U. z 2018 r. poz. 913 ze zm.)
- art. 6 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1–88)
- art. 1 pkt 6 ustawy z 11.1.2018 r. o zmianie niektórych ustaw w celu zwiększenia udziału obywateli w procesie wybierania, funkcjonowania i kontrolowania niektórych organów publicznych (Dz.U. z 2018 r. poz. 130 ze zm.)

[2] Szerzej na temat podstaw dopuszczalności przetwarzania danych, w tym zgody por. *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, s. 126–130 oraz s. 157 i n.

Podsumowanie

Wprowadzenie obowiązku transmitowania i rejestracji obrad kolegialnych organów samorządowych jest rozwiązaniem prawnym, które może przyczynić się do pełniejszej realizacji jawności życia publicznego i zwiększy możliwość kontroli sprawowania władzy publicznej przez organy jednostek samorządu terytorialnego. Jednak można wyrazić ubolewanie, że prawodawca, wprowadzając ten obowiązek, poprzestał na bardzo ogólnym sformułowaniu przepisu i nie przewidział bardziej szczegółowych regulacji, które pozwoliłyby uniknąć problemów omówionych w niniejszym opracowaniu. Warto postulować, aby ustawodawca pochylił się ponownie nad tą problematyką i rozważył możliwość uzupełniania regulacji o szczegółowe normy, jednoznacznie przesądzające wątpliwości wskazane powyżej.

Nadmiarowe upublicznianie danych w sieci

Monika Krasińska
Dyrektor Zespołu ds. Sektora Publicznego w Urzędzie Ochrony Danych Osobowych. Wieloletni wykładowca akademicki

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 96/45/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L Nr 119, s. 1; dalej: RODO), stosowane i egzekwowane od 25.5.2018 r., wywarło ogromny wpływ na realizację wszystkich procesów przetwarzania danych osobowych zarówno w sektorze publicznym, jak i w prywatnym. Ten akt, stanowiący kolejny etap ewolucji standardów ochrony danych osobowych w UE, zmusił wielu administratorów do przeglądu istniejących zasobów informacji pod kątem ochrony danych osobowych, a osoby, których dane są przetwarzane, do ponownego oszacowania wartości własnej prywatności.

Dane osobowe – nie bez przyczyny nazywane walutą XXI wieku – w świetle RODO stały się przedmiotem wzmocnionej ochrony prawnej. Równocześnie, przy zachowaniu określonych standardów przetwarzania, są materiałem, z wykorzystaniem którego firmy mogą budować nowe modele biznesowe, poszerzać swoje rynki zbytu, stawać się bardziej konkurencyjnymi w dobie rozwoju coraz bardziej wyrafinowanych technologii. Wiele procesów komunikacji przeniosło się do rzeczywistości wirtualnej. Coraz więcej zasobów informacyjnych jest przechowywanych w sieci, w tzw. chmurze. Intencją prawodawcy unijnego i krajowego jest jak najszybsze przejście na etap gospodarki cyfrowej w zintegrowanej Europie. Państwa UE dążą do zagwarantowania także zmian w zakresie funkcjonowania administracji publicznej, która ma być bardziej otwarta na obywatela, bardziej przyjazna w komunikacji i transparentna w realizacji swoich zadań. Trudno wyobrazić sobie realizację tych wszystkich celów bez uwzględnienia korzyści, ale i ryzyk związanych z przetwarzaniem danych osobowych – w konsekwencji bez uwzględnienia zasad RODO.

Rozporządzenie wyraźnie wskazuje, że aby zapobiec ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik (motyw 15 RODO). Neutralność tech-

nologiczna zagwarantowana w RODO ma ogromne znaczenie przy określaniu sposobów przetwarzania danych i doborze środków, za pomocą których będą przetwarzane. Realizacja wszystkich obowiązków przy zastosowaniu adekwatnych rozwiązań techniczno-organizacyjnych oraz odpowiedzialność za wykazanie przestrzegania zasad RODO staje się kluczowym elementem dla zalegalizowania jakichkolwiek inicjatyw z udziałem danych osobowych (art. 5 ust. 2 RODO). Zapewnienie jak najwyższego poziomu realizacji zasady rozliczalności leży więc w interesie każdego administratora i przetwarzającego dane, a zwłaszcza w przypadku przetwarzania danych osobowych w środowisku tak naprawdę wciąż tajemniczym i nierozpoznanym, tj. w Internecie.

Upublicznianie a przetwarzanie

Rozporządzenie, choć zdefiniowało pojęcie przetwarzania, nie określa wszystkich czynności, jakie mogą stanowić przetwarzanie. Jedynie przykładowo wyliczone są operacje lub zestawy operacji, jakie mogą być wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany (art. 4 pkt 2 RODO). Wśród tych przykładów nie znajduje się wprost wymienione upublicznienie, ale wskazane jest „innego rodzaju udostępnianie". W świetle powyższego upublicznienie danych może być uznane za jedną z form ich udostępnienia. Nie zachodzi tutaj jednak relacja udostępnienia na rzecz konkretnego odbiorcy (adresata), ale kręgu odbiorców, przy czym będą to zarówno:

1) odbiorcy zidentyfikowani – upublicznienie w określonym miejscu na rzecz określonych osób (np. na zebraniu pracowników);
2) odbiorcy niezidentyfikowani – upublicznienie na rzecz użytkowników określonej przestrzeni (np. na stronie BIP, na sesji rady gminy, na słupie ogłoszeniowym itp.).

Żeby doszło do przetworzenia danych poprzez upublicznienie, muszą być zrealizowane następujące przesłanki:

1) upublicznienie musi być dokonane przez człowieka działającego bezpośrednio lub za pomocą określonej technologii (decyzja o zastosowaniu określonego algorytmu);
2) upublicznienie musi dotyczyć danych osobowych (nie będzie upublicznieniem danych osobowych ujawnienie informacji publicznej, w zakres której wchodzą wyłącznie informacje o charakterze statystycznym lub ujawnione w ten sposób dane będą dotyczyć osób prawnych albo nieposiadających osobowości prawnej jednostek organizacyjnych);
3) upublicznienie musi stanowić operację lub zestaw operacji, a więc być działaniem zmierzającym do wykonania określonego celu[1].

Upublicznić, oznacza podać do powszechnej wiadomości[2]. Upublicznienie nie jest tożsame z pojęciem upowszechnienia, które oznacza uczynić coś popularnym, ogólnie stosowanym[3].

Ważne

Upublicznienie określonych informacji, które albo mogą być danymi osobowymi, albo zawierać w sobie także element danych osobowych, wiąże się zatem z procesem udostępnienia danych w sposób czyniący je powszechnie dostępnymi.

Powszechna dostępność informacji rodzi natomiast określone konsekwencje i ryzyka, jakich nie doświadcza informacja znajdująca się w wyłącznym posiadaniu konkretnego administratora, czy też przetwarzającego z polecenia administratora.

Podstawy prawne upublicznienia danych – zasada legalizmu, rzetelności i przejrzystości

Żeby przetwarzanie danych osobowych było zgodne z prawem, muszą zostać spełnione określone w RODO przesłanki. Dla danych zwykłych przesłanki te statuuje art. 6 RODO, a w przypadku przetwarzania szczególnych kategorii danych art. 9 ust. 2 RODO. Przesłanki ukształtowane treścią przywołanych przepisów mają charakter alternatywny, tzn. spełnienie przynajmniej jednej z nich warunkuje uznanie przetwarzania danych osobowych za proces legalny. Z punktu widzenia legalności przetwarzania danych przez organy władzy publicznej, nie wszystkie z przesłanek określonych w art. 6 RODO mogą być przywoływane dowolnie. Ponieważ organy władzy publicznej są upoważnione do działania wyłącznie na podstawie i w granicach prawa (art. 7 ustawy z 2.4.1997 r. – Konstytucja Rzeczypospolitej Polskiej, Dz.U. Nr 78, poz. 483 ze zm.), zasadnicze znaczenie dla administratorów z tego sektora przetwarzających dane dla realizacji swoich zadań ma art. 6 ust. 1 lit. c) RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze) i art. 6 ust. 1 lit. e) RODO (przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi). Powinna zatem istnieć podstawa prawna określona w prawie krajowym lub prawie UE, któremu podlega administrator. Administrator z sektora publicznego nie może zatem w zakresie upubliczniania danych osobowych, np. poprzez

[1] Por. RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. nauk. *E. Bielak-Jomaa*, *D. Lubasz*, Warszawa 2018, s. 188.
[2] http://sjp.pwn.pl/slowniki/upublicznienie.html.
[3] https://sjp.pwn.pl/szukaj/upowszechnienie.html.

umieszczenie ich w BIP, powoływać się na przesłankę swego prawnie uzasadnionego interesu, gdyż przesłanka z art. 6 ust. 1 lit. f) RODO[4] nie może mieć zastosowania do przetwarzania danych przez organy publiczne w ramach realizacji przez nie swoich zadań (art. 6 ust. 1 ak. 2 RODO). Przesłanka ta może mieć z kolei zastosowanie, gdy przedsiębiorca, dążąc do zapewnienia jak najlepszej jakości swoich usług, upublicznia na stronie internetowej swojej firmy dane kontaktowe swoich pracowników.

Przepisami, na podstawie których w sektorze publicznym będzie dochodziło do upublicznienia danych, będą przykładowo przepisy ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.; dalej: DostInfPubU). Nie zawierają one wprawdzie wprost norm określających konieczność udostępnienia danych osobowych, gdyż odnoszą się do pojęcia informacji publicznej, ale w ich oparciu administrator udostępniający dane osobowe w BIP może skutecznie powoływać się na przesłankę niezbędności wykonania zadania w interesie publicznym lub w ramach sprawowania powierzonej mu władzy publicznej (art. 6 ust. 1 lit. e) RODO). W przepisach tych została także pośrednio wyrażona zasada adekwatności przetwarzania, gdyż na ich podstawie prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa (art. 5 ust. 2 DostInfPubU).

Przy upublicznianiu danych osobowych, organy władzy publicznej powinny także z dużą dozą ostrożności sięgać po przesłankę zgody, o której mowa w art. 6 ust. 1 lit. a) RODO. Jeśli bowiem w oparciu o tę przesłankę odbywa się przetwarzanie, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, zgodę tę wyraziła, że jest świadoma tego faktu, tak co do zakresu tej zgody, jak i celu, dla którego przetwarzanie na podstawie zgody będzie realizowane. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji (motyw 42 RODO). RODO określa szczególne gwarancje dla osób, których dane przetwarzane są z wykorzystaniem przesłanki zgody. Badanie, chociażby warunku dobrowolności jej udzielenia, powinno być uzależnione m.in. od zbadania środowiska relacji zachodzących pomiędzy tą osobą a administratorem. W sytuacji, gdy istnieje pomiędzy nimi wyraźny brak równowagi, a w szczególności gdy administrator jest podmiotem publicznym i dlatego mało prawdopodobne jest, że w tej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach, zgody takiej nie można uznawać za dobrowolną (motyw 43 RODO).

Ważne

Osoba wyrażająca zgodę powinna mieć także możliwość jej wycofania w każdym czasie, o czym przed pozyskaniem takiego oświadczenia powinien administrator poinformować (art. 7 RODO). Wycofanie zgody powinno być równie łatwe, jak jej wyrażenie (art. 7 RODO).

Wraz z wykazywaniem podstawy upublicznienia w oparciu o zgodę administrator musi wykazać, że pozyskuje zgodę jedynie na upublicznienie danych adekwatnych, niezbędnych dla realizacji określonego celu. Bez poinformowania osoby o prawie cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, podmiot danych może podważać zachowanie warunków zgody świadomej. Realizacja zatem procesów upubliczniania danych w oparciu o zgodę musi odbywać się nie tylko z uwzględnieniem zasady legalizmu, ale także zasady rzetelności i przejrzystości (art. 13 ust. 2 pkt c) oraz art. 14 ust. 2 pkt d) RODO). W przypadku upublicznienia danych w sieci, administratorzy działający z uwzględnieniem tych zasad, powinni jasnym, prostym językiem zakomunikować, w jaki sposób i w jakim zakresie autonomia informacyjna jednostki będzie doznawać ograniczeń. Chodzić tutaj będzie m.in. o wskazanie podstaw prawnych udostępnienia, kategorii odbiorców, okresu, przez który dane będą przechowywane, a gdy nie jest to możliwe, kryteriów ustalania tego okresu. Poinformowanie o prawach podmiotów danych przy tej okazji jest także istotne. Osoba powinna mieć informacje, czy służy jej prawo do zgłoszenia żądania usunięcia danych z miejsca, gdzie zostały upublicznione, czy też poinformowana o prawie zgłoszenia sprzeciwu wobec takiego przetwarzania. Ograniczenie przekazanych informacji w tym zakresie lub też ich nieprzekazanie będzie wpływać na ocenę zarówno wyrażonej zgody, jak i całościową ocenę procesu legalności przetwarzania na podstawie innych niż zgoda przesłanek.

Nie powinno dochodzić do pozyskiwania zgód w sytuacji istnienia przepisów prawa regulujących obowiązek czy też wyłącznie uprawnienie do

[4] Zgodnie z art. 6 ust. 1 lit. f) RODO przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

upublicznienia danych. W takiej bowiem sytuacji osoba jest wprowadzana *de facto* w błąd, co do skuteczności jej oświadczenia woli. Przykładowo, udostępnienie w BIP danych osobowych osoby piastującej funkcję organu lub działającej z upoważnienia organu i podpisującej decyzję administracyjną będzie realizacją przepisów prawa dostępu do informacji publicznej w zakresie, w jakim przepisy prawa przewidują obowiązek publikacji informacji o osobach pełniących funkcje publiczne w związku z realizacją tych funkcji[5]. Przesłanka zgody nie może być także wykorzystywana do „omijania" obowiązujących reguł prawnych. W sytuacji, gdy szkoły i placówki publikują listy kandydatów zakwalifikowanych i niezakwalifikowanych oraz przyjętych i nieprzyjętych, powinny czynić to w swojej siedzibie, a nie na stronach internetowych szkoły. Wynika to wprost z art. 157 ust. 2 pkt 2 i art. 158 ust. 1, 3 i 4 ustawy z 14.12.2016 r. – Prawo oświatowe (t.j. Dz.U. z 2018 r. poz. 996 ze zm.). Zatem publikowanie wyników procesu rekrutacyjnego na stronie internetowej szkoły jest niedopuszczalne, niezależnie od tego, czy na taką publikację wyraził zgodę uczeń lub opiekun prawny ucznia.

W orzecznictwie sądów administracyjnych odnoszącym się do relacji prawa do prywatności względem prawa dostępu do informacji publicznej, za wadliwe uznano stanowisko, że dane mogą znaleźć się w treści publikowanej w BIP uchwały, wówczas gdy osoba, której dane dotyczą, wyrazi na to zgodę. Jeżeli ustawa szczególna przewiduje pełną jawność dokumentu, udostępnienie informacji stanowi jednostronne działanie organu władzy publicznej. Dopuszczenie warunku, że ujawnianie danych osobowych w uchwałach jest zależne od zgody podmiotu danych prowadziłoby do „wybiórczej jawności", która – tak jak w przypadku każdorazowego badania przesłanki „zniekształcenia przekazu informacji" – ograniczy transparentność władzy samorządowej. Gdyby zaakceptować takie stanowisko, to podanie danych osobowych w uchwale będzie uzależnione od różnorodnych interesów indywidualnych osób, których dane dotyczą i nie pozwoli na pełną kontrolę społeczną nad działalnością rady, a wręcz może wprowadzać społeczeństwo w błąd (np. osoba nabywająca różne nieruchomości od jednostki samorządu terytorialnego może – w zależności od spodziewanego odbioru społecznego w stosunku do transakcji – raz wyrażać, a w innych przypadkach odmawiać zgody na ujawnienie w uchwale swoich danych osobowych)[6].

Ważne

Gdy z przepisów prawa nie będą płynęły odpowiednie prerogatywy do upublicznienia danych osobowych, a będzie istniał uzasadniony cel dla realizacji określonego zadania, poszukiwanie przesłanki zgody stanie się konieczne dla zalegalizowania umieszczania danych w przestrzeni publicznie dostępnej (np. zgoda rodziców na udostępnienie danych o wizerunku dziecka w związku z jego naukowymi osiągnięciami).

Podobne uwagi należy odnieść do upubliczniania przez organy władzy publicznej szczególnych kategorii danych osobowych. Przetwarzanie tej kategorii danych, a więc także ich upublicznianie, jest co do istoty zabronione (art. 9 ust. 1 i art. 10 RODO). Administrator decydujący się na upublicznienie danych wrażliwych ponosi szczególną odpowiedzialność za wskazanie, na jakiej podstawie prawnej będzie to czynił. Sprawując władztwo publiczne (np. administracyjne), jest zobowiązany do działania w granicach obowiązujących przepisów i ujawniając takie dane, jak np. pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych czy też dane o stanie zdrowia, ma ograniczoną swobodę w doborze przesłanek z RODO, co wynika także z przywoływanych już zasad konstytucyjnych. Z zasadą praworządności (art. 7 Konstytucji RP) koreluje przesłanka z art. 9 ust. 2 pkt g) RODO, zgodnie z którą przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne, jeżeli jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. Akcenty w tej przesłance położone są w szczególności na istnienie ważnego interesu publicznego oraz adekwatnych dla realizacji wyznaczonych celów przepisów prawa, które mają przewidywać odpowiednie i konkretne środki ochrony praw podmiotów danych.

W świetle powyższego, upubliczniając w BIP szczególne kategorie danych, organ władzy publicznej nie powinien się powoływać na przetwarzanie danych w sposób oczywisty uprzednio upublicznionych przez osobę, której dane dotyczą, np. na Facebooku (art. 9 ust. 2 pkt e) RODO). Nie oznacza to wszakże, że danych w ten sposób uprzednio upublicznionych, nie mógłby wykorzystać, np. w prowadzonym postępowaniu administracyjnym, przy spełnieniu wszystkich zasad wynikających z procedury administracyjnej[7].

[5] Por. wyr. TK z 20.3.2006 r., K 17/05 (Dz.U. Nr 49, poz. 358).
[6] Wyr. NSA z 14.3.2013 r., I OSK 620/12; Legalis.
[7] Rozdział II ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U z 2018 r. poz. 2096 ze zm.)

Minimalizacja danych w sieci

Upublicznienie danych osobowych powinna poprzedzać szczególnie staranna analiza zakresu danych osobowych poddanych wskazanemu procesowi. Kluczowe znaczenia ma przy tej analizie wyrażona w art. 5 ust. 1 lit. c) RODO zasada minimalizacji. Administrator powinien przetwarzać dane osobowe adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Dla pełnej realizacji zasady minimalizacji konieczne jest zatem:

1) **zweryfikowanie zakresu danych, które mają podlegać upublicznieniu**, przy czym weryfikacja ta powinna mieć charakter zarówno uprzedni, jak i następczy.

   Administrator powinien na jak najwcześniejszym etapie dokonać zbadania zakresu danych osobowych podlegających ujawnieniu na stronach internetowych. Taka analiza będzie niezbędna zarówno wtedy, gdy umieszczonych ma być wiele danych osobowych, jak również wtedy, gdy ze względu na ich rodzaj, kontekst i cele – publikacja danych może powodować wysokie ryzyko naruszenia praw i wolności. Zasada minimalizacji stanowi jeden z filarów, na którym opiera się zapewnienie ochrony danych w fazie projektowania (*privacy by design*) oraz towarzyszy nierozłącznie zasadzie domyślnej ochrony danych (*privacy by default*). Zgodnie z art. 25 RODO, żeby przetwarzanie danych było zgodne z przepisami o ochronie danych i w sposób efektywny chroniło prawa osób, których dane dotyczą, przy uwzględnieniu charakteru, kontekstu i celu przetwarzania oraz wynikającego z niego ryzyka dla praw i wolności osób fizycznych administratorzy mają obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych zarówno w momencie ustalania sposobów przetwarzania danych, jak i w czasie samego procesu przetwarzania. Minimalizacja danych jest jednym ze środków taką ochronę zapewniających.

   Ochrona proaktywna i prewencyjna, a nie działania naprawcze, są podwaliną koncepcji uwzględniania ochrony danych w fazie projektowania. Dlatego ustalenie zakresu danych podlegających upublicznieniu powinno być dokonane na jak najwcześniejszym etapie, np. projektowania polityki informacyjnej administratora, polityki dostępu do informacji publicznej, organizacji pracy pracodawcy czy promocji danej jednostki.

2) **zweryfikowanie celowości upubliczniania jakichkolwiek danych osobowych**, żeby nie dopuścić do nadmiarowego udostępnienia danych, administrator powinien także dokonać oceny, czy w ogóle dane osobowe powinny być upubliczniane. Przykładowo naruszeniem zasady minimalizacji będzie przetwarzanie danych osobowych w sytuacji, gdy także bez ich udostępnienia cel może zostać osiągnięty. Jeżeli można osiągnąć zakładany rezultat poprzez ujawnienie danych wyłącznie statystycznych, upublicznienie danych osobowych jawi się jako nadmiarowe. Jak wynika z art. 11 RODO, jeżeli cele, w których administrator przetwarza dane, nie wymagają lub nie wymagały zidentyfikowania osoby, nie powinien tych danych przetwarzać. Zasada przetwarzania danych niewymagających identyfikacji powinna być także stosowana przy sukcesywnym przeglądzie struktur informacji upublicznianych w Internecie, gdyż jest ściśle powiązana z zasadą ograniczenia czasowego przechowywania danych. W tym przypadku chodzi głównie o to, aby dane osobowe albo w ogóle, albo w zbyt szerokim zakresie nie funkcjonowały w obrocie publicznym.

   Adekwatną formułą minimalizacji przetwarzania danych osobowych jest **proces anonimizacji**. Przez anonimizację danych osobowych należy rozumieć technikę przekształcenia danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej czy możliwej do zidentyfikowania osoby fizycznej lub w przypadku, kiedy ustalenia takiego można by dokonać jedynie niewspółmiernie dużym nakładem kosztów i czasu. Przyjęcie zasady anonimizacji danych osobowych w treści uchwał czy też publikowanych orzeczeń sądów staje się standardem funkcjonowania administratorów z tych sektorów. Powyższe wynika zarówno z konsekwentnie od lat prezentowanych w tym zakresie stanowisk Prezesa Urzędu Ochrony Danych Osobowych (wcześniej Generalnego Inspektora Ochrony Danych Osobowych), jak i utrwalonej już linii orzeczniczej. W wielu wyrokach akcentowana jest koncepcja anonimizacji, która nie pozostaje w konflikcie z prawem do zapewnia dostępu do informacji publicznej. Uznano, że brak danych personalnych osoby, zawartych w treści uchwały rady gminy, nie zniekształci przekazu omawianej informacji publicznej. Istotą tej informacji jest przecież stanowisko, jakie zaprezentowała rada. Ten podmiot wytworzył bowiem omawianą informację. Bez wpływu na treść uchwały pozostaje zaś informacja o danych osobowych inicjatora postępowania, które zakończyło się wydaniem uchwały[8]. W ocenie sądów administracyjnych usunięcie

[8] Wyr. WSA z 24.11.2011 r. (II SA/Wa 1828/11, Legalis).

personaliów osób prywatnych, czy też ich zanonimizowanie w ogłoszonej w BIP uchwale organu gminnego, nie wpływa na czytelność dokonanego w ten sposób przekazu. W tym przypadku treść aktu administracyjnego nie traci waloru informacyjnego, albowiem wynika z niej, kto, kiedy i w jakiej sprawie publicznej zajął określone stanowisko[9].

Podobne stanowisko zostało zaprezentowane w judykaturze w odniesieniu do danych osobowych upublicznionych w treści wyroku Trybunału Konstytucyjnego[10]. Sądy administracyjne uznały, że Prezes Trybunału Konstytucyjnego może publikować orzeczenia Trybunału Konstytucyjnego w Biuletynie Informacji Publicznej dopiero po poddaniu ich anonimizacji, tj. po usunięciu z ich treści informacji identyfikujących osobę fizyczną.

Nie bez znaczenia pozostaje także stanowisko Europejskiego Trybunału Sprawiedliwości w Luksemburgu z 1.7.2018 r. Przypomniano w nim, że zgodnie z art. 8 ust. 2 i 3 Karty Praw Podstawowych Unii Europejskiej, dane osobowe muszą być przetwarzane rzetelnie, w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, a przestrzeganie tych zasad podlega kontroli niezależnego organu. Sąd europejski przyjął, że w konfrontacji wartości prawa do informacji z prawem do ochrony danych osobowych pierwszeństwo ma ochrona prawa do prywatności osób fizycznych. W konsekwencji wprowadzono obligatoryjny, proceduralny wymóg anonimizacji orzeczeń w zakresie ujawniania w ich treści danych osobowych osób fizycznych. Uzasadniając swoje stanowisko, ETS podkreślił, że w ten sposób podąża za obserwowaną w państwach członkowskich tendencją wzmacniania ochrony danych osobowych w obliczu rosnącej liczby narzędzi wyszukiwania i rozpowszechniania informacji[11].

3) **zweryfikowanie jakości danych upublicznianych**

Administrator jest zobowiązany zapewnić, aby upubliczniane dane były prawidłowe i w razie potrzeby jest zobligowany do ich uaktualnienia. Obowiązek ten jest związany z realizacją zasady prawidłowości (art. 5 ust. 1 lit d RODO), która stanowi, że w przypadku, gdy występują nieprawidłowości w danych, powinny być one niezwłocznie sprostowane bądź usunięte. Zasada ta ma charakter gwarancyjny dla osób, których dane są upubliczniane. Osoba, której dane są nieprawidłowe czy też niekompletne, zgodnie z art. 16 RODO, ma określone prawa, o których mowa w sekcji 3 RODO (art. 16–20 RODO), ma np. prawo żądać ich sprostowania, uzupełnienia, usunięcia czy też ograniczenia przetwarzania, a administrator w określonym czasie powinien do tego żądania się odnieść i albo je niezwłocznie uwzględnić, albo podać przyczyny nieuwzględnienia. W tym zakresie RODO wprowadza całą odrębną procedurę (art. 12 i 15 RODO), która powinna być, od 25.5.2018 r. w pełni wdrożona. Zgodnie z art. 15 ust. 2 RODO, jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek je usunąć, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmie rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Obowiązek ten nie będzie miał zastosowania do organów władzy publicznej, w zakresie, w jakim przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 15 ust. 3 lit b).

Ważne

Odpowiedzialność po stronie organów publicznych i podmiotów realizujących zadania publiczne, w ramach władzy publicznej im powierzonej, za jakość danych poddanych procesowi upublicznienia jest bardzo duża, gdyż zazwyczaj za złą jakością danych podążają określone społeczne czy też zawodowe konsekwencje dla osób, których dane są w ten sposób udostępniane.

Przekazanie w oświadczeniu majątkowym dokładnych danych o adresie zamieszkania składającego oświadczenie może prowadzić do naruszenia nawet interesów żywotnych tej osoby.

4) **zweryfikowanie okresu przechowywania danych w sieci – zasada ograniczenia przechowywania**

Upublicznienie danych osobowych jest procesem, który ze swej istoty nie kończy się na realizacji czynności przekazania danych, np. do sieci publicznej. Wręcz przeciwnie, realizacja tego procesu tak naprawdę rozpoczyna się z chwilą utrwalenia tych danych w przestrzeni publicznie dostępnej. W dalszej kolejności następu-

[9] Wyr. WSA z 18.11.2008 r. (II SA/Wa 1177/08), wyr. NSA z 14.3.2013 r. (I OSK 620/12, Legalis).
[10] Wyr. WSA z 19.1.2017 r. (II SA/Wa 1434/16, Legalis).
[11] https://curia.europa.eu/jcms/pl 1168588/fr/.

je przechowywanie w niej danych i umożliwianie dostępu do tych danych innym podmiotom, co powoduje wiele zagrożeń. Administrator w tym momencie traci bowiem kontrolę nad tym, co z danymi osobowymi dalej się dzieje, tzn. kto dalej te dane będzie pozyskiwał i w jakich celach następnie wykorzystywał. Coraz powszechniejsze zjawisko profilowania[12] niesie określone konsekwencje dla osób, których dane dotyczą i nie zawsze ze skutkiem pozytywnym dla ochrony ich praw i wolności.

Ponadto UE już dawno dostrzegła potencjał gospodarczy w zjawisku wykorzystywania informacji wytwarzanych w sektorze publicznym, czego wyrazem jest dyrektywa Parlamentu Europejskiego i Rady 2013/37/UE z 26.6.2013 r., zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.Urz. UE L 175/1). Uznano, że polityka otwartego dostępu do danych propagująca szeroką dostępność i ponowne wykorzystywanie informacji sektora publicznego do celów prywatnych lub komercyjnych, przy minimalnych ograniczeniach prawnych, technicznych lub finansowych bądź bez takich ograniczeń, i wspierająca obieg informacji przeznaczonych nie tylko dla podmiotów gospodarczych, lecz także dla opinii publicznej, może odegrać ważną rolę w stymulowaniu rozwoju nowych usług opartych na nowatorskich sposobach łączenia i korzystania z takich informacji, pobudzić wzrost gospodarczy i wesprzeć zaangażowanie społeczne.

Dopuszczenie ponownego wykorzystywania dokumentów będących w posiadaniu organów sektora publicznego, jak wynika z treści tego aktu, stanowi wartość dodaną dla ponownych użytkowników, dla użytkowników końcowych, dla ogółu społeczeństwa, a w wielu przypadkach dla samego organu sektora publicznego, wspierając przejrzystość i odpowiedzialność oraz zapewniając informację zwrotną od ponownych użytkowników i użytkowników końcowych, która pozwala zainteresowanemu organowi sektora publicznego na poprawę jakości gromadzonych informacji. W Polsce pełna implementacja wskazanej dyrektywy odbyła się w przepisach ustawy z 25.2.2016 r. o ponownym wykorzystaniu informacji sektora publicznego (t.j. Dz.U. z 2018 r. poz. 1243 ze zm.). Informacja niezastrzeżona do ponownego wykorzystania staje się informacją, do której prawo ma każdy z ograniczeniami wynikającymi ze wskazanych przepisów (m.in. z uwagi na prawo do prywatności).

Ważne

Administratorzy z sektora publicznego już nie tylko ze względu RODO, ale także na obowiązujące regulacje dostępu do informacji publicznej i ponownego wykorzystania informacji sektora publicznego muszą ważyć wszystkie prawa podmiotów danych tymi regulacjami gwarantowane. Nie jest to zadanie łatwe wobec wysokiej uznaniowości płynącej z interpretacji tych przepisów oraz także wobec niejednolitości rozstrzygnięć sądów administracyjnych. Jednym z trudniejszych elementów dla dokonywania oceny realizacji zasady minimalizacji danych jest ukształtowanie okresu, przez który dane będą upubliczniane.

Zgodnie z art. 5 ust. 1 lit. e) RODO, dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia, w celu ochrony praw i wolności osób, których dane dotyczą.

Na administratorze danych spoczywa zatem szczególna odpowiedzialność nie tylko za kształtowanie zakresu informacji podlegających ujawnieniu, ale i określenie ram czasowych przetwarzania danych. Znajomość okresu przetwarzania danych ma fundamentalne znaczenie zarówno na etapie prowadzenia rejestru czynności przetwarzania, jak i przy realizacji obowiązku informacyjnego. Zgodnie z art. 30 ust. 1 lit. f) RODO, w rejestrze czynności administrator umieszcza planowane terminy usunięcia poszczególnych kategorii danych. Natomiast w momencie pozyskania danych od osoby, której dane dotyczą, jak również w inny sposób niż od osoby, której dane dotyczą, administrator podaje jej także – dla zapewnienia rzetelności i przejrzystości przetwarzania – okres, przez który dane osobowe jej dotyczące będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu (art. 13 ust. 2 lit. a) i art. 14 ust. 2 lit. a) RODO).

Określaniu takich ram często nie sprzyja brak ustalenia tych okresów w powszechnie obowiązujących przepisach, np. brak w DostInfPubU terminu bądź też kryteriów dla kształtowania okresu przechowywania danych w BIP. Ustawodawca jedynie ograniczył się do ukształtowania reguł dla udostępniania informacji publicznej, której elementem mogą być dane oso-

[12] Zgodnie z art. 4 pkt 4 RODO, profilowaniem jest dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

bowe, ale nie wskazał żadnych zasad przechowywania danych tam zawartych. W rezultacie od chwili wejścia w życie przepisów o dostępie do informacji publicznej (czyli od 1.1.2001 r.) w BIP stale przybywa danych osobowych i są one z założenia przechowywane tam wieczyście. Takie podejście nie jest zgodne z zasadami RODO, które w tym przypadku będzie miało bezpośrednie zastosowanie. Weryfikacja zawartości danych umieszczanych w BIP, także pod kątem ustalania okresu ich przechowywania, należy do administratora, który będzie musiał również wykazać adekwatność wprowadzonych w tym celu rozwiązań technicznych i organizacyjnych, zgodnie z zasadą rozliczalności.

Ocena poziomu ochrony danych osobowych

Wobec zmieniających się warunków technicznych i organizacyjnych w jednostkach, podyktowanych chociażby fluktuacją kadr, wobec licznych zmian w obowiązujących przepisach prawa oraz w dobie prawdziwej rewolucji informatycznej, rośnie ryzyko niewłaściwej ochrony danych osobowych. Popyt na dane osobowe stale rośnie i coraz bardziej dynamicznie rozwijają się technologie zarządzania informacją, w szczególności jej rozpowszechniania. Administratorzy danych muszą być tego świadomi. Administratorzy z sektora publicznego, dla których Konstytucja RP wyznacza dopuszczalne ramy realizacji ich obowiązków, są poddawani szczególnej ocenie społecznej. Składa się na nią także ocena poziomu ochrony danych osobowych. W pierwszej kolejności taka ocena powinna być jednak dokonywana przez samego administratora, który w ramach swoich wewnętrznych polityk ochrony danych osobowych, powinien ocenić przyjęte rozwiązania pod kątem ich zgodności z RODO. Ten unijny akt prawa jest prawdziwą szansą dla podnoszenia kompetencji osób przetwarzających dane osobowe na różnych odcinkach, także udostępniających dane osobowe w sieci.

Podstawa prawna

- art. 4 pkt 2, art. 5 ust. 1 lit. c), lit. e), ust. 2, art. 6, art. 7, art. 9 ust. 2, art. 11, art. 13 ust. 2 pkt c), art. 14 ust. 2 pkt d), art. 30 ust. 1 lit. f) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 96/45/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L Nr 119, s. 1)
- art. 5 ust. 2 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.)
- art. 157 ust. 2 pkt 2, art. 158 ust. 1, 3 i 4 ustawy z 14.12.2016 r. – Prawo oświatowe (t.j. Dz.U. z 2018 r. poz. 996 ze zm.)

Podsumowanie

RODO przewiduje wiele mechanizmów mających wspierać administratorów przy realizacji ich obowiązków oraz służących zapewnieniu praw podmiotom danych. Koordynacja przetwarzania danych w Internecie, z punktu widzenia ujawniającego te dane administratora, leży w jego interesie, a właściwe wdrożenie zasady rozliczalności pozwoli mu na zminimalizowanie ryzyk związanych z przetwarzaniem danych nadmiarowych, nieusuwaniem danych zbędnych czy też ujawnieniem danych osobom nieuprawnionym. W tym celu administrator powinien zastosować odpowiednie środki techniczne i organizacyjne, gdyż to często wskutek błędu ludzkiego, a nie wadliwości funkcjonowania systemów informatycznych, dochodzi do naruszenia przepisów o ochronie danych osobowych. Kontrola jakości i retencji danych osobowych przetwarzanych na stronach internetowych i w BIP jest mniejszym wyzwaniem dla administratorów, których w procesach tych wspomaga inspektor ochrony danych. Będąc właściwie umocowany w jednostce, autonomiczny i mając pełen dostęp do informacji niezbędnych dla realizacji swojej funkcji, jest w stanie aktywnie podnosić poziom wiedzy przetwarzających dane osobowe i odpowiedzialnych za ich ochronę na swoich stanowiskach. Zmniejszając poziom niepewności, co do stosowania przepisów o ochronie danych osobowych i gwarantując osobom, których dane są przetwarzane, pełną zgodność z RODO, administrator wchodzi na wyższy szczebel rozwoju swojej organizacji.

Inspektor puka do drzwi – jak przygotować się do kontroli Prezesa UODO

Anna Kobylańska
Adwokat, Wspólnik w Kancelarii Kobylańska & Lewoszewski

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1; dalej: RODO) wiąże się z obowiązkami, które spełnić muszą przedsiębiorcy przetwarzający dane osobowe, ale także z możliwością skontrolowania spełniania tych obowiązków przez Prezesa Urzędu Ochrony Danych Osobowych (dalej: PUODO). W artykule przedstawiono podstawowe wskazówki, jak przygotować się do takiej kontroli.

Przeszkolenie pracowników

Przygotowanie do kontroli warto zacząć od przeszkolenia pracowników w zakresie tego, jak przebiega kontrola, kto może kontrolować i kto może być kontrolowany, jaki jest zakres uprawnień PUODO. Pracownicy powinni poznać podstawowe informacje na temat prawidłowego zachowania w trakcie kontroli, działań, które mogą być uznane za utrudnianie przeprowadzenia kontroli (co stanowi przestępstwo w świetle przepisu art. 108 ustawy z 10.5.2018 r. o ochronie danych osobowych; t.j. Dz.U. z 2018 r. poz. 1000 ze zm.; dalej: OchrDanychU) oraz swoich praw.

Zebranie dokumentów

Kolejnym krokiem przygotowującym administratora do kontroli jest przygotowanie dokumentów, które mogą podlegać badaniu przez kontrolujących. Przy założeniu, że kontrolowany będzie administrator danych osobowych, dokumentami, które warto przygotować (lub choćby sprawdzić ich dostępność dla inspektorów) są:

1) statut podmiotu lub inny akt regulujący działanie administratora;
2) pełnomocnictwa (jeśli osoby reprezentujące administratora działają na podstawie pełnomocnictw, w tym pełnomocnictwa udzielone adwokatom lub radcom prawnym); warto pamiętać o opłacie skarbowej od udzielonego pełnomocnictwa (w wysokości 17 zł), ponieważ organ nadzorczy może sprawdzić także uiszczenie takiej opłaty;
3) pisemne wskazanie osoby upoważnionej do reprezentowania kontrolowanego, jeśli kontrolowany chciałby być reprezentowany przez taką osobę;

4) rejestr czynności przetwarzania danych;
5) umowy powierzenia przetwarzania danych oraz dokumentacja związana z wyborem i sprawdzeniem dostawców usług;
6) polityki, procedury i instrukcje dotyczące ochrony danych osobowych;
7) wzory upoważnień i poleceń przetwarzania danych;
8) stosowane klauzule informacyjne i klauzule zgody na przetwarzanie danych osobowych;
9) rejestry związane z dokumentowaniem prawidłowego wykonywania obowiązków wynikających z przepisów RODO, w tym rejestr naruszeń ochrony danych, rejestr żądań osób, których dane dotyczą, rejestr umów o powierzeniu przetwarzania danych, rejestr udzielonych zgód na przetwarzanie danych osobowych, rejestr usuniętych danych osobowych itp.;
10) dokumentacja związana z przeprowadzeniem analizy istnienia uzasadnionego interesu (art. 6 ust. 1 lit. f) RODO) oceny skutków przetwarzania dla ochrony danych, projektowaniem ochrony danych i stosowaniem domyślnej ochrony danych;
11) dokumentacja związana z wyznaczeniem inspektora ochrony danych (w tym dokument dotyczący wyznaczenia inspektora i wyznaczenia jego zadań);
12) ewentualna dokumentacja korespondencji prowadzonej z osobami, których dane dotyczą, na skutek zgłoszenia przez te osoby żądań związanych z ich uprawnieniami wynikającymi z przepisów RODO (żądanie dostępu do danych, ich sprostowania, ograniczenia ich przetwarzania, przeniesienia, usunięcia lub zgłoszenie sprzeciwu wobec przetwarzania danych).

Przygotowując dokumenty do kontroli warto pomyśleć o przygotowaniu tłumaczenia na język polski dokumentów sporządzonych w innych językach. Dokumenty takie tworzone są najczęściej w przypadku zawierania umów z zagranicznym dostawcą usług *on-line*.

Zebranie informacji i dokonanie niezbędnych ustaleń

Przygotowanie do kontroli wymaga także przyjrzenia się całemu programowi ochrony danych osobowych u danego administratora. Przepisy RODO nie zawierają dokładnej listy dokumentów, które powinny powstać na skutek wdrożenia wymagań RODO, ale nakładają na administratorów wiele obowiązków związanych z ochroną danych. Przed kontrolą PUODO warto zastanowić się, które obowiązki spełnione przez administratora nie zostały odzwierciedlone w dokumentacji lub zostały wykazane w innej, nie związanej wprost z ochroną danych osobowych, dokumentacji (np. faza projektowania ochrony danych osobowych może być odzwierciedlona tylko w dokumentacji projektowania funkcjonalności oprogramowania, którą administrator przygotował na potrzeby zamówienia nowego systemu informatycznego).

W ramach zbierania takich informacji warto sprawdzić gotowość wykazania wykonania następujących zadań:

1) identyfikacja danych osobowych, ustalenie celów ich przetwarzania oraz przygotowanie rejestru czynności przetwarzania danych (dla podmiotów przetwarzających: rejestru kategorii czynności przetwarzania danych);
2) zapewnienie, aby przetwarzane dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja zakresu przetwarzanych danych osobowych);
3) wyznaczenie terminów przechowywania danych i wprowadzenie zasad usuwania danych po upływie terminu retencji; sprawdzenie, czy zostały usunięte dane osobowe, których termin retencji już upłynął;
4) ustalenie podstawy prawnej przetwarzania danych osobowych, w tym danych szczególnych kategorii; sprawdzenie ważności zgód na przetwarzanie danych osobowych pozyskanych przed rozpoczęciem stosowania RODO; sprawdzenie poprawności stosowanych klauzul zgody oraz właściwego odnotowywania ich uzyskania;
5) wykonanie obowiązku informacyjnego wobec osób, których dane osobowe dotyczą; przygotowanie dokumentów potwierdzających wykonanie tego obowiązku;
6) wykonywanie uprawnień osób, których dane dotyczą (w tym prawa dostępu do danych, żądania ich usunięcia, ograniczenia ich przetwarzania, sprostowania, przenoszenia, wyrażenia sprzeciwu wobec przetwarzania danych); przygotowanie dokumentów potwierdzających wykonywanie tego obowiązku;
7) ustalenie listy podmiotów, którym należy powierzyć przetwarzanie danych; prawidłowe powierzenie przetwarzania danych; udokumentowanie sprawdzenia dostawców usług pod kątem spełnienia przez nich wymagań RODO;
8) zapewnienie podstawy prawnej transferu danych osobowych do państw trzecich (poza Europejski Obszar Gospodarczy);
9) przeprowadzenie oceny skutków przetwarzania dla ochrony danych (lub udokumentowania braku potrzeby przeprowadzenia takich analiz);
10) przeprowadzenie analiz związanych z projektowaniem ochrony

danych i stosowaniem domyślnej ochrony danych;
11) przygotowanie do reagowania na naruszenia ochrony danych, w tym przygotowanie rejestru naruszeń ochrony danych;
12) wyznaczenie i zgłoszenie inspektora ochrony danych;
13) zabezpieczenie danych osobowych (wdrożenie odpowiednich środków technicznych i organizacyjnych ochrony danych);
14) przeprowadzenie szkoleń z zakresu ochrony danych osobowych wśród pracowników przedsiębiorcy.

Ważne

Część informacji może być w posiadaniu podmiotów, którym administrator powierzył przetwarzanie danych osobowych (np. informacje o miejscu przechowywania danych, sposobie ich usuwania czy stosowanych środkach ochrony danych). W celu uniknięcia poszukiwania takich informacji w trakcie kontroli, warto zebrać wszystkie takie informacje w jednym miejscu lub zapewnić ich dostępność na czas kontroli.

Kolejnym elementem do rozważenia jest ustalenie, kto będzie reprezentował kontrolowanego przed PUODO. Czy będzie to jedna osoba, czy więcej? Czy będzie to inspektor ochrony danych, czy może ustanowiony pełnomocnik? Ustalenie to warto poczynić przed wszczęciem kontroli, aby uniknąć w jej trakcie chaosu informacyjnego i decyzyjnego.

Przygotowanie do kontroli wymaga także ustalenia listy osób mających wiedzę o poszczególnych elementach sytemu ochrony danych osobowych u danego administratora, a także miejsca dostępności poszczególnych dokumentów lub informacji.

Działania w trakcie kontroli

W ramach przygotowania do kontroli warto przemyśleć jej możliwy przebieg i ustalić pewne rozwiązania przed jej rozpoczęciem, a także ustalić, kto i w jakim trybie będzie podejmował decyzje w trakcie trwania kontroli.

Działania w trakcie kontroli powinny uwzględniać:
1) sprawdzenie tożsamości kontrolujących i ich upoważnienia do przeprowadzenia kontroli (legitymacji i imiennego upoważnienia); w związku z pojawiającymi się informacjami o fałszywych kontrolujących (osobach podających się za reprezentantów organu nadzorczego), warto na początku kontroli wykonać telefon do biura PUODO w celu potwierdzenia tożsamości kontrolujących;
2) przygotowanie miejsca do pracy osób kontrolujących;
3) ustanowienie jednej (lub więcej) osoby koordynującej po stronie kontrolowanego administratora;
4) ustalenie terminów obecności osób mających wiedzę o poszczególnych elementach sytemu ochrony danych osobowych u danego administratora;
5) zapewnienie dostępności uprzednio przygotowanych dokumentów i informacji;
6) zapewnienie kontrolującym dostępu do miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
7) zapoznanie się z protokołem pokontrolnym, wniesienie do niego ewentualnych zastrzeżeń oraz jego podpisanie.

Pierwsze kontrole przestrzegania przepisów RODO będą wyzwaniem zarówno dla kontrolowanych, jak i dla kontrolujących. Przepisy RODO są bowiem nietypowe w porównaniu z przepisami prawa polskiego, do których przyzwyczajeni są polscy administratorzy.

Z przepisów RODO wynika wiele obowiązków, które należy spełnić, ale brak jest dokładnych wskazówek, jak należy je spełnić i udokumentować ich wykonanie. Pierwsze kontrole PUODO pokażą, czy udowodnienie spełnienia tych wymagań okaże się wyzwaniem i jak do mniejszych lub większych błędów przedsiębiorców będzie podchodzić organ nadzorujący. Ze względu jednak na szeroki zakres obowiązków, warto wcześniej podjąć przygotowania do ewentualnej kontroli. Działania te mogą okazać się przydatne do samokontroli administratora, co do stanu wdrożenia wymagań RODO.

Podstawa prawna

- art. 108 ustawy z 10.5.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.)
- art. 6 ust. 1 lit. f) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1)

Rola Prezesa Urzędu Ochrony Danych Osobowych w świetle ustawy o ochronie danych osobowych

Dorota Krajewska-Kekusz
Dyrektor Zespołu Organizacyjnego w UODO, poprzednio dyrektor Departamentu Rejestracji ABI i Zbiorów Danych Osobowych w Biurze GIODO

Obowiązująca od 25.5.2018 r. ustawa z 10.5.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.; dalej: OchrDanychU) ustanowiła organem właściwym w sprawie ochrony danych osobowych Prezesa Urzędu Ochrony Danych Osobowych (dalej: PUODO). Do niedawna organem do spraw ochrony danych osobowych był Generalny Inspektor Ochrony Danych Osobowych, ustanowiony przez nieobowiązującą już ustawę z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.).

Prawne podstawy działania

Zmiana nazwy organu nie ma charakteru wyłącznie kosmetycznego. Prezesowi Urzędu Ochrony Danych Osobowych wyznaczono szerszy obszar działania niż Generalnemu Inspektorowi oraz nowe obowiązki, ale również nadano większe uprawnienia. Podkreślić też należy, że rola organu właściwego w sprawie ochrony danych osobowych – określonego w unijnej nomenklaturze jako organ nadzorczy – opisana została w trzech unijnych regulacjach przywołanych przez OchrDanychU.

Jak wskazuje przepis art. 34 ust. 2 OchrDanychU, PUODO jest organem nadzorczym w rozumieniu:

1) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1; dalej: RODO);
2) dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.U. UE L 119 z 4.5.2016 r., s. 89–131);
3) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z 11.5.2016 r. w sprawie Agencji

Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującego i uchylającego decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016 r., s. 53–114).

W pierwszym z wymienionych aktów – RODO – znajdują się zapisy stanowiące, że zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, jest utworzenie w państwach członkowskich organów nadzorczych, uprawnionych do wypełniania zadań i wykonywania uprawnień w sposób całkowicie niezależny oraz że organy te powinny monitorować stosowanie przepisów RODO i przyczyniać się do jego spójnego stosowania w całej Unii Europejskiej (motyw 117 i 123 Preambuły do RODO).

Podstawowe zadania PUODO

Zadania organu nadzorczego opisane zostały bezpośrednio w Rozdziale VI RODO, które jest aktem prawnym stosowanym bezpośrednio, co oznacza, że jego normy stały się automatycznie częścią polskiego porządku prawnego, bez konieczności ich dodatkowej implementacji. Niemniej jednak OchrDanychU, jako akt prawny służący stosowaniu RODO, zawiera w swej treści przepisy określające rolę PUODO – jako organu nadzorczego – na gruncie prawa krajowego. Jeżeli chodzi o zadania PUODO, to obejmują one następujące czynności:

1) przeprowadzanie kontroli przestrzegania przepisów o ochronie danych osobowych. Podkreślić przy tym należy, że kwestia wszczęcia kontroli nie jest pozostawiona do swobodnego uznania PUODO. Kontrolę wszczyna się zgodnie z planem kontroli lub na podstawie uzyskanych informacji lub w ramach monitorowania przestrzegania RODO (procedurę prowadzenia kontroli opisuje Rozdział 9 ustawy);
2) prowadzenie postępowań w sprawie naruszenia przepisów o ochronie danych osobowych (zgodnie z przepisami zawartymi w Rozdziale 7 OchrDanychU).
3) zatwierdzanie, po uprzednio przeprowadzonych konsultacjach, kodeksów postępowania mających pomóc we właściwym stosowaniu RODO (o czym mówi art. 40). PUODO udziela również akredytacji podmiotom mającym monitorować stosowanie kodeksów;
4) udzielanie zezwoleń na przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej (art. 56 pkt 1 OchrDanychU).
5) współpraca w sprawach ochrony danych osobowych z organami nadzorczymi kościołów i związków lub wspólnot wyznaniowych, o ile organy takie zostaną utworzone zgodnie z warunkami określonymi w RODO (art. 59 OchrDanychU);
6) utworzenie i prowadzenie systemu certyfikacji (przewidzianej w art. 42 RODO) obejmującego opublikowanie kryteriów certyfikacji, rozpatrywanie wniosków w tej sprawie oraz wydawanie i cofanie certyfikatów (czynności opisane w Rozdziale 4 OchrDanychU). Nadmienić należy, że certyfikacji, o której mowa w art. 42 RODO, dokonywać może nie tylko PUODO, ale również tzw. podmiot certyfikujący po uzyskaniu akredytacji Polskiego Centrum Akredytacji. PUODO spełnia przy tym istotną rolę, udostępniając na swojej stronie przedmiotowej – w Biuletynie Informacji Publicznej – kryteria akredytacji. Ponadto prowadzi publicznie dostępny wykaz podmiotów, którym udzielono certyfikacji (art. 23 ust. 2 OchrDanychU) oraz podmiotów akredytowanych (art. 33 ust. 1 OchrDanychU). Nadmienić należy, że za czynności związane z certyfikacją PUODO pobiera opłatę, której wysokość odpowiada przewidywanym kosztom poniesionym z tytułu wykonywania tych czynności.

Niezależnie od przedstawionych wcześniej zadań, OchrDanychU zobowiązuje PUODO do działań mających wskazać administratorom oraz podmiotom przetwarzającym, takie sposoby postępowania w toku przetwarzania danych, które zapewnią maksymalną ochronę danych i ujednolicą praktykę w tym zakresie.

W związku z tym PUODO:

1) ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (art. 54 ust. 1 pkt 1 OchrDanychU), przy czym do wydania pierwszego komunikatu w tej sprawie – w terminie 3 miesięcy od dnia wejścia w życie ustawy – PUODO został specjalnie zobligowany w innym przepisie (art. 172 OchrDanychU)[1];
2) przystępuje – na wniosek administratora danych lub podmiotu przetwarzającego – do uprzednich konsultacji, których celem jest wypracowanie rozwiązań minimalizujących ryzyko naruszenia praw lub wolności osób fizycznych w toku przetwarzania danych osobowych (art. 57 OchrDanychU);
3) udostępnia na swojej stronie przedmiotowej w Biuletynie Informacji Publicznej rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych (art. 53 ust. 1 pkt 4 OchrDanychU);

[1] PUODO wykonał ten obowiązek, wydając 17.8.2018 r. stosowny komunikat, który opublikowany został w M.P. 2018 r. poz. 827.

4) udostępnia na swojej stronie przedmiotowej w Biuletynie Informacji Publicznej standardowe klauzule umowne, o których mówi art. 28 ust. 8 RODO, przyjęte dla umów dotyczących przetwarzania danych osobowych zawieranych pomiędzy administratorami a podmiotami przetwarzającymi dane (art. 53 ust. 1 pkt 1 OchrDanychU) oraz wspomniane wcześniej kodeksy postępowania (art. 53 ust. 1 pkt 1 OchrDanychU);
5) zatwierdza wiążące reguły korporacyjne, o których mowa w art. 47 RODO.

Dodatkowo, PUODO może również ogłosić w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych, które nie wymagają oceny skutków przetwarzania dla ich ochrony (art. 54 ust. 1 pkt 2 PUODO) oraz prowadzić system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszeń ochrony danych osobowych (art. 55 OchrDanychU).

Innym obowiązkiem, który nie ma – być może – bezpośredniego wpływu na przestrzeganie przepisów o ochronie danych osobowych, lecz jest mocno zaakcentowany w obecnej ustawie, jest złożenie rocznego sprawozdania z działalności. Zgodnie z art. 50 OchrDanychU, PUODO raz w roku – do dnia 31 sierpnia – przedstawia Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności, zawierające w szczególności informacje o liczbie i rodzaju prawomocnych orzeczeń sądowych uwzględniających skargi na decyzje lub postanowienia PUODO oraz wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych. Sprawozdanie to powinno zostać również udostępnione na stronie podmiotowej PUODO w Biuletynie Informacji Publicznej.

Jako organ właściwy w sprawie ochrony danych osobowych, PUODO posiada także uprawnienia do:
1) kierowania wystąpień zmierzających do zapewnienia skutecznej ochrony danych osobowych (adresatami są tu organy państwowe i samorządu terytorialnego, państwowe i komunalne jednostki organizacyjne, podmioty niepubliczne realizujące zadania publiczne, osoby fizyczne i prawne, jednostki organizacyjne niebędące osobami prawnymi oraz inne podmioty);
2) występowania do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

Podmioty, do których zostały skierowane wystąpienia lub wnioski, są obowiązane ustosunkować się do nich w terminie 30 dni od daty ich otrzymania.

W ustawie zawarto również wymóg, żeby założenia i projekty aktów prawnych dotyczące danych osobowych były przedstawiane Prezesowi Urzędu do zaopiniowania.

Uprawnienia do wystąpień (jak wspomniane powyżej) oraz do opiniowania aktów prawnych dotyczących danych osobowych przysługiwały również Generalnemu Inspektorowi pod rządami ustawy z 29.8.1997 r. o ochronie danych osobowych.

Prezes UODO udziela także porad administratorowi zgodnie z procedurą uprzednich konsultacji, o których mowa w art. 36 RODO.

Wymierzanie kar finansowych

Wyznaczając PUODO liczne zadania i obowiązki, ustawodawca wyposażył go jednocześnie w uprawnienia mające służyć skuteczniejszemu egzekwowaniu przepisów o ochronie danych osobowych. Za najistotniejsze z nich uznać można uprawnienie do nałożenia – w drodze decyzji administracyjnej – na podmiot obowiązany do przestrzegania przepisów RODO administracyjnej kary pieniężnej.

Nadmienić należy, że OchrDanychU dokonuje rozróżnienia pomiędzy grupami podmiotów, na które kara może zostać nałożona. Artykuł 102 OchrDanychU wskazuje Narodowy Bank Polski, instytuty badawcze oraz jednostki sektora finansów publicznych, o których mowa w art. 9 ustawy z 27.8.2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r. poz. 2077 ze zm.) – m.in. organy władzy publicznej, jednostki samorządu terytorialnego, ZUS, KRUS, instytucje gospodarki publicznej, NFZ jako te, na które PUODO nałożyć może karę pieniężną do wysokości 100 tys. zł (wyjątkowo potraktowano państwowe i samorządowe instytucje kultury – tu kara może wynosić do 10 tys. zł).

Surowsze sankcje spotkać mogą natomiast podmioty inne niż wymienione. W ich przypadku OchrDanychU (art. 101) odwołuje się bezpośrednio do art. 83 RODO. Ten przepis również różnicuje maksymalne wysokości kar pieniężnych.

Naruszenie przepisów dotyczących obowiązków administratora, podmiotu przetwarzającego, podmiotu certyfikującego i podmiotu monitorującego zagrożone jest karą do 10 mln euro, natomiast w przypadku przedsiębiorstwa – do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa). Z kolei za naruszenie przepisów dotyczących m.in. podstawowych zasad przetwarzania, praw osób, których dane dotyczą, przekazywanie danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej grozi kara do 20 mln euro, zaś w przypadku przedsiębior-

stwa – do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa).

Ważne

Nakładanie kar finansowych oraz określanie ich wysokości wymaga od PUODO szczególnej rozwagi. Artykuł 38 RODO domaga się, aby administracyjne kary pieniężne nakładać zależnie od okoliczności każdego indywidualnego przypadku. RODO wskazuje przy tym kilkanaście czynników, jakie muszą zostać wzięte przy tym pod uwagę (np. umyślność naruszenia, kategorie danych, których dotyczy naruszenie, sposób, w jaki organ nadzorczy dowiedział się o naruszeniu).

O złożoności problemu świadczyć może fakt, że Grupa Robocza Art. 29[2] przyjęła – 3.10.2017 r. – „Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679". Jednocześnie PUODO uzyskał prawo do udzielania ulg w wykonaniu kary administracyjnej, co może mieć postać odroczenia terminu uiszczenia kary lub rozłożenia jej na raty (co jednak wiąże się z naliczaniem odsetek za zwłokę).

Prezes Urzędu Ochrony Danych Osobowych ma również do dyspozycji środki naprawcze, opisane w art. 58 ust. 2 RODO, w postaci m.in. zakazów i nakazów określonego działania wydawanych administratorom i podmiotom przetwarzającym dane. Kary finansowe nakładane są natomiast oprócz lub zamiast środków naprawczych.

Nałożenie administracyjnej kary finansowej nie jest jedynym instrumentem finansowego oddziaływania, w jaki został wyposażony PUODO. W toku postępowania w sprawie naruszenia przepisów o ochronie danych osobowych ma on również prawo wymierzenia grzywny w wysokości od 500 do 5 tys. zł w przypadkach, o których mowa w art. 88 ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257 ze zm.; dalej: KPA) (nieuzasadnione niestawienie się przed organem w charakterze świadka lub biegłego lub nieuzasadniona odmowa złożenia zeznań, wydania opinii okazania przedmiotu oględzin lub udziału w innej czynności procesowej). Warto zwrócić uwagę na modyfikację przepisu art. 88 KPA. Wskazanie w OchrDanychU minimalnej wysokości grzywny na kwotę 500 zł oraz maksymalnej na kwotę 5000 zł, uzasadnione jest wagą spraw związanych z naruszeniem przepisów o ochronie danych osobowych, co wymaga zapewnienia sprawności i skuteczności postępowania.

Omówienie uprawnień PUODO do wymierzania kar finansowych i grzywien nadanych mu przez OchrDanychU uzupełnić należy o kwestię egzekucji w rozumieniu ustawy z 17.6.1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz.U. z 2018 r. poz. 1314 ze zm.; dalej: EgzAdmU).

Artykuł 12 § 2 pkt 12 EgzAdmU przewiduje, że egzekucji administracyjnej podlegają obowiązki z zakresu ochrony danych osobowych nakładane w drodze decyzji PUODO. Z kolei art. 20 § 2 EgzAdmU wymienia m.in. PUODO jako organ egzekucyjny w zakresie egzekwowania obowiązków o charakterze niepieniężnym (w przypadkach określonych szczególnymi przepisami). Oznacza to, że PUODO ma prawo stosować środki egzekucyjne, wśród których, gdy chodzi obowiązki o charakterze niepieniężnym, na pierwszym miejscu wskazana jest grzywna w celu przymuszenia (poza tym art. 1a pkt 12 lit. b) wymienia inne środki: wykonanie zastępcze, odebranie rzeczy ruchomej, odebranie nieruchomości, opróżnienie lokali i innych pomieszczeń, przymus bezpośredni).

Analogiczne uprawnienia posiadał Generalny Inspektor Ochrony Danych Osobowych, którego jednym z zadań było zapewnienie wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym, wynikających z wydanych decyzji administracyjnych w sprawach wykonania przepisów o ochronie danych osobowych. Jak wynika ze „Sprawozdania z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2017", na koniec roku pozostało niewykonanych 25 (spośród wydanych 85) decyzji administracyjnych, które objęte są działaniami egzekucyjnymi w 2018 r.

Środki wspierające postępowania prowadzone przez PUODO

Prezes Urzędu Ochrony Danych Osobowych wyposażony został także w uprawnienia do zastosowania środka tymczasowego polegającego na zobowiązaniu podmiotu, któremu zarzucane jest naruszanie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych. Uczynić to może jeszcze w toku postępowania w sprawie naruszenia przepisów, wtedy gdy uprawdopodobnione zostanie, że przetwarzanie danych narusza przepisy, a dalsze ich przetwarzanie może wywołać poważne i trudne do usunięcia skutki (art. 70 OchrDanychU).

Ważne

Innym instrumentem, jaki PUODO ma do dyspozycji w toku postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, jest wystąpienie do Trybunału Sprawiedliwości Unii

[2] Pełna nazwa: Grupa Robocza do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana na mocy Dyrektywy 95/46 WE Parlamentu i Rady Europy z 24.10.1995 r.

Europejskiej z pytaniem prawnym w sprawie ważności niektórych decyzji Komisji Europejskiej. Chodzi tu o decyzje dotyczące kodeksów postępowania (kwestie te wchodzą w obszar kompetencji KE, gdy kodeksy dotyczą przetwarzania danych w kilku państwach UE) oraz niektórych aspektów przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. Obowiązek skierowania pytania prawnego pojawia się, gdy w toku postępowania w sprawie naruszenia przepisów PUODO uzna, że istnieją uzasadnione wątpliwości, co do zgodności decyzji KE z prawem unijnym. Pytanie do TSUE kierować należy za pośrednictwem sądu administracyjnego, zgodnie z procedurą opisaną w art. 71 OchrDanychU.

Z kolei w toku kontroli przestrzegania przepisów PUODO (lub upoważniona przez niego osoba zwana kontrolującym) może zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeśli jest to niezbędne do wykonania czynności kontrolnych. Pomoc ta polega na zapewnieniu kontrolującemu bezpieczeństwa osobistego, dostępu do miejsca kontroli oraz porządku w tym miejscu, a także na zapewnieniu bezpieczeństwa innym osobom uczestniczącym w czynnościach kontrolnych, mając w szczególności na względzie poszanowanie godności osób biorących udział w kontroli (art. 85 OchrDanychU).

Niezależność PUODO

RODO (art. 52) bardzo mocno akcentuje kwestię niezależności organu nadzorczego podczas wypełniania przez niego zadań i wykonywania uprawnień, domagając się zagwarantowania mu wolności od bezpośrednich i pośrednich wpływów zewnętrznych. W związku z tym OchrDanychU zawiera przepis stanowiący wprost, że PUODO w zakresie wykonywania swoich zadań podlega tylko ustawie (art. 34 ust. 5 OchrDanychU). Jednak przepis ten nie wyczerpuje gwarancji niezależności PUODO, z których najważniejsze przedstawiane są poniżej:

1) kadencyjność, przy czym kadencja przerwana może zostać jedynie śmiercią, utratą obywatelstwa polskiego lub odwołaniem ze stanowiska. Podkreślić należy, że to ostatnie nastąpić może wyłącznie przy zaistnieniu ustawowych przesłanek (zrzeczenie się stanowiska, trwała niezdolność do pełnienia obowiązków stwierdzona orzeczeniem lekarskim, sprzeniewierzenie się ślubowaniu, skazanie prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego, pozbawienie praw publicznych). Trwanie kadencji określone zostało na 4 lata z zastrzeżeniem, że ta sama osoba nie może być PUODO więcej niż przez dwie kadencje;
2) zakaz przynależności do partii politycznej, związku zawodowego oraz wykonywania zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami PUODO. Wyjątek uczyniono jedynie dla stanowisk naukowych, dydaktycznych i naukowo-dydaktycznych w placówkach naukowych i badawczych. Dodać należy, że ograniczenie to dotyczy nie tylko PUODO, ale również jego zastępców;
3) immunitet polegający na tym, że PUODO nie może być – bez uprzedniej zgody Sejmu Rzeczypospolitej Polskiej – pociągnięty do odpowiedzialności karnej ani pozbawiony wolności;
4) powoływanie i odwoływanie dokonywane przez Sejm za zgodą Senatu, co uniezależnia PUODO od formalnej podległości organom administracji rządowej[3].

Istotnymi atrybutami niezależności PUODO są również, przyznane mu przez ustawę, uprawnienia do:

1) nadania – w drodze zarządzenia – statutu Urzędowi Ochrony Danych Osobowych (pod rządami poprzedniej ustawy statut nadawał Prezydent RP w drodze rozporządzenia);
2) samodzielnego mianowania swoich zastępców, których może być do 3 (poprzednia ustawa dopuszczała tylko jednego, którego powoływał i odwoływał Marszałek Sejmu na wniosek Generalnego Inspektora).

Rada do Spraw Ochrony Danych Osobowych

Rolę jaką pełni PUODO jako organ właściwy do spraw ochrony danych określać może również fakt, że ustawodawca przewidział utworzenie i działanie – przy PUODO – organu opiniodawczo-doradczego w postaci Rady do Spraw Ochrony Danych Osobowych. Prawo do zgłaszania kandydatów do Rady uzyskały: Rada Ministrów, Rzecznik Praw Obywatelskich, izby gospodarcze, jednostki naukowe oraz fundacje i stowarzyszenia wpisane do Krajowego Rejestru Sądowego, których celem statutowym jest działalność na rzecz ochrony danych osobowych (art. 48 OchrDanychU). Zadaniem Rady jest m.in. opracowywanie propozycji kryteriów certyfikacji, inicjowanie działań w obszarze danych osobowych oraz przedstawianie propozycji zmian prawa w tym obszarze, ale także wyrażanie opinii w sprawach przedstawionych jej przez PUODO (w tym projektów aktów prawnych i innych dokumentów).

[3] Odstępstwo od przyjętego trybu powołania PUODO zostało zawarte w art. 166. ust. 2 OchrDanychU, który stanowi, że osoba powołana na stanowisko Generalnego Inspektora Ochrony Danych Osobowych na podstawie uchylonej ustawy z 29.8.1997 r. o ochronie danych osobowych, pozostaje na stanowisku do czasu upływu kadencji, na którą została powołana.

Obszary poza właściwością PUODO

RODO zawiera też przepisy o ograniczeniu zakresu jego stosowania. Najbardziej uniwersalny jest – jak się zdaje – przepis art. 2 ust. 1 lit. d), który stanowi, że RODO nie ma zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Z kolei art. 23 ust. 1 RODO zezwala państwom członkowskim Unii Europejskiej na wydanie prawa, które może ograniczać prawa osoby, której dane są przetwarzane lub złagodzić obowiązek administratora danych do niezwłocznego informowania o naruszeniu, jeżeli okazałoby się środkiem niezbędnym służącym m.in.: bezpieczeństwu narodowemu, obronie, bezpieczeństwu publicznemu, ochronie niezależności sądów i postępowania sądowego, innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu. Ponadto art. 55 RODO stanowi, że organ nadzorczy nie jest właściwy do nadzorowania operacji przetwarzania dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości.

Zatem i OchrDanychU zawiera przepis o ograniczeniu zakresu jej stosowania. Artykuł 6 stanowi, że ustawy oraz RODO nie stosuje się do:

1) przetwarzania danych osobowych przez wskazane jednostki sektora finansów publicznych spośród wymienionych w art. 9 ustawy z 29.8.2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r. poz. 2077 ze zm.), w zakresie, w jakim to przetwarzanie jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego, jeżeli przepisy szczególne przewidują niezbędne środki ochrony praw i wolności osoby, której dane dotyczą (wskazane jednostki sektora finansowego to: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały, jednostki budżetowe, agencje wykonawcze, instytucje gospodarki budżetowej, inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego);
2) działalności służb specjalnych w rozumieniu art. 11 ustawy z 24.5.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (czyli Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego) (t.j. Dz.U. z 2017 r. poz. 1920 ze zm.).

Podstawa prawna

- art. 6, art. 23 ust. 1, ust. 2, art. 33 ust. 1, art. 34 ust. 2, art. 50, art. 53, art. 54 ust. 1, art. 55, art. 56 pkt 1, art. 57, art. 59, art. 70, art. 71, art. 85, art. 101, art. 102, art. 172 ustawy z 10.5.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.)
- art. 36, art. 38, art. 42, art. 58 ust. 2, art. 83, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1)
- art. 9 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.)
- art. 12 § 2 pkt 12, 20 § 2 ustawy z 17.6.1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz.U. z 2018 r. poz. 1314 ze zm.)

Podsumowanie

Ustawa o ochronie danych osobowych, uwzględniając przepisy RODO, określiła na nowo rolę organu właściwego w sprawie ochrony danych osobowych. Zachowane zostały obowiązki organu w zakresie kontroli przestrzegania przepisów o ochronie danych osobowych i prowadzenia postępowań w sprawach ich naruszenia. Zniesiono natomiast obowiązek prowadzenia ogólnokrajowych, jawnych rejestrów zbiorów danych osobowych i administratorów bezpieczeństwa informacji. Jednocześnie PUODO zyskał uprawnienia, jakich nie miał jego poprzednik pod rządami ustawy z 29.8.1997 r. o ochronie danych osobowych (np. do nakładania kar finansowych i zwracania się o pomoc do Policji). Silniej zaakcentowana też została niezależność PUODO. Podkreślić jednak należy zadania wyznaczone PUODO w zakresie:

1) certyfikacji;
2) tworzenia kodeksów postępowania;
3) uprzednich konsultacji;
4) zatwierdzania reguł korporacyjnych czy udostępniania informacji istotnych dla bezpiecznego przetwarzania danych osobowych.

Sytuują one PUODO w roli nie tyle strażnika przepisów, co organu wspierającego ich prawidłowe stosowanie.

Wniosek o przeniesienie danych osobowych do innego administratora

Agnieszka Sagan-Jeżowska
Radca prawny, IOD w branży informacji gospodarczych, big data, direct marketingu oraz w branży medycznej, specjalista ds. RODO z jedenastoletnim doświadczeniem w dziedzinie ochrony danych osobowych oraz trener szkoleniowy

Od 25.5.2018 r. osoby, których dane są przetwarzane, mogą korzystać z nowych uprawnień przysługujących im na gruncie RODO. Zmianie uległ nie tylko katalog praw, jakie przysługują osobom fizycznym, ale także ogólne warunki ich realizacji, nakładając na administratorów danych większe obowiązki niż te obowiązujące przed wejściem w życie RODO.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1; dalej: RODO) wprowadza kilka nowych uprawnień, których realizacja może być wyzwaniem dla administratorów. W praktyce również sam zakres praw może budzić wątpliwości i wymagać pogłębionej analizy poszczególnych wniosków i żądań skierowanych do administratora przez osoby, których dane dotyczą.

Nowe uprawnienia na gruncie RODO

Nowym prawem osób, których dane dotyczą, jest **prawo do przenoszenia danych osobowych**. Prawo to polega na możliwości żądania przez osobę, której dane dotyczą, aby administrator przekazał dane osobowe tej osoby samemu wnioskodawcy lub bezpośrednio innemu, wskazanemu przez wnioskodawcę podmiotowi, który w ten sposób stanie się ich odrębnym administratorem. Uprawnienie to nie jest jednak bezwzględne, dotyczy bowiem tylko tych danych, które łącznie spełniają następujące wymogi:

1) są przetwarzane w sposób zautomatyzowany oraz
2) są przetwarzane przez administratora na podstawie zgody osoby, której dane dotyczą lub umowy zawartej z tą osobą, a także
3) zostały dostarczone do administratora przez osobę, której one dotyczą.

Podkreślić należy, że prawu do przenoszenia danych osobowych podlegają tylko te dane osobowe, które spełniają łącznie ww. kryteria. Pozostałe dane osobowe są wyłączone z obowiązku realizacji prawa do przenoszenia, nawet jeśli administrator przetwarza inne dane o wnioskodawcy, np. na innej podstawie prawnej, wyłącznie

w formie papierowej lub dane pozyskane z innych źródeł niż osoba, której te dane dotyczą.

Jednym z dobrze znanych praw osób, których dane dotyczą, jest **prawo dostępu do danych**, polegające na przyznaniu uprawnienia do uzyskania potwierdzenia, czy administrator przetwarza dane osobowe wnioskodawcy, Jeżeli tak jest, osoba ta ma prawo otrzymać od administratora następujące informacje:

1) cele przetwarzania;
2) kategorie danych osobowych;
3) informacje o odbiorcach lub kategoriach odbiorców danych, zarówno tych, którym dane zostały już ujawnione, jak i tych, którym administrator planuje je udostępniać;
4) planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu (tzw. okres retencji);
5) informacje o przysługujących osobie prawach:
   a) do sprostowania,
   b) usunięcia,
   c) ograniczenia przetwarzania,
   d) wniesienia sprzeciwu;
6) informacje o prawie wniesienia skargi do organu nadzoru;
7) w przypadku pozyskiwania danych z innych źródeł niż osoba, której dane dotyczą – informacje o źródłach przetwarzanych danych;
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO wraz z istotnymi informacjami o zasadach ich podejmowania, o ich znaczeniu oraz o przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Nowością wprowadzoną przez RODO jest przyznanie osobie, której dane dotyczą, **prawa dostępu do danych** oraz **do otrzymania kopii danych**. Prawa te nie są ograniczone zakresem żądanych danych, co oznacza, że wnioskujący może żądać dostępu do pełnego zakresu swoich danych, niezależnie od tego, czy są one przetwarzane w sposób zautomatyzowany, czy papierowo, na jakiej podstawie prawnej oraz niezależnie od źródła ich pozyskania przez administratora. Prawo dostępu do danych osobowych jest zatem najszerszym prawem o zakresie znacznie większym niż prawo do przenoszenia danych.

Ważne

Co do zasady, realizacja praw osób, których dane dotyczą, jest bezpłatna i nie można jej uzależniać od warunków dodatkowych, np. od wykazania interesu w pozyskaniu określonych informacji lub kopii danych.

Ograniczenia w realizacji praw

RODO przewiduje jednak wyjątek od ogólnej zasady obowiązkowej realizacji praw osób, mianowicie administrator może odmówić realizacji wniosku lub pobrać od wnioskodawcy opłatę za jego realizację, jeżeli złożone żądanie jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Opłata musi być w rozsądnej wysokości wynikającej z kosztów administracyjnych udzielenia informacji, podejmowanej komunikacji oraz podjęcia żądanych działań.

Dodatkowo, realizacja prawa do otrzymania kopii jest ograniczona:

1) ilościowo – mianowicie osobie, której dane dotyczą, przysługuje prawo do bezpłatnego żądania kopii określonych danych tylko raz. Za każdą kolejną żądaną kopię administrator może pobrać rozsądną opłatę wynikającą z kosztów administracyjnych (w tym przypadku nie można do opłaty doliczyć kosztów komunikacji);
2) zakresowo, bowiem prawo do otrzymania kopii danych nie może niekorzystnie wpływać na prawa i wolności innych, np. na ochronę danych osobowych innych osób, prawa własności intelektualnej administratora lub jego kontrahenta, tajemnicę przedsiębiorstwa. Nie oznacza to natomiast, że administrator może całkowicie odmówić realizacji prawa do otrzymania kopii danych. Jeżeli zachodzi konflikt z prawami i wolnościami innych, administrator powinien zaproponować inny sposób realizacji prawa, np. sporządzić kopię danych w inny sposób niż żądany przez osobę, której dane dotyczą lub zrealizować wniosek częściowo, a odmówić tylko w uzasadnionym zakresie.

Natomiast prawo do przenoszenia jest dodatkowo ograniczone warunkami określonymi w RODO i podlegają temu prawu wyłącznie dane, które:

1) są przetwarzane w sposób zautomatyzowany;
2) są przetwarzane na podstawie zgody lub umowy zawartej z osobą, której one dotyczą;
3) zostały dostarczone przez osobę, której one dotyczą, przy czym prawo do przenoszenia obejmuje dane przekazane przez osobę do administratora, jak i dane zaobserwowane przez administratora dotyczące działań tej osoby (np. informacje o wyświetlanych stronach lub kupowanych przedmiotach).

A zatem administrator może odmówić realizacji prawa do przenoszenia również w zakresie, w jakim wniosek przekracza ramy uprawnienia określone w art. 20 RODO.

Może jednak zdarzyć się, że administrator odmówi realizacji wniosku o przeniesienie do innego administratora ze względów bezpieczeństwa lub braku możliwości technicznych. Obowiązkiem administratora jest realiza-

cja prawa do przenoszenia w interoperacyjnym formacie, czyli w formacie umożliwiającym przeniesienie tych danych do innych narzędzi informatycznych stosowanych przez administratora odbierającego dane. RODO nie nakłada jednak obowiązku wprowadzenia przez administratora kompatybilnych technicznie systemów przetwarzania. Oznacza to, że w zależności od tego, w jakich systemach są przetwarzane dane, o których przeniesienie wnioskuje osoba oraz od sposobu, w jaki ma zostać dokonane przeniesienie, może ono być technicznie możliwe lub niemożliwe dla administratora, a każdy taki przypadek powinien być rozpatrywany indywidualnie. Również kwestie bezpieczeństwa mogą uniemożliwiać realizację wniosku. Administrator dokonujący przenoszenia nie odpowiada bowiem za legalność i bezpieczeństwo przetwarzania przeniesionych danych osobowych przez administratora odbierającego te dane, jednak odpowiada za bezpieczeństwo danych na etapie ich przekazywania, zanim trafią one do nowego administratora.

A zatem, jeśli administrator nie ma możliwości technicznych lub nie jest w stanie zapewnić odpowiedniego bezpieczeństwa przy realizacji wniosku zgodnie z życzeniem wnioskodawcy, powinien odmówić jego realizacji we wnioskowanej formie.[1]

Wówczas wniosek powinien zostać zrealizowany w inny sposób, np. wobec wnioskodawcy w miejsce wskazanego administratora lub w sposób alternatywny uzgodniony z wnioskodawcą. Administrator nie może również celowo tworzyć lub wyolbrzymiać przeszkód przy realizacji prawa osoby, której dane dotyczą, bowiem takie działania mogą zostać uznane za nieuprawnioną odmowę realizacji prawa do przenoszenia danych lub za naruszenie ogólnego obowiązku ułatwiania osobie realizacji jej praw, o którym mowa w art. 12 ust. 2 RODO.

Procedury realizacji praw

Podczas realizacji wniosków należy przestrzegać ogólnych zasad ustanowionych przez RODO, w szczególności:

1) komunikacji z osobami, których dane dotyczą; powinna ona odbywać się jasnym, prostym językiem, w zwięzłej i przejrzystej formie, tj. udzielone informacje powinny być zrozumiałe dla osoby, która nie jest specjalistą ds. RODO, prawnikiem, technikiem itd.;
2) administrator ma obowiązek ułatwiać osobie realizację jej praw, np. przy rozpatrywaniu wniosku powinien wziąć pod uwagę cel, jaki osoba chce osiągnąć, a nie literalną treść wniosku, który może zawierać sprzeczności, powoływanie się na niewłaściwe podstawy prawne;
3) administrator ma obowiązek udzielenia informacji i nie później niż w ciągu miesiąca:
   a) zrealizować wniosek osoby,
   b) poinformować o odmowie realizacji wniosku, podać przyczyny odmowy oraz poinformować, że osoba może złożyć skargę do organu nadzoru lub skierować sprawę do sądu,
   c) poinformować o wydłużeniu terminu maksymalnie o kolejne 2 miesiące oraz podać przyczynę tego opóźnienia (przyczyną może być wysoki stopień skomplikowania wniosku lub ilość żądań osoby, której dane dotyczą);
4) jeżeli wniosek wpłynął elektronicznie, należy odpisać również elektronicznie, chyba że w określonym przypadku nie jest to możliwe (np. osoba skorzystała z formularza kontaktowego i podała błędny adres e-mail do odpowiedzi i w efekcie administrator otrzymał informację, że jego e-mail wysłany do wnioskodawcy nie został dostarczony).

Ważne

Procedury realizacji praw osób powinny przewidywać zatem obowiązek udzielania pomocy i ustalania rzeczywistego celu, jaki osoba wnioskująca chce osiągnąć, jeżeli z treści wniosku nie da się tego określić w sposób jednoznaczny.

W praktyce najczęściej wpływające wnioski są skonstruowane na tak wysokim poziomie ogólności, że bez poczynienia dodatkowych ustaleń lub podjęcia decyzji o wariantowej realizacji prawa administrator nie byłby w stanie skutecznie realizować otrzymywanych wniosków i w efekcie odmawiałby, powołując się na ich ewidentną nadmierność.

PRZYKŁAD

„Żądam otrzymania wszystkich moich danych osobowych, które podmiot o mnie przetwarza". Literalna treść tego żądania oznaczałaby konieczność przygotowania kopii nie tylko danych osobowych rozumianych wąsko jako zakres danych o osobie, ale także nagrań wszystkich rozmów telefonicznych, kopii korespondencji mailowej, wszystkich spraw załatwianych z tą osobą, dokumentów z nią

[1] Szerzej w wytycznych Grupy Roboczej Art. 29 dotyczących prawa do przenoszenia danych przyjętych 13.12.2016 r. ostatnio zmienionych i przyjętych 5.4.2017 r. WP 242 rev. 01, s. 17, w szczególności:
„Artykuł 20 ust. 2 nakłada na administratorów danych obowiązek przekazywania danych osobowych podlegających przenoszeniu bezpośrednio do innych administratorów danych «o ile jest to technicznie możliwe». Techniczna możliwość przesłania danych przez administratora danych innemu administratorowi, pod kontrolą osoby, której dane dotyczą, powinna być oceniana dla poszczególnych przypadków. Motyw 68 dalej wyjaśnia granice tego, co jest «technicznie możliwe», wskazując że «nie powinno to nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania».
Oczekuje się, że administratorzy danych będą przesyłać dane osobowe w interoperacyjnym formacie, mimo że nie nakłada to na innych administratorów danych obowiązku wspierania tych formatów. Zatem bezpośrednie przesłanie danych przez jednego administratora do innego może mieć miejsce, gdy możliwa jest komunikacja między dwoma systemami, w zabezpieczony sposób, oraz gdy system otrzymujący ma techniczną możliwość otrzymania przychodzących danych. Jeżeli przeszkody techniczne uniemożliwiają bezpośrednie przekazanie, administrator danych powinien wyjaśnić osobom, których dane dotyczą, kwestię tych przeszkód, ponieważ w przeciwnym razie jego decyzja będzie miała podobny skutek jak odmówienie podjęcia działań na żądanie osoby, której dane dotyczą (art. 12 ust. 4)".

związanych i pism wysłanych w formie papierowej, np. skarg i zażaleń. A często celem tak złożonego wniosku jest tylko otrzymanie zakresu danych o tej osobie w ujęciu ogólnym, tj. jej danych potwierdzających tożsamość, danych kontaktowych, ogólnego wskazania na kategorie przetwarzanych o tej osobie danych.

Dopuszczalne jest **warstwowe spełnianie prawa do przenoszenia oraz prawa dostępu do danych i otrzymania ich kopii**, co sprowadza się do tego, że administrator procedurami wewnętrznymi określa sposób interpretacji tak ogólnie ujętych wniosków i podstawowy zakres realizacji takiego wniosku. Jeżeli administrator decyduje się na warstwowe spełnienie wniosku, powinien w odpowiedzi do wnioskodawcy zaznaczyć, że jeżeli takie załatwienie jego sprawy nie jest dla niego wystarczające, może on doprecyzować wniosek, wskazując, jakie konkretne dane chciałby pozyskać. Dobrą praktyką jest zaznaczenie, że w określonych przypadkach może zostać ustalona opłata za realizację wniosku w szerszym zakresie i że wówczas osoba otrzyma informację z wyliczeniem należnej kwoty i prośbą o jej uprzednie uiszczenie.

Dobrą praktyką jest opracowanie odpowiednich formularzy, które ułatwią wnioskodawcy skuteczne złożenie wniosku, a administratorowi zapewnią dokładniejsze określenie oczekiwań osoby, której dane dotyczą. Należy jednak mieć na względzie, że formularze powinny mieć charakter pomocniczy i administrator nie powinien odrzucać wniosków tylko dlatego, że nie zostały złożone na formularzu. Jeżeli wniosek zawiera określenie wnioskodawcy, zakres żądania oraz ewentualne inne informacje pozwalające na realizację wniosku, wniosek ten powinien zostać uznany za złożony skutecznie, niezależnie od tego, w jakiej formie lub jaką drogą komunikacji został złożony.

Wniosek o przeniesienie danych osobowych do innego administratora

Opracowanie wzoru wniosku o przeniesienie danych osobowych do innego administratora jest dobrym rozwiązaniem nie tylko ze względu na ewentualne ułatwienia dla wnioskodawcy i administratora, ale też ze względu na podwyższone ryzyko naruszenia praw i wolności osób, których dane dotyczą, w przypadku realizacji wniosku w zakresie szerszym niż wnioskowany. Realizacja prawa do przeniesienia do innego administratora w zakresie szerszym niż wnioskowane przez osobę, której dane dotyczą, może spowodować nie tylko niezadowolenie wnioskodawcy i niezgodność z RODO, ale także może również spowodować szkodę wywołaną otrzymaniem przez nowego administratora informacji o osobie, których ta osoba ujawniać nie chciała.

Wzór Nr 1

Wniosek o realizację prawa do przeniesienia danych osobowych przysługującego na gruncie art. 20 RODO [1]	
1. Dane wnioskodawcy **[2]**	Imię i nazwisko **[3]**:
	Numer PESEL **[4]**:
	Adres korespondencyjny **[5]**:
	Numer telefonu do kontaktu **[6]**:
2. Zakres danych osobowych podlegających przeniesieniu na żądanie wnioskodawcy (*należy opisać, które dane osobowe lub ich kategorie są objęte żądaniem*) **[7]** Prawu do przeniesienia danych osobowych podlegają wyłącznie dane osobowe, które spełniają łącznie poniższe warunki: 1) są przetwarzane w podmiocie w sposób zautomatyzowany/elektronicznie;	…… …… …… …… …… …… …… **[8]**

2) są przetwarzane na podstawie zgody wnioskodawcy lub umowy zawartej z wnioskodawcą; 3) zostały dostarczone do podmiotu przez wnioskodawcę	
3. Określenie, komu przeniesione dane mają zostać doręczone **[9]**	☐ Wnioskodawcy **[10]**
	☐ innemu administratorowi (*należy podać pełną nazwę administratora oraz adres siedziby*) **[11]**: …… ……
4. Sposób dostarczenia przeniesionych danych osobowych **[12]**	☐ e-mail **[13]** 1) adres e-mail, na który zostanie wysłany plik: …… 2) numer telefonu komórkowego, na który zostanie wysłane hasło do pliku: ……
	☐ płyta CD/pendrive **[14]** adres do korespondencji, na który zostanie wysłany nośnik danych: …… ……
	☐ inny sposób – jaki **[15]**: …… ……
Data i miejsce: ……	Podpis wnioskodawcy: ……**[16]**
Realizacja wniosku jest bezpłatna, jednak w przypadku, gdy złożone żądanie okaże się ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może odmówić jego realizacji lub pobrać opłatę wynikającą z kosztów administracyjnych realizacji wniosku oraz prowadzenia komunikacji. W takim przypadku wnioskodawca zostanie poinformowany o wysokości opłaty oraz o możliwych sposobach jej uiszczenia, a po dokonaniu zapłaty wniosek zostanie niezwłocznie zrealizowany **[17]**.	
Administratorem danych osobowych zawartych w niniejszym wniosku jest …… . Dane będą przetwarzane na podstawie prawnie uzasadnionego interesu administratora wyłącznie w celu realizacji niniejszego wniosku oraz w celu obrony przed ewentualnymi roszczeniami i możliwości wykazania rozliczalności przez okres …..[2] lat od zrealizowania żądania **[18]**. Wszelkie informacje dotyczące przetwarzania danych osobowych, które wnioskodawca otrzymał od administratora w związku z przetwarzaniem jego danych osobowych, pozostają aktualne również wobec przetwarzania danych osobowych zawartych w niniejszym wniosku. Prawo dostępu do danych osobowych, ograniczenia przetwarzania, usunięcia danych po upływie okresu retencji, złożenia sprzeciwu[3] przysługuje w szczególności osobie, której dane dotyczą.	

[2] Okresy retencji powinny zostać ustalone indywidualnie przez każdego administratora, zgodnie z jego potrzebami. Autorka proponuje okres przedawnienia pięcioletni, tj. ustalony zgodnie z ustawą z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257 ze zm.) określającego 5-letni okres możliwości ukarania administratora z tytułu niezgodności z przepisami prawa. Inny okres retencji to okres 6-letni, czyli okres obecnie obowiązującego terminu przedawnienia roszczeń cywilnoprawnych (od 9.7.2018 r.) lub inny ustalony przez administratora. Należy jednak mieć na względzie, aby na potrzeby realizacji zasady rozliczalności, zasady ograniczenia celu oraz ograniczenia przetwarzania móc zawsze wykazać podstawy, na których administrator opierał swoje ustalenia.

[3] Zawarcie skróconej klauzuli informacyjnej zakłada, że administrator spełnił już pełen obowiązek informacyjny na wcześniejszym etapie pozyskiwania innych danych osobowych. Jeżeli jednak administrator nie spełnił pełnego obowiązku informacyjnego lub z ostrożności, na wszelki wypadek, woli zamieścić pełną klauzulę informacyjną, należy ją odpowiednio uzupełnić.

Adnotacja o realizacji wniosku [19]

Wniosek został zrealizowany w dniu …… przez ……. .

Wniosek nie został zrealizowany z następujących przyczyn: ……

……..

Wzór Nr 2

W dniu ……. **[20]** otrzymaliśmy Pani/Pana wniosek o informacje dotyczące przetwarzania Pani/Pana danych osobowych przez administratora.

Uprzejmie informujemy, że Pani/Pana wniosek został zrealizowany. Poniżej przesyłamy żądane przez Panią/Pana informacje dotyczące przetwarzania Pani/Pana danych osobowych:

Lp.	Zakres udzielanej informacji	Odpowiedź
1.	Potwierdzenia, czy administrator przetwarza dane osobowe wnioskodawcy	**[21]**
2.	Możliwość realizacji prawa dostępu do danych	**[22]**
3.	Cele przetwarzania	**[23]**
4.	Kategorie odnośnych danych osobowych	**[24]**
5.	Informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych	**[25]**
6.	Planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu	**[26]**
7.	Informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania	**[27]**
8.	Informacje o prawie wniesienia skargi do organu nadzorczego	**[28]**
9.	Jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle	**[29]**
10.	Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą	**[30]**

Gdyby okazało się, że sposób spełnienia wniosku nie odpowiada w pełni Pani/Pana oczekiwaniom, prosimy o poinformowanie nas oraz o sprecyzowanie Pani/Pana żądania, wówczas postaramy się je spełnić.

Jeżeli możemy Pani/Panu pomóc w realizacji Pani/Pana praw przysługujących zgodnie z RODO, zapraszamy do kontaktu z nami. Osobą kontaktową w Pani/Pana sprawie jest ……. **[31]**.

Wzór Nr 3

W dniu …… **[32]** otrzymaliśmy Pani/Pana wniosek dotyczący przeniesienia przetwarzania Pani/Pana danych osobowych.

Przeanalizowaliśmy Pani/Pana wniosek i uprzejmie informujemy, że niestety nie możemy przychylić się do Pani/Pana wniosku.

Zgodnie z art. 20 RODO osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

1) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz

2) przetwarzanie odbywa się w sposób zautomatyzowany.

Pani/Pana wniosek nie mieści się w ramach przewidzianych przez RODO, ponieważ …… **[33]**. Wobec tego nie może on zostać zrealizowany.

Jednocześnie uprzejmie informujemy, że w każdej chwili może Pan/Pani ponownie złożyć wniosek w zakresie przewidzianym w RODO i wówczas taki wniosek zostanie przez nas zrealizowany.

Informujemy również, że przysługuje Pani/Panu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 w Warszawie, kancelaria@uodo.gov.pl.

Jeżeli możemy Pani/Panu pomóc w realizacji Pani/Pana praw przysługujących zgodnie z RODO, zapraszamy do kontaktu z nami. Osobą kontaktową w Pani/Pana sprawie jest …… **[34]**.

Objaśnienia do wzorów Nr 1–3

[1] tytuł formularza;

[2] określenie informacji do uzupełnienia w polach (3)–(4) – dane wnioskodawcy;

[3] miejsce na wpisanie imienia i nazwiska wnioskodawcy;

[4] miejsce na wpisanie numeru PESEL wnioskodawcy;

[5] miejsce na wpisanie adresu korespondencyjnego – na wypadek, gdyby administrator miał potrzebę komunikacji z wnioskodawcą, np. wysłać mu informację o przedłużeniu terminu na realizację wniosku, o odmowie realizacji wniosku, o nałożeniu opłaty oraz w przypadku żądania doręczenia przeniesionych danych do wnioskodawcy;

[6] miejsce na wpisanie numeru telefonu – na wypadek, gdyby administrator potrzebował podjąć szybki kontakt z wnioskodawcą, np. w celu doprecyzowania zakresu danych podlegających przeniesieniu;

[7] zakres danych osobowych podlegających wnioskowi. W celu uniknięcia nieporozumień pole to zawiera również krótkie pouczenie o zakresie danych podlegających prawu do przeniesienia;

[8] miejsce na wpisanie zakresu danych osobowych, które zgodnie z żądaniem wnioskodawcy mają podlegać przeniesieniu. W tym polu wnioskodawca powinien dokładnie wskazać dane osobowe, które chce poddać przeniesieniu;

[9] określenie informacji do wyboru i uzupełnienia w polach (10)–(11) – wskazanie, komu przeniesione dane mają zostać dostarczone;

[10] pole wyboru dostarczenia przeniesionych danych wnioskującemu – to pole wnioskujący powinien zaznaczyć, jeżeli chce, aby przeniesione dane zostały mu doręczone;

[11] pole wyboru dostarczenia przeniesionych danych do innego administratora – to pole wnioskujący powinien zaznaczyć, jeżeli chce, aby przeniesione dane zostały doręczone innemu administratorowi oraz wskazać pełną nazwę i adres siedziby tego administratora;

[12] określenie informacji do wyboru i uzupełnienia w polach (14)–(16) – wskazanie sposobu dostarczenia przeniesionych danych osobowych;

[13] pole wyboru doręczenia przeniesionych danych za pośrednictwem wiadomości e-mail oraz miejsce na wpisanie adresu e-mail, na który ma zostać dokonane doręczenie oraz numeru telefonu, na który zostanie wysłane hasło do wysłanych plików. Rozwiązanie to zakłada, że admini-

strator będzie stosował zabezpieczenie w postaci odpowiednio złożonego hasła podczas przesyłania plików zawierających dane osobowe z użyciem publicznej sieci Internet. Jeżeli administrator zdecyduje się na inną formę zabezpieczenia danych lub zdecyduje, że nie zgadza się na przesyłanie określonych danych osobowych drogą elektroniczną, powinien odpowiednio dostosować to pole;

[14] pole wyboru doręczenia przeniesionych danych na nośniku danych (pendrive, płyta CD) oraz miejsce na wpisanie adresu do korespondencji, na który ma zostać doręczony nośnik. Jeżeli administrator będzie stosował zabezpieczenie danych w postaci hasła nałożonego na plik zapisany na nośniku, w tym polu powinien dodać również numer telefonu, na który zostanie wysłane hasło do pliku;

[15] pole wyboru doręczenia przeniesionych danych w inny sposób niż proponowany przez administratora – w tym polu wnioskujący może zaproponować inny sposób dostarczenia przeniesionych danych do wybranej osoby lub podmiotu;

[16] pole do wpisania daty, miejsca złożenia wniosku oraz złożenia podpisu przez wnioskodawcę;

[17] pole zawierające pouczenie dla wnioskodawcy dotyczące możliwości odmowy realizacji wniosku lub nałożenia opłaty za jego realizację;

[18] pole zawierające skrócony obowiązek informacyjny określający cele przetwarzania danych osobowych zawartych we wniosku, podstawę prawną, okres retencji tych danych oraz odesłanie do wcześniej spełnionego, pełnego obowiązku informacyjnego;

[19] formularz zawiera miejsce na sporządzenie przez administratora adnotacji o realizacji wniosku lub o odmowie jego realizacji. Pole to jest w pełni dobrowolne, a jego zawartość może być dowolnie dostosowywana przez administratora.

Przykładowe odpowiedzi na wnioski o realizację praw osób, których dane dotyczą

Pomocne może okazać się nie tylko opracowanie wzorów o realizację praw osób, których dane dotyczą, ale także wzory odpowiedzi udzielanych na wpływające wnioski. Wzory odpowiedzi powinny przewidywać zarówno pozytywne ich rozpatrzenie, czyli informować o realizacji wniosku, jak i odmowę realizacji wniosku. Wprowadzenie wzorów w organizacji zapewni rzetelną realizację praw osób, których dane dotyczą oraz ułatwią pracę pracowników odpowiedzialnych za przygotowywanie odpowiedzi.

Odpowiedź pozytywna na wniosek o prawo dostępu do danych osobowych

Wzór Nr 2 stanowi odpowiedź pozytywną na wniosek o dostęp do danych osobowych[4].

[20] miejsce na uzupełnienie daty, w której wniosek o realizację prawa dostępu wpłynął do administratora;

[21] pole na potwierdzenie, że administrator przetwarza dane osobowe wnioskodawcy;

[22] pole na wskazanie możliwości realizacji prawa dostępu do danych osobowych. Jeżeli osoba wnioskowała wyłącznie o prawo dostępu do danych osobowych, można udzielić wyłącznie tej informacji i zrezygnować z udzielania pełnej informacji o przetwarzaniu danych osobowych wnioskodawcy. Jeżeli natomiast z wniosku wynika, że zamiarem wnioskodawcy nie jest otrzymanie dostępu do danych, a uzyskanie pełnej informacji o przetwarzaniu jej danych osobowych, wówczas można usunąć pola z wiersza **[3]**;

[23] pole na wskazanie wszystkich celów przetwarzania danych osobowych wnioskodawcy;

[24] pole na wskazanie kategorii odnośnych danych osobowych przetwarzanych o wnioskodawcy;

[25] pole na podanie informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

[26] pole na wskazanie wszystkich okresów retencji danych osobowych, tj. planowanych okresów przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu;

[27] pole na udzielenie informacji o przysługujących wnioskodawcy prawach: do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

[28] pole na podanie informacji o prawie wniesienia skargi do organu nadzorczego;

[29] pole na podanie informacji o źródłach danych osobowych, jeżeli zostały zebrane od osoby, której dane dotyczą;

[30] pole na podanie informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 oraz – przynajmniej w tych przypadkach – istotne in-

[4] Wzór został opracowany w oparciu o wzór pochodzący z publikacji autorki: Klauzule RODO. Wzory klauzul z praktycznym komentarzem, Wydawnictwo C.H.Beck 2018, s. 144–145.

formacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

[31] miejsce na podanie danych kontaktowych do osoby odpowiedzialnej za realizację wniosku.

Można podać również ogólny kontakt na infolinię. Podanie tej informacji nie jest obowiązkowe, lecz stanowi przejaw dobrej praktyki, może też uchronić administratora przed kolejnym wnioskiem lub skargą skierowaną do administratora lub bezpośrednio do organu nadzoru. Gdyby bowiem okazało się, że osoba nie jest do końca usatysfakcjonowana otrzymaną odpowiedzią lub nie do końca rozumie przekazane jej informacje, jeżeli podamy w piśmie bezpośredni kontakt, mamy większe prawdopodobieństwo, że osoba najpierw zadzwoni, a dopiero później rozważy napisanie skargi czy kolejnego wniosku.

Odpowiedź negatywna na wniosek o przeniesienie danych osobowych z powodu przekroczenia zakresu prawa określonego w RODO

Wzór Nr 3 stanowi odpowiedź negatywną na wniosek o przeniesienie danych[5].

[32] miejsce na uzupełnienie daty, w której wniosek o realizację prawa dostępu wpłynął do administratora;

[33] miejsce na dokładne opisanie przyczyn, dla których wniosek nie został zrealizowany, tj. na czym polega przekroczenie zakresu prawa określonego w RODO;

[34] miejsce na podanie danych kontaktowych do osoby odpowiedzialnej za realizację wniosku. Można podać również ogólny kontakt na infolinię. Podanie tej informacji nie jest obowiązkowe, lecz stanowi przejaw dobrej praktyki i jest zalecane szczególnie w przypadku odpowiedzi odmownych, może bowiem uchronić administratora przed skargą skierowaną bezpośrednio do organu nadzoru. Jeżeli podamy w piśmie bezpośredni kontakt, pod który osoba może zadzwonić i uzyskać dodatkowe wyjaśnienia dotyczące przyczyn odmowy realizacji jej wniosku, mamy większe prawdopodobieństwo, że osoba najpierw zadzwoni, a dopiero później rozważy napisanie skargi.

Podstawa prawna

- art. 12 ust. 2, art. 20, art. 22 ust. 1 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1)

[5] Wzór pochodzi z publikacji: *A. Sagan-Jeżowska*, Klauzule RODO. Wzory klauzul z praktycznym komentarzem, Wydawnictwo C.H.Beck 2018, s. 158.

C·H·BECK
Klauzule RODO
Agnieszka Sagan-Jeżowska
Gotowe do zastosowania zapisy klauzul wyrażających zgodę na przetwarzanie danych osobowych.
www.ksiegarnia.beck.pl | 22 311 22 22


Wniosek o usunięcie danych osobowych i realizację prawa „do bycia zapomnianym" – schemat postępowania

Piotr Kowalik
Radca prawny, specjalizujący się w problematyce ochrony danych osobowych, dostępu do informacji publicznej i obrotu informacjami prawnie chronionymi

Przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE. L Nr 119, s. 1; dalej: RODO) , w bardzo szerokim zakresie odnoszą się do praw i wolności osób, których dane dotyczą. Tworząc tę regulację prawodawca europejski planował wzmocnić ochronę praw takich osób. Prawa te zostały zatem ujęte w tym akcie szerzej i co do zasady, w sposób bardziej precyzyjny, niż miało to miejsce dotychczas. Jednym z takich praw, często omawianym w literaturze tematu, jest wynikające z art. 17 RODO prawo do usunięcia danych, które w pewnych sytuacjach może zostać rozszerzone także na prawo „do bycia zapomnianym".

Żądanie usunięcia danych

Warto zatem przeanalizować, jak powinien postępować administrator danych, do którego ktoś zwróci się o realizację jednego lub obu tych praw. Wprawdzie przepisy RODO wprost o tym nie stanowią, ale osoba, która będzie chciała zrealizować swoje prawo do usunięcia swoich danych, czy też prawo „do bycia zapomnianym" (o czym niżej), powinna zwrócić się do administratora danych z żądaniem w tym przedmiocie.

O ile samo RODO nie wymaga szczególnej formy czy treści takiego żądania, aby było możliwe jego rozpatrzenie, należałoby w nim co najmniej określić, jakich danych (czy wszystkich danych, czy też ich części i ewentualnie jakiej części) i na jakiej podstawie usunięcia żąda osoba, której dane dotyczą oraz krótko opisać okoliczności faktyczne sprawy. W sytuacji, gdyby administrator na podstawie złożonego żądania miał uzasadnione wątpliwości, co do tożsamości osoby fizycznej skła-

dającej ten wniosek, może zażądać od tej osoby dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości osoby (por. art. 12 ust. 6 RODO).

Ważne

Rozpoznanie żądania jest bezwzględnym obowiązkiem administratora. W razie jakichkolwiek wątpliwości co do treści wniosku, w tym zakresu żądania, administrator powinien komunikować się z osobą, której dane dotyczą, w celu ich wyeliminowania.

Dalsze czynności – terminy, opłaty

Wniosek o usunięcie danych powinien być przez administratora rozpoznany, co do zasady, niezwłocznie. Jeśli z jakichś względów byłoby to utrudnione, termin na rozpoznanie tego wniosku i usunięcie danych nie powinien być dłuższy niż jeden miesiąc (por. art. 12 ust. 3 RODO).

W razie potrzeby, jeśli sprawa jest skomplikowana i trudno ocenić zasadność żądania usunięcia danych, termin jednego miesiąca administrator może przedłużyć o kolejne dwa miesiące. Jednak wówczas w terminie miesiąca od otrzymania żądania, administrator musi poinformować osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje te także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy (por. art. 12 ust. 3 RODO).

Postępowanie i wszystkie czynności administratora danych zmierzające do zrealizowania wniosku są wolne od jakichkolwiek opłat, należy jednak pamiętać, że jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

1) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo
2) odmówić podjęcia działań w związku z żądaniem.

Ważne

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze (por. art. 12 ust. 5 RODO). Wydaje się, że przepis ten może sprawiać trudności w stosowaniu administratorom danych z sektora publicznego. Przy naliczaniu należności muszą się oni poruszać w regulacjach prawa krajowego i ocenić, w jakim trybie i w jaki sposób egzekwowana byłaby taka opłata.

Usunięcie danych

W świetle art. 17 ust. 1 RODO, administrator danych będzie związany wnioskiem o usunięcie danych i musi usunąć przetwarzane przez siebie dane osobowe, w następujących sytuacjach:

1) gdy dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane (o możliwości przetwarzaniach danych w innym celu niż w ten, dla jakiego dane zostały zebrane stanowi art. 6 ust. 4 RODO);
2) gdy osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
3) gdy osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO (jest to sprzeciw wobec przetwarzania danych w celach marketingu bezpośredniego) lub art. 21 ust. 1 RODO (jest to sprzeciw z przyczyn związanych z szczególną sytuacją osoby, której dane dotyczą). Administrator jest związany takim sprzeciwem, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą;
4) gdy dane osobowe były przetwarzane niezgodnie z prawem;
5) gdy dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator (istnieje przepis prawa, który wprost nakazuje usuniecie danych);
6) gdy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 (wniosek o usunięcie danych dotyczy danych dziecka poniżej 16. roku życia, nawet wówczas, gdy osoba, która podała swoje dane jako dziecko, już takim dzieckiem nie jest – por. motyw 65 preambuły RODO).

Jak widać prawodawca europejski pokusił się o enumeratywne wskazanie wszystkich sytuacji, w których administrator ma obowiązek usunąć dane osobowe. To niewątpliwie dobre rozwiązanie, które uporządkuje praktykę stosowania przepisów o ochronie danych osobowych.

Odmowa usunięcia danych

Jeśli administrator uzna, że nie ma podstaw prawnych do usunięcia danych, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach swojego rozstrzygnięcia oraz o możliwości wniesienia skargi do organu nadzor-

czego (Prezesa Urzędu Ochrony Danych Osobowych) oraz skorzystania ze środków ochrony prawnej przed sądem (art. 12 ust. 4 RODO).

Wydaje się, że zgodnie z art. 17 ust. 3 RODO, odmowa usunięcia danych powinna być zastosowana przez administratora również wówczas, gdy dalsze przetwarzanie danych, jest niezbędne:

1) do korzystania z prawa do wolności wypowiedzi i informacji;
2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego, zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO;
4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do usunięcia danych, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
5) do ustalenia, dochodzenia lub obrony roszczeń.

Co ważne, odmowa usunięcia danych, nie ma waloru rozstrzygnięcia administracyjnego i nie stosuje się do niej przepisów ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257 ze zm.), nawet wówczas, gdy odmawiającym usunięcia danych administratorem jest podmiot publiczny. Odmowę taką należy traktować jako czynność materialno-techniczną, która jest możliwa do wzruszenia jedynie na drodze skargi do PUODO, o której mowa w art. 77 RODO.

Prawo do „bycia zapomnianym"

Ze szczególną sytuacją będziemy mieli do czynienia wówczas, gdy administrator danych upublicznił dane, które na mocy art. 17 ust. 1 RODO ma obowiązek usunąć. W takiej sytuacji ciąży na nim dodatkowy obowiązek. Biorąc pod uwagę dostępną technologię i koszt realizacji musi podjąć rozsądne działania, w tym środki techniczne, aby poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje (art. 17 ust. 2 RODO).

W związku z treścią wskazanego przepisu we wniosku o usuniecie danych, osoba, której dane dotyczą, powinna wyraźnie określić, że niezależnie od żądania usunięcia danych, chce skorzystać również ze swojego prawa do „bycia zapomnianym". W innym przypadku administrator może swoje działania ograniczyć jedynie do usunięcia danych ze swoich zasobów.

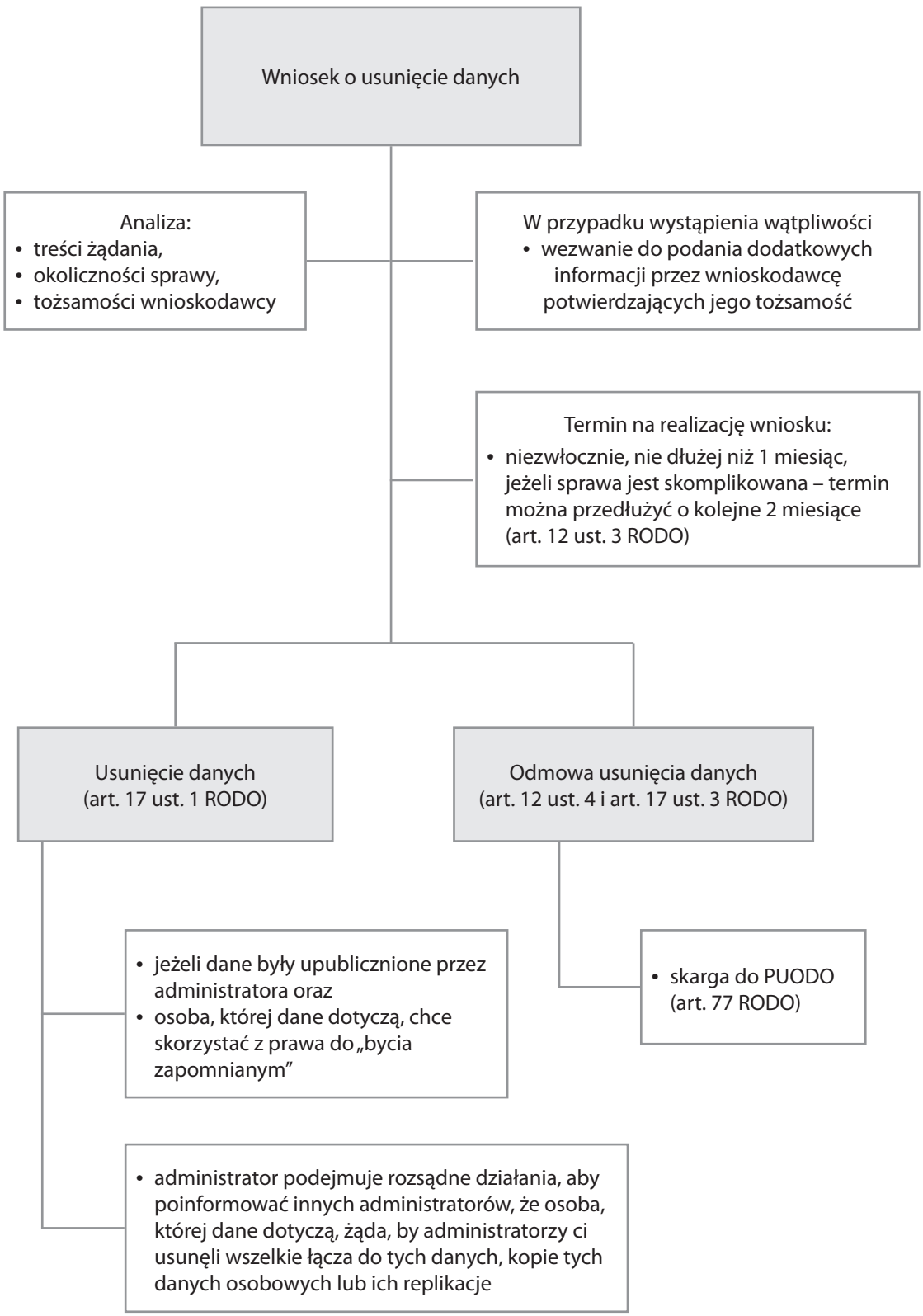
▶ Podstawa prawna

- art. 12 i art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz.UE L Nr 119, s. 1)

ZYSKAJ DOSTĘP
DO WERSJI ONLINE
SWOJEGO CZASOPISMA
informacja
W ADMINISTRACJI PUBLICZNEJ

1 Wejdź na stronę www.czasopisma.beck.pl
2 Zarejestruj bezpłatne konto, podając te same dane co przy zamówieniu prenumeraty
3 W momencie opłacenia faktury za czasopismo, do Twojego konta online dodamy dostęp do wersji elektronicznej czasopisma
4 Dostęp będzie trwał tak długo, jak okres prenumeraty

Schemat wniosku o usunięcie danych osobowych i realizację prawa „do bycia zapomnianym"



RODO jako czynnik porządkujący granice jawności informacji o osobach pełniących funkcje publiczne

dr Piotr Sitniewski
Krajowa Szkoła Administracji Publicznej
im. Prezydenta Rzeczypospolitej Polskiej
Lecha Kaczyńskiego, Prezes Fundacji JAWNOSC.PL,
założyciel i prowadzący portale www.jawnosc.pl
oraz www.jawnoscsamorzadu.pl

Same przepisy RODO nie definiują pojęcia osoby pełniącej funkcję publiczną, gdyż nie taka jest rola tych przepisów. Niemniej jednak w zakresie uregulowania określonych nowych praw, jakie przysługują osobie, której dane są przetwarzane, ale i również określenia obowiązków, jakie ciążą na administratorze danych, RODO może mieć potencjalnie porządkujący wpływ na praktyczny wymiar określenia wzmiankowanej w tytule kwestii.

Założeniem niniejszego artykułu jest rozważenie, w jakim zakresie mające zastosowanie od 25.5.2018 r. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1; dalej: RODO) może mieć porządkujący wpływ na ustalenie granic jawności informacji odnoszących się do osób pełniących funkcje publiczne w rozumieniu prawa do informacji, a w szczególności art. 5 ust. 2 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.; dalej: DostInfPubU).

Założenia brzegowe analizy

Podstawą dla przetwarzania danych osobowych w ramach realizacji prawa do informacji jest art. 6 ust. 1 lit. c) RODO, według którego przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Obowiązkiem tym jest realizacja powinności, jakie nakłada na podmioty obowiązane DostInfPubU. Takie podejście do prawnej podstawy przetwarzania danych osobowych w kontekście realizacji prawa do informacji jest zgodne z motywem 45 RODO, z którego wynika, że jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, podstawę przetwarzania powin-

no stanowić prawo państwa członkowskiego, gdyż RODO nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może fakt, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego. Za takie uregulowanie prawne należy traktować konstytucyjne prawo do informacji określone w art. 61 ustawy z 2.4.1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. Nr 78, poz. 483 ze zm.; dalej: Konst) oraz jego uszczegółowienie w treści DostInfPubU. Teoretycznie istnieje możliwość, aby podstawą dla przetwarzania danych osobowych była zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a) RODO[1]), lecz taka sytuacja miałaby miejsce wyłącznie wtedy, gdy wniosek o udostępnienie informacji publicznej dotyczyłby osób, które nie pełnią funkcji publicznej albo osób pełniących funkcje publiczne w zakresie informacji wykraczającym poza związek z pełnieniem tej funkcji (art. 5 ust. 2 DostInfPubU – w dalszej części).

Można stwierdzić, że przepisy RODO w równym stopniu gwarantują określone prawa osobom, których dane osobowe są przetwarzane, bez rozróżniania na osoby pełniące funkcje publiczne i ich niepełniące. Niemniej konstytucyjna zasada dostępu do informacji publicznej daje możliwość każdemu zainteresowanemu pozyskiwania informacji o osobach pełniących funkcje publiczne w trybie DostInfPubU. W tym więc obszarze warto zauważyć określone prawne gwarancje ochrony, jakie przysługują również osobom pełniącym funkcje publiczne.

Dotychczasowe bogate orzecznictwo sądów administracyjnych z obszaru prawa do informacji, ale i wyraźna wola ustawodawcy wyrażona w art. 5 ust. 2 DostInfPubU, wskazują, że to nie ochrona danych osobowych jest podstawą do ograniczenia prawa do informacji, ale przede wszystkim prawo do prywatności. Niewątpliwie jednak dane osobowe są kluczem do prywatności, gdyż trudno jest mówić o ochronie prywatności osób niezidentyfikowanych.

Ważne

Ochrona prywatności, jako podstawa do ograniczenia prawa do informacji, jest możliwa do realizacji wyłącznie wtedy, gdy określonego rodzaju dane osobowe dotyczące konkretnych osób fizycznych będą mogły być przetwarzane w trybie DostInfPubU.

Naczelny Sąd Administracyjny zwrócił uwagę, że „przesłankę prywatności osoby fizycznej należy (...) powiązać z konstytucyjnym potwierdzeniem prawa do prywatności uregulowanym w art. 47 Konst, który to przepis nakłada na władze publiczne obowiązek ochrony chronionych prawem dóbr jednostki przed nieuzasadnioną ingerencją”[2]. Nie oznacza to jednak, że na gruncie DostInfPubU relacje między dostępem do informacji oraz ochroną danych osobowych nie występują, ale należy je oceniać w oparciu o prywatność, o której mowa w art. 5 ust. 2 DostInfPubU, a dopiero następnie to rozwiązanie odnieść do przepisów RODO[3]. „Przy rozstrzyganiu o udostępnieniu określonej informacji publicznej należy mieć na uwadze to, że w myśl art. 1 ust. 2 i art. 5 ust. 1 DostInfPubU przepisy innych ustaw, w tym ustawy o ochronie danych osobowych zawierają unormowania ograniczające prawo do informacji publicznej. Jednak nie oznacza to, że przepisy o ochronie danych osobowych mają charakter szczególny w stosunku do ustawy o dostępie do informacji publicznej i w konsekwencji przysługuje im pierwszeństwo. Obie omawiane ustawy stanowią równorzędne akty prawne i w każdej sprawie konieczne staje się wyważenie możliwości realizacji prawa do informacji publicznej w sytuacji, gdy w tej informacji zawarte są jednocześnie dane osobowe. Z przepisów wymienionych ustaw nie można wyprowadzić generalnego zakazu udostępnienia informacji publicznej, w treści której figurują określone dane osobowe”[4].

Syntetycznie ujął to zagadnienie Trybunał Konstytucyjny w niezwykle istotnym wyroku odnoszącym się do granic dostępu do informacji w kontekście prawa do zachowania prywatności, również osób pełniących funkcje publiczne: „(...) prywatność osób pełniących funkcje publiczne, pozostając pod ochroną gwarancji konwencyjnych (zwłaszcza art. 8 europejskiej Konwencji[5]), może podlegać ograniczeniom, które, co do zasady, znajdować mogą usprawiedliwienie ze względu na wartość, jaką jest jawność i dostępność informacji o funkcjonowaniu instytucji publicznych w państwie demokratycznym. Wartość ta związana z transparentnością życia publicznego nie może prowadzić do całkowitego przekreślenia i zanegowania ochrony związanej z życiem prywatnych osób wykonujących funkcje publiczne”[6].

[1] „Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów”.
[2] Cyt. za wyr. NSA z 25.4.2014 r., I OSK 2499/13, Legalis.
[3] Por. *G. Sibiga*, Glosa do wyroku SN z 8.11.2012 r., I CSK 190/12, MoP 2013, Nr 8, s. 59–62.
[4] Wyr. NSA z 5.3.2013 r. (I OSK 2872/12, Legalis).
[5] Chodzi o art. 8 Europejskiej Konwencji Praw Człowieka otwartej do podpisu 4.11.1950 r., która weszła w życie 3.9.1953 r. W Polsce weszła w życie 19.1.1993 r. (Dz.U. z 1993 r. Nr 91, poz. 284). Artykuł 8 stanowi: „1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. 2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób”.
[6] Wyr. TK z 20.3.2006 r., K 17/05, Dz.U. z 2006 r. Nr 49, poz. 358, s. 2101; Wsp. 2006, Nr 13, s. 46; Prok. i Pr. 2006, Nr 6, poz. 43, s. 45; OTK Seria A 2006, Nr 3, poz. 30; ZNSA 2006, Nr 4–5, s. 77.

Zdefiniowanie osoby pełniącej funkcje publiczne dla potrzeb prawa do informacji

Zanim podejmiemy analizę pojęcia osoby pełniącej funkcję publiczną, warto wyraźnie podkreślić, że obowiązująca Konstytucja RP w art. 61 ust. 1 stanowi, że obywatel ma prawo do uzyskiwania informacji o działalności osób pełniących funkcje publiczne, natomiast same osoby, jeżeli nie piastują jednocześnie funkcji organu władzy publicznej, nie stają się podmiotami obowiązanymi do stosowania DostInfPubU.

Sztandarowym tego przykładem jest orzecznictwo NSA, wedle którego posłowie nie są podmiotami obowiązanymi do stosowania DostInfPubU, gdyż czym innym jest pytać o posłów, a czym innym pytać bezpośrednio posłów i w razie braku odpowiedzi skarżyć ich bezczynność w realizacji otrzymanych wniosków do WSA. Skargi takie jako niedopuszczalne podlegają odrzuceniu.

ORZECZENIE

Poseł na Sejm RP nie sprawuje władzy publicznej, bowiem nie ma ustawowego prawa egzekucji określonych zadań i celów. Posłowie na Sejm RP nie powinni być także utożsamiani z podmiotami wykonującymi zadania publiczne. Zadanie publiczne stanowi bowiem każde działanie administracji, jakie realizuje na podstawie przepisów ustaw. Z kolei poseł na Sejm RP nie wchodzi w skład administracji publicznej rozumianej jako struktury organizacyjnej państwa, na którą składa się administracja samorządowa trzech szczebli, administracja rządowa oraz administracja państwowa nie podlegająca rządowi (np. Prezydent, Najwyższa Izba Kontroli, Rzecznik Praw Obywatelskich, Krajowa Rada Sądownictwa, Narodowy Bank Polski). Nie można także podzielić stanowiska zażalenia, że poseł jest podmiotem zobowiązanym do udzielenia informacji publicznej (zob. post. NSA z 14.2.2014 r., I OZ 91/14, Legalis).

ORZECZENIE

Nie można również podzielić stanowiska skargi kasacyjnej, iż przepisy Konstytucji RP dają podstawę do twierdzenia, że poseł jest podmiotem zobowiązanym do udzielenia informacji publicznej. Co prawda art. 61 Konstytucji RP stanowi, iż obywatel ma prawo do uzyskiwania m.in. informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne, jednak według ust. 4 tego przepisu, tryb udzielania informacji, o których mowa w ust. 1 i 2, określają ustawy, a w odniesieniu do Sejmu i Senatu ich regulaminy [post. NSA z 14.12.2011 r. (I OSK 2287/11, Legalis) oraz post. NSA z 6.12.2012 r. (I OSK 2843/12, Legalis)].

Zatem podmiotami obowiązanymi do stosowania DostInfPubU nie są osoby pełniące funkcje publiczne, chyba że osoby takie pełnią jednocześnie funkcję organów władzy publicznej w rozumieniu art. 61 ust. 1 Konst lub innych podmiotów obowiązanych w rozumieniu art. 4 ust. 1 i 2 DostInfPubU. To te organy/podmioty są samodzielnie podmiotami obowiązanymi do stosowania DostInfPubU w rozumieniu art. 4 ust. 1 i 2 DostInfPubU.

W polskim porządku prawnym brak jest – od samego początku istnienia prawa do informacji – legalnej definicji osoby pełniącej funkcję publiczną. Pewną próbę regulacji zjawiska podjęto w projekcie ustawy o jawności życia publicznego, poprzez odesłanie bezpośrednie do definicji osoby pełniącej funkcję publiczną zawartej w art. 115 § 19 ustawy z 6.6.1997 r. – Kodeks karny (t.j. Dz.U. z 2018 r. poz. 1600 ze zm.)[7], jednak ma to obecnie mniejsze znaczenie wobec zawieszenia prac nad projektem ustawy.

W takiej sytuacji, poszukując definicji osoby pełniącej funkcje publiczne dla potrzeb prawa do informacji publicznej, należy odwołać się do bogatego orzecznictwa sądów administracyjnych. Sądy administracyjne w licznych orzeczeniach[8] będących przejawem sądowej kontroli procesu realizacji prawa do informacji publicznej, uznają zaproponowany w wyroku Trybunału Konstytucyjnego (K 17/05, Legalis)[9] wzorzec dochodzenia do odpowiedzi na pytanie – jakie cechy powinna spełniać osoba uznana za pełniącą funkcję publiczną dla potrzeb prawa do informacji – za powszechnie akceptowany. Zatem wskazane przez TK zasady interpretacji pojęcia „pełnienie funkcji publicznej", są obecnie wzorcem postępowania i analizy dla sądownictwa administracyjnego.

Wobec ciągłego braku legalnej definicji osoby pełniącej funkcję publiczną dla potrzeb prawa do informacji, należy przyjąć, że w treści wyroku TK (K 17/05, Legalis) odnajdujemy najbardziej realny i faktycznie osiągalny model poszukiwania odpowiedzi na pytanie, kto w konkretnej instytucji jest osobą pełniącą funkcje publiczne z punktu widzenia prawa do informacji. „Analiza bardzo bogatego orzecznictwa sądowego w tym zakresie pozwala przyjąć, że ścierają się ze sobą dwa sposoby definiowania osób pełniących funkcje publiczne: **definicja funkcjonalna** oraz **definicja instytucjonalna**. W moim przekonaniu, dla potrzeb prawa do informacji dominującym sposobem definiowania pojęcia «osoba pełniąca funkcję publiczną», powinno być stosowanie definicji funkcjonalnej, wedle której osobą pełniącą funkcję publiczną jest ta osoba, która współwykonuje zadania przynależne podmiotowi publicznemu, w którego strukturach jest zatrudniona. Decydujący jest rodzaj zadań, jakie wykonuje, natomiast rzeczą wtórną jest status

[7] Zachęcam do zapoznania się w tym zakresie z moim artykułem pt.: ‚Nowe zasady dostępu do informacji publicznych – uwagi krytyczne do projektu ustawy o dostępie do informacji publicznej, Informacja w Administracji 2018, Nr 2, s. 33–41.

[8] Na dzień 5.10.2018 r. system CBOSA podaje, że w bazie orzeczeń sądów administracyjnych, od dnia wejścia w życie DostInfPubU, czyli od 1.1.2002 r. do 4.10.2018 r. powstało 12 364 orzeczeń sądów w kategorii spraw „Dostęp do informacji publicznej".

[9] Fraza „K 17/05" pojawiła się w okresie od dnia wejścia w życie DostInfPubU, czyli 1.1.2002 r. do 4.10.2018 r., w kategorii „Dostęp do informacji publicznej" – w 85 wyrokach NSA oraz 339 wyrokach WSA. Informacja ze strony CBOSA z 5.10.2018 r., godz. 6.31.

pracowniczy i zaszeregowanie w danej służbie czy formacji. W przeciwieństwie do definicji instytucjonalnej, która zakłada, że o statusie osoby pełniącej funkcje publiczne decyduje przede wszystkim zatrudnienie w określonej instytucji, bez względu na to, jaki zakres obowiązków dana osoba realizuje. Przyjęcie jako wiodącej definicji funkcjonalnej, pozwala w sposób bardziej realny uwzględniać ogromną różnorodność specyfiki podmiotów wykonujących zadania publiczne, lub gospodarujących mieniem publicznym, przez co stają się podmiotami zobowiązanymi do stosowania DostInfPubU"[10].

Dla ustalenia statusu osoby pełniącej funkcje publiczne w rozumieniu art. 61 ust. 1 Konst oraz art. 5 ust. 2 DostInfPubU, przyjąć należy obowiązkowe zaistnienie czterech okoliczności:

1. Pomiędzy osobą a instytucją musi istnieć organizacyjna więź, na podstawie której osoba ta działa w imieniu instytucji.
2. W ramach swoich obowiązków osoba musi wykonywać zadania tej instytucji publicznej[11].
3. Osoba w ramach swych obowiązków wykonuje działania władcze oddziałujące na podmioty znajdujące się na zewnątrz danej struktury, które podejmowane są przy stosowaniu określonej, choćby niewielkiej dozy samodzielności.
4. Z grupy tej wyłączone są osoby, które wykonują wyłącznie działania o charakterze technicznym i usługowym[12].

Prawna reglamentacja sfery informacyjnej wykazującej związek z pełnieniem funkcji publicznej

Podstawowym przepisem regulującym zakres informacji o osobach pełniących funkcje publiczne, które są informacjami publicznymi, jest art. 5 ust. 2 zd. 2 DostInfPubU, zgodnie z którym ograniczenie prawa do informacji publicznej ze względu na prywatność osoby fizycznej nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Wprawdzie art. 61 Konst nie zawiera odpowiedzi na pytanie, jakiego rodzaju informacje o osobach pełniących funkcje publiczne mogą być przekazywane w odpowiedzi na otrzymany wniosek o udostępnienie informacji publicznej, niemniej sądy administracyjne zwracają uwagę, że generalnie do zagadnienia prawa do informacji należy podchodzić w ujęciu podmiotowo-przedmiotowym. „Każdy wniosek o udostępnienie informacji publicznej podlega ocenie z punktu widzenia przesłanek podmiotowych i przedmiotowych. Udostępnienie informacji objętej wnioskiem może bowiem nastąpić jedynie wówczas, gdy podmiot, do którego zostało skierowane żądanie, należy do katalogu podmiotów zobowiązanych do udostępniania informacji publicznej określonych w art. 4 ust. 1 i 2 DostInfPubU oraz gdy stwierdzone zostanie, że żądana informacja stanowi informację o charakterze publicznym w rozumieniu art. 1 ust. 1 DostInfPubU"[13]. „Prawo do informacji publicznej to zatem prawo do informacji o działalności podmiotów wskazanych w Konstytucji RP, co oznacza, że informacja dotycząca tych podmiotów, lecz wykraczająca poza granice ich działalności nie jest informacją publiczną"[14].

Ważne

Nie każda zatem informacja dotycząca osoby pełniącej funkcję publiczną będzie mogła uzyskać miano informacji publicznej lub nawet będąc informacją publiczną nie każda będzie mogła być udostępniona ze względu na sferę chronioną wyznaczoną prawem do prywatności.

Należy zatem przyjąć za NSA, że „aktywność, która jest związana ze sferą życia prywatnego i jednocześnie nie pozostaje w jakimkolwiek związku z (...) działaniami ukierunkowanymi na wypełnianie zadań publicznych nie stanowi działalności, o jakiej mowa w art. 61 ust. 1 Konstytucji RP. Istnieje sfera ogólnej działalności osób pełniących funkcje publiczne, w tym piastunów organów i urzędów, która nie podlega prawu do informacji publicznej"[15]. „Informacja publiczna to taka informacja, która – co do zasady – nie obejmuje spraw prywatnych, niepublicznych, osobistych, intymnych (danych osobowych, życia prywatnego, rodzinnego), a także informacji, które naruszałyby godność, cześć (dobre imię), a więc dobra osobiste organu lub osób będących piastunem organu (*M. Jabłoński*, Udostępnianie informacji publicznej w trybie wnioskowym, Wrocław 2009). Jeśli informacja dotyczy sfery prywatnej, niezwiązanej z działalnością państwa nie podlega ona udostępnieniu"[16]. „Zakres stosowania DostInfPubU wy-

[10] *P. Sitniewski*, Kim jest osoba pełniąca funkcję publiczną?, Informacja w Administracji 2017, Nr 3, s. 52.

[11] Sam sposób i charakter zatrudnienia w instytucji publicznej nie ma decydującego znaczenia dla uznania danej osoby za pełniącą funkcję publiczną. Decydujące bowiem jest ustalenie, czy zakres obowiązków konkretnej osoby mieści się w zakresie zadań instytucji, w której ramach wykonuje ona swoje obowiązki, a jednocześnie czy te obowiązki można uznać za wykraczające poza czynności czysto usługowe i techniczne. Decydujące znaczenie ma ustalenie, jaki jest zakres obowiązków konkretnej osoby w odniesieniu do zakresu zadań i działalności instytucji, w której osoba ta wykonuje swoje obowiązki/prace/zlecenie.

[12] Nie będą osobami pełniącymi funkcje publiczne ci, którzy w ramach prawnie określonego stosunku łączącego ich z instytucją publiczną wykonują czynności techniczne, organizacyjne niezbędne dla funkcjonowania instytucji, ale w swej istocie nie będące realizacją zadań tejże instytucji.

[13] Wyr. WSA w Gdańsku z 23.11.2016 r., (II SAB/Gd 133/16, Legalis) oraz pozostałe wyroki WSA w Gdańsku (30.5.2017 r., II SAB/Gd 26/17; 11.10.2017 r., II SAB/GD 42/17; 5.4.2018 r., II SAB/GD 62/17; 16.5.2018 r., II SAB/GD 35/18; 14.8.2018 r., II SAB/GD 62/18; 4.9.2018 r., II SAB/GD 51/18, Legalis).

[14] Wyr. NSA z 21.4.2017 r. (I OSK 1953/15, Legalis).

[15] Wyr. NSA z 21.4.2017 r., (I OSK 1953/15, Legalis).

[16] Wyr. WSA w Krakowie z 7.3.2016 r., (II SAB/Kr 18/16, Legalis).

tycza tylko dostęp do informacji publicznej, nie zaś publiczny dostęp do wszelkich informacji. Ustawa ta znajduje zastosowanie jedynie w sytuacjach, gdy spełniony jest jej zakres podmiotowy i przedmiotowy”[17]. Na poziomie rozważań konstytucyjnych istotna jest ocena TK, że „gwarancje konstytucyjne dotyczące prawa dostępu do informacji (art. 61) nie mogą być w pełni utożsamione z prawem określonym w art. 54 Konstytucji[18], zapewniającym wolność wyrażania poglądów oraz pozyskiwania i rozpowszechniania informacji. (…) Nie każda bowiem informacja, która zgodnie z wolnością ujętą w art. 54 Konstytucji może być pozyskana i rozpowszechniona, w tym także odnosząca się do sfery prywatnej osoby, może być uznana za informację, co do której istnieje po stronie danego organu władzy publicznej obowiązek ujawnienia, skonkretyzowany w DostInfPubU”[19].

Określenie zakresu pojęciowego pojęć „warunki powierzenia i wykonywania funkcji publicznej”

Rozważając powyższe poglądy, należy się zastanowić, czym są warunki powierzenia funkcji publicznej, a czym są warunki wykonywania funkcji publicznej. W samej DostInfPubU nie znajdziemy wyjaśnienia, jakiego rodzaju informacje są objęte dyspozycją art. 5 ust. 2 DostInfPubU. Czy są to pojęcia tożsame, czy też znajdują się na biegunowo odległych od siebie obszarach?

Wydaje się, że warunki powierzenia funkcji publicznej należy rozumieć następująco: są to wszelkie warunki formalne, jakie musi spełniać kandydat na dane stanowisko, które albo wynikają wprost z przepisów ustawowych[20], albo też dodatkowo są doprecyzowywane lub dookreślane w ramach danego naboru na stanowisko. Są to informacje o osobie, które warunkują – z formalnego punktu widzenia – jej zatrudnienie, awans, utrzymanie na stanowisku związanym z pełnieniem funkcji publicznej, a które regulowane są przepisami powszechnie obowiązującymi lub na ich podstawie są uszczegóławiane w związku z naborem na stanowisko określone w ogłoszeniu o naborze. Z całą pewnością podstawowym dokumentem określającym warunki powierzenia jest umowa o pracę, czy też inna umowa kontraktowa (umowa cywilnoprawna powierzenia określonych czynności, np. kontrakt menadżerski jako rozbudowana umowa zlecenia, której przedmiotem jest powierzenie wykonywania zarządu, np. nad szpitalem).

Bogate orzecznictwo sądowe również wskazuje na potrzebę uznania, że proces rekrutacji na stanowiska w instytucjach publicznych musi się charakteryzować transparentnością.

ORZECZENIE

Osoba kandydująca do służby publicznej musi godzić się już od momentu złożenia zgłoszenia do procedury naboru na stanowisko w służbie publicznej z zainteresowaniem opinii publicznej co do samego faktu jej kandydowania i kwalifikacji umożliwiających ubieganie się o określone stanowisko. (…) Publiczne ujawnienie faktu ubiegania się konkretnych osób o powołanie na stanowisko w służbie publicznej – a do tego sprowadzało się żądanie skarżącej, nie stanowi w żadnej mierze naruszenia prawa do prywatności, które mogłoby uzasadnić odmowę uwzględnienia dostępu do informacji publicznej [wyr. NSA z 12.6.2014 r. (I OSK 2488/13, Legalis)].

ORZECZENIE

Dokumenty wskazujące na poziom kompetencji osoby sprawującej funkcję publiczną stanowią informację publiczną także w zakresie formy. Dokumenty dotyczące wykształcenia, specjalizacji takiej osoby w momencie złożenia do właściwego organu w związku z wykonywaniem określonej funkcji publicznej, tracą swój walor dokumentu prywatnego i stanowią źródło informacji publicznej na temat kompetencji osoby sprawującej funkcję publiczną w rozumieniu art. 6 ust. 1 pkt 2 lit. d) DostInfPubU [wyr. WSA w Szczecinie z 18.5.2017 r. (II SAB/Sz 155/16, Legalis)].

Natomiast warunki wykonywania funkcji publicznej należy rozumieć dwojako:

1) po pierwsze, jako sferę faktów i informacji związanych z oceną, w jaki sposób i w jakim zakresie osoba wypełnia powierzone jej zadania publiczne, co wynika z mniej lub bardziej sformalizowanych systemów oceny (z reguły są to oceny dokonywane cyklicznie lub co jakiś czas w zależności od stosunku zatrudnienia danej osoby w instytucji publicznej)[21];
2) po drugie, jako wszelkie zdarzenia, które mają bezpośredni wpływ na warunki powierzenia tej funkcji, zarówno traktowane jako warunkujące pełnienie funkcji, jak i uniemożliwiające jej dalsze pełnienie.

Przykładowo, jeżeli pełnienie danej funkcji publicznej jest uzależnione od posiadania obywatelstwa polskiego, niekaralności, wieku *etc*., to są to okoliczności warunkujące, a każda zmiana w tym zakresie staje się automatycznie okolicznością uniemożliwiającą dalsze pełnienie funkcji. Nie oznacza to jednak, że w trybie DostInfPubU każdy ma prawo uzyskać informacje o danej osobie z Krajowego Rejestru Karnego, gdyż ustawa z 24.5.2000 r. o Krajowym

[17] Wyr. NSA z 18.5.2011 r., (I OSK 198/11, Legalis) oraz liczne wyroki NSA potwierdzające tę tezę: 21.9.2012 r., I OSK 1393/12; 27.9.2012 r., I OSK 758/12; 9.10.2012 r., I OSK 1737/12; 27.11.2012 r., I OSK 1985/12; Legalis oraz wcześniejsze 11.1.2018 r. I OSK 549/16; 15.6.2018 r. I OSK 1187/18; 15.6.2018 r., I OSK 1188/18; Legalis.

[18] Artykuł 54 ust. 1 Konstytucji RP: „Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji”.

[19] Cyt. wyr. TK z 20.3.2006 r., (K 17/05, Legalis).

[20] Przykładowo wymogi jakie określa art. 6 ustawy o pracownikach samorządowych z 21.11.2008 r., (t.j. Dz.U. z 2018 r. poz. 1260 ze zm.) jako obligatoryjne wobec kandydatów na określone stanowiska lub też wymogi wobec osób zatrudnianych w służbie cywilnej, jakie stawia art. 4 ustawy o służbie cywilnej z 21.11.2008 r. (t.j. Dz.U. z 2018 r. poz. 1559 ze zm.).

[21] Zob. zasady oceny pracy w służbie cywilnej określone w art. 37, 38, 81, 108 ustawy z 21.11.2008 r. o służbie cywilnej (t.j. Dz.U. z 2018 r. poz. 1559 ze zm.) oraz zasady oceny pracowników samorządowych określone w art. 27 i 28 ustawy z 21.11.2008 r. o pracownikach samorządowych (t.j. Dz.U. z 2018 r. poz. 1260 ze zm.).

Rejestrze Karnym (t.j. Dz.U. z 2018 r. poz. 1218 ze zm.; dalej: KrRejKarU) wyraźnie stanowi, jakim podmiotom i pod jakimi warunkami są udostępniane informacje z KRK[22]. Podobnie sytuacja będzie wyglądała, jeżeli pełnienie danej funkcji jest uzależnione od posiadanego wieku. Nie oznacza to wcale, że każdy w trybie DostInfPubU ma prawo zapoznać się z kopią aktów stanu cywilnego, które, mimo że stanowią wyłączny dowód zdarzeń w nich stwierdzonych – zawierają całą masę informacji z życia prywatnego, które w żadnym stopniu nie wykazują związku z pełnieniem funkcji publicznej[23].

W tym miejscu należy przywołać orzecznictwo sądów administracyjnych, z których wynika, że aczkolwiek nośniki informacji publicznej mogą być bardzo różne (nie tylko dokumenty urzędowe), to zawsze należy odróżniać prawo do informacji od prawa do uzyskania nośnika tejże informacji:

1. „Definicja dokumentu urzędowego, zawarta w ustępie 2 art. 6 DostInfPubU, nie stanowi podstawy do ograniczenia dostępu do informacji publicznej, definiowanej w art. 1 ust. 1 DostInfPubU”[24].

2. „Informacją publiczną są nie tylko dokumenty bezpośrednio redagowane i wytworzone przez organ administracji publicznej, ale charakter mają również takie dokumenty, które organ wykorzystuje do zrealizowania powierzonych prawem zadań. (…) Podstawowe bowiem znaczenie ma fakt, że dokumenty te służą realizacji zadań publicznych przez określone organy i zostały wytworzone na zlecenie tych organów”[25].

3. „Przepisy DostInfPubU o dostępie do informacji publicznej nie ograniczają zakresu dostępu do informacji jedynie do dokumentów urzędowych”[26].

4. „Pojęcie dokumentu urzędowego różni się od dokumentu zawierającego informację publiczną. Istotne znaczenie ma zatem nie to, czy dokument został sporządzony przez funkcjonariusza publicznego w znaczeniu przepisów Kodeksu karnego, lecz przede wszystkim to czy zawiera on informację publiczną”[27].

Wpływ RODO – zakres autonomii informacyjnej osób pełniących funkcje publiczne

Przepisy RODO w trzech miejscach odnoszą się do zagadnienia dostępu do informacji publicznych: w art. 17 ust. 3 lit. a), art. 86 i w motywach 4, 65, 153 i 154. Najistotniejsze są te zawarte w art. 17 ust. 3 lit. a) oraz art. 86, będące rozwinięciem zapisów we wskazanych motywach.

Z treści art. 86 wynika, że dane osobowe zawarte w dokumentach urzędowych, które posiada podmiot obowiązany do stosowania DostInfPubU, mogą zostać przez ten podmiot ujawnione zgodnie z prawem krajowym, któremu ten podmiot podlega, dla pogodzenia publicznego dostępu do dokumentów z prawem do ochrony danych. Przy założeniu, że z art. 5 ust. 2 DostInfPubU wynika, iż przedmiotem prawa do informacji mogą być informacje dotyczące dwóch grup osób: pełniących i niepełniących funkcji publicznych, można stwierdzić, że w obu tych grupach różnie kształtowany jest zakres autonomii informacyjnej. Poprzez autonomię informacyjną rozumiem taki zakres informacji o osobie, który dla ich udostępnienia wymaga zgody osoby, której one dotyczą. Jeżeli określone informacje dotyczące osób pełniących funkcje publiczne nie wymagają ich zgody dla ich udostępnienia w trybie DostInfPubU, gdyż wykazują realny i ścisły związek z pełnioną funkcją, są to informacje nieobjęte zakresem autonomii informacyjnej tej osoby. Im bardziej dana osoba zaczyna zwiększać swój wpływ na sferę publiczną z racji pełnienia funkcji publicznej oraz im bardziej jej działania mają bezpośredni wpływ na sferę publiczną, tym bardziej kurczy się jej autonomia informacyjna.

Sfera dóbr chronionych w kontekście anonimizacji

Z treści motywu 154 RODO wynika, że obowiązywanie RODO pozwala na uwzględnienie zasady publicznego dostępu do dokumentów urzędowych, który to dostęp można uznać za interes publiczny. A jednocześnie w motywie 154 użyto określenia o fragmentach dokumentów dostępnych w ramach krajowych systemów dostępowych. Można zatem stwierdzić, że przepisy RODO przewidują, a tym samym akceptują praktykę anonimizacji dokumentów będących nośnikiem informacji publicznej, a będących przedmiotem wniosku o udostępnienie informacji publicznej.

Samą potrzebę stosowania czynności anonimizacyjnych potwierdza bogate w tym zakresie orzecznictwo sądów administracyjnych powstałe na gruncie stosowania DostInfPubU, akceptując praktykę polegającą na zasłonięciu części dokumentów, przy jednoczesnym braku odmowy udostępnienia informacji w całości:

„Proces anonimizacji jest konieczny wtedy, gdy dokument jako całość stanowi informację publiczną, lecz określone zawarte w nim dane nie stanowią informacji publicznej i z tego powodu nie są ujawnianie, gdyż za ich anonimizacją przemawiają inne wartości prawnie chronione. Anonimizacja jest czynnością o charakterze technologicznym, dokonywaną na dokumencie stanowiącym informację publiczną, polegającą

[22] Zob. art. 6 i 6a KrRejKarU.
[23] Zob. art. 3 ustawy z 28.11.2014 r. – Prawo o aktach stanu cywilnego (t.j. Dz.U. z 2016 r. poz. 2064 ze zm.).
[24] Wyr. NSA z 7.3.2012 r. (I OSK 2265/11, Legalis).
[25] Wyr. NSA z 15.7.2011 r., (I OSK 667/11, Legalis). Podobnie w innych wyrokach NSA: (9.2.2007 r., I OSK 517/06; 7.12.2010 r., I OSK 1774/10; 18.9.2008 r., I OSK 315/08, Legalis).
[26] Wyr. NSA z 27.2.2008 r., (I OSK 1744/2007, Legalis) oraz wyr. NSA z 5.3.2013 r. (I OSK 2888/12, Legalis).
[27] Wyr. NSA z 29.2.2012 r., (I OSK 2215/11, Legalis) oraz powtórzone w pozostałych wyrokach NSA (3.1.2012 r., I OSK 2311/12; 27.6.2013 r., I OSK 513/13; 27.6.2017 r., I OSK 2894/15; 24.8.2016 r., I OSK 12/16, Legalis).

na zasłonięciu części tego dokumentu, która to część zawiera informacje niestanowiące informacji publicznej. Potrzeba anonimizacji nie wynika z faktu odmowy dostępu do informacji, gdyż ta następuje w drodze decyzji administracyjnej, lecz z faktu, iż określone dane nie stanowią informacji publicznej"[28].

„W sytuacji, gdy żądanie wniosku dotyczy udostępnienia dokumentu, a nie wyłącznie informacji o jego treści, udostępnienie dokumentu zanonimizowanego, który zwykle stanowi kserokopię oryginału z zasłoniętymi danymi osobowymi, w większości przypadków czyni zadość temu żądaniu. Wskazać bowiem należy, że praktyka anonimizowania (zaczerniania, wybiałkowania) danych osobowych w udostępnianych informacjach publicznych, co do zasady, nie jest kwestionowana"[29].

„Z zestawienia zasady jawności informacji publicznych oraz obowiązku ochrony prywatności i danych osobowych osób fizycznych, można wyprowadzić wniosek, że możliwe jest udostępnianie informacji publicznej w sposób nie naruszający wskazanych dóbr chronionych. Służy temu m.in. stosowana przez organy tzw. anonimizacja danych wrażliwych. W takim wypadku nie zachodzi jednak potrzeba wydawania oddzielnej decyzji na podstawie art. 16 ustawy, gdyż przepis ten może mieć zastosowanie tylko w wypadku odmowy udostępnienia informacji, a nie w przypadku jej udzielenia z zachowaniem zasady ochrony dóbr chronionych"[30].

Zdaniem NSA „nie można podzielić poglądu, że w każdym wypadku, kiedy zachodzi możliwość ujawnienia «przy okazji» udostępniania informacji publicznej danych podlegających ochronie na podstawie przepisów ustawy o ochronie danych osobowych, należy całkowicie odmówić udzielenia informacji na podstawie przepisu art. 16 ustawy, zwłaszcza, gdy strona nie jest sama zainteresowana ujawnieniem takich danych, żądając udzielenia informacji o konkretnych sprawach publicznych"[31].

„Ochrona prywatności w zakresie realizacji prawa dostępu do informacji publicznej charakteryzuje się dążeniem do poddania anonimizacji konkretnego dokumentu, co jest równoznaczne z eliminacją danych osobowych pozwalających na zidentyfikowanie konkretnej osoby fizycznej. Tego rodzaju działanie postrzega się jako pozbawienie dokumentu cech indywidualizujących, a tym samym identyfikujących konkretną osobę fizyczną w sposób, który mógłby stanowić naruszenie jej prywatności"[32].

Na marginesie warto wspomnieć, że anonimizacja jako czynność nie jest uznawana za przetworzenie w rozumieniu art. 3 ust. 1 pkt 1 DostInfPubU i jest dokonywana jako czynność materialno-techniczna, bez potrzeby wydawania w tym zakresie decyzji administracyjnej o odmowie udostępnienia informacji publicznej.

„Wprawdzie samo zanonimizowanie wnioskowanych do udostępnienia orzeczeń nie stanowi przetworzenia informacji wynikającej z tych orzeczeń, a jedynie jej przekształcenie, dlatego stanowi ona informację prostą, to jeżeli jednak utworzenie zbioru informacji prostych wymaga takiego nakładu środków i zaangażowania pracowników, które negatywnie wpływa na tok realizacji ustawowych zadań nałożonych na zobowiązanego do udostępnienia informacji publicznej, a w szczególności gdy wymaga to analizowania całego zasobu posiadanych dokumentów w celu wybrania tylko tych, których oczekuje wnioskodawca, to jest to informacja przetworzona"[33].

„Zanonimizowanie danych, co do zasady, nie wymaga wydania decyzji o odmowie udostępnienia informacji publicznej"[34].

„Zasłonięcie części dokumentu zawierającego określone dane, które nie stanowią informacji publicznej, można wciąż uznać za anonimizację wtedy, gdy czynność ta nie pozbawi dokumentu waloru informacyjnego, jaki wynika ze złożonego wniosku o udostępnienie informacji publicznej. Anonimizacja dokumentu nie może niweczyć rezultatu, do którego dążył wnioskodawca, składając wniosek"[35].

Podstawowe obowiązki informacyjne administratora danych

Uregulowanie zawarte w art. 13 RODO nakłada na administratora określone obowiązki informacyjne wobec osoby, której dane dotyczą. Obowiązki tam określone dotyczą sytuacji, gdy dochodzi do tzw. pierwotnego zbierania danych osobowych od osoby, której dane dotyczą, a ten sposób zbierania danych jest najczęściej występującym, jeżeli chodzi o pozyskiwanie danych o osobach pełniących funkcje publiczne.

Szczególne znaczenie z punktu widzenia prawa do informacji o osobach pełniących funkcje publiczne, mają dwa obowiązki, jakie ciążą na administratorze danych podczas pozyskiwania danych osobowych w sposób pierwotny:

Obowiązek poinformowania o celu przetwarzania danych oraz o podstawie prawnej przetwarzania (art. 13 ust. 1 lit. c) RODO)

W omawianym obszarze oznaczałoby to, że administrator danych ma obo-

[28] *P. Sitniewski*, Dostęp do informacji publicznej. Pytania i odpowiedzi. Wzory pism, Warszawa 2016, s. 132.
[29] Wyr. WSA we Wrocławiu z 25.4.2017 r. (IV SAB/Wr 34/17, Legalis).
[30] Wyr. NSA z 11.1.2013 r. (I OSK 2267/12, Legalis) oraz wyr. NSA z 12.4.2017 r. (I OSK 1928/15, Legalis) i wyr. NSA z 20.9.2017 r. (I OSK 227/17, Legalis).
[31] Wyr. NSA z 11.1.2013 r. (I OSK 2267/12, Legalis).
[32] Wyr. NSA z 30.1.2015 r. (I OSK 617/14, Legalis).
[33] Zob. wyr. NSA z 18.2.2014 r. (I OSK 2129/13, Legalis).
[34] Zob. wyr. WSA we Wrocławiu z 20.12.2016 r. (IV SA/Wr 369/16, Legalis).
[35] *P. Sitniewski*, Dostęp do informacji publicznej. Pytania i odpowiedzi. Wzory pism, Warszawa 2016, s. 134. Zob. również wyr. WSA w Gliwicach z 1.10.2013 r. (IV SAB/Gl 86/13, Legalis).

wiązek poinformować osobę pełniącą funkcje publiczne, jakiego rodzaju informacje jej dotyczące mogą być udostępniane w ramach realizacji prawa do informacji. Nie ma tu większego znaczenia, czy realizacja prawa do informacji będzie się odbywać na wniosek, czy w trybie bezwnioskowym poprzez zamieszczenie informacji o osobach na stronie BIP (art. 10 ust. 1 DostInfPubU). W każdym przypadku realizacji prawa do informacji, zarówno wnioskowym jak i bezwnioskowym, osoba pełniąca funkcje publiczne powinna być poinformowana, jakiego rodzaju informacje jej dotyczące będą mogły być przedmiotem udostępnienia w trybie DostInfPubU. Istnienie tego obowiązku wynika z konstrukcji art. 13 RODO. Żaden przepis nie wyłącza określonych tam obowiązków, tak jak np. czyni to art. 17 ust. 3 RODO – wyłączając tzw. prawo do zapomnienia w zakresie, w jakim przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji. Istnienie tego typu obowiązków musi być uznane za element porządkujący określenie granic jawności informacji o osobach pełniących funkcje publiczne. Ma to szczególne znaczenie wobec faktu, że w obecnym stanie prawnym, osoba o którą pyta wnioskodawca realizujący prawo do informacji, nie posiada żadnego statusu w typie postępowania regilowanym DostInfPublU . Osoba taka nie posiada żadnych praw procesowych i nie może uczestniczyć w toczącym się postępowaniu, którego przedmiotem są m.in. dane osobowe jej dotyczące.

W orzecznictwie sądowym wskazuje się, że „stroną postępowania w sprawie o udostępnienie informacji publicznej, wszczynanego na wniosek, jest wyłącznie wnioskodawca, co powoduje, że w sprawach tych nie znajduje zastosowania art. 28 KPA”[36]. Do 29.12.2011 r. obowiązywał przepis art. 22 DostInfPubU, który podmiotowi, którego dotyczy wyłączenie informacji publicznej, przyznawał interes prawny w przystąpieniu w charakterze interwenienta ubocznego po stronie pozwanej.

Dodatkowo, jeżeli podmiot obowiązany do stosowania DostInfPubU zatrudnia minimum 250 osób[37], to zgodnie z art. 30 ust. 1 lit. b) RODO ma obowiązek prowadzić rejestr czynności przetwarzania. Obowiązek ten będzie miał zastosowanie wobec dużych urzędów administracji[38], choć sam jako taki ma charakter następczy i jakiegokolwiek wpływu na określenie granic jawności informacji o osobach pełniących funkcje publiczne raczej mieć nie będzie.

Obowiązek poinformowania o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją (art. 13 ust. 1 lit. e) RODO)

W zakresie realizacji tego obowiązku, informacja powinna być krótka i odzwierciedlać zakres podmiotowy prawa do informacji. Każda osoba pełniąca funkcję publiczną powinna być poinformowana, że określone informacje mogą być udostępnione każdemu, kto o to wniesie w trybie wnioskowym określonym w art. 2 ust. 1 i art. 10 ust. 1 DostInfPubU. Wynika to wprost z treści art. 2 DostInfPubU, zgodnie z którym prawo do informacji przysługuje każdemu i realizujący prawo do informacji nie musi wykazywać się posiadaniem interesu prawnego lub prawa.

Dodatkowe obowiązki informacyjne administratora danych

Administrator posiada również inne obowiązki jakie formułuje RODO, które jednak nie mają tak bezpośredniego wpływu na ustalenie granic jawności informacji o osobach pełniących funkcje publiczne, jak wymienione powyżej. Są one następujące:

Informacja o okresie, przez który dane osobowe będą przechowywane

W krajowym systemie prawa do informacji, a więc w treści DostInfPubU brak jakichkolwiek regulacji na ten temat. Nie można zatem prawa do informacji publicznej o osobach pełniących funkcje publiczne ograniczyć wyłącznie do osób aktualnie zatrudnionych. Ustawa o dostępie do informacji publicznej obejmuje również sytuacje, jakie miały miejsce przed jej wejściem w życie (1.1.2002 r.). Jedynym wskaźnikiem czasowym stosowania DostInfPubU może być czas przechowywania dokumentów kadrowych, po upływie którego są one przekazywane do archiwum państwowego. W takim momencie dostęp do nich nie jest już regulowany DostInfPubU i jako taki, z punktu widzenia RODO, podlega odmiennemu reżimowi prawnemu (patrz art. 14 ust. 5 lit. b) RODO).

Jednocześnie same przepisy RODO pozbawiają prawa do zapomnienia (patrz art. 17 ust. 1 i 2 RODO), w zakresie w jakim przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji. Z tego też powodu **osoby pełniące funkcje publiczne po zakończeniu pełnienia tychże funkcji, zgodnie z treścią art. 17 ust. 3 RODO, nie posiadają prawa do zapomnienia, o którym mowa w art. 17 ust. 1 i 2 RODO**.

Oczywiście istniejące regulacje krajowe mogłyby ustalić okres dla przechowywania określonych informacji o osobach, a związanych z realizacją prawa do informacji. Przykładem tego typu regulacji jest np. określenie, przez jaki okres przechowuje się jawne

[36] Wyr. NSA z 4.11.2016 r. (I OSK 1372/15, Legalis).

[37] Artykuł 30 ust. 5 RODO przewiduje sytuacje, gdy obowiązki rejestracji czynności obejmowałyby również podmiot zatrudniający poniżej 250 osób.

[38] Zob. art. 30 ust. 5 RODO, który przewiduje jednak pod pewnymi warunkami zastosowanie tego obowiązku nawet przy niespełnieniu warunku zatrudnienia 250 osób.

oświadczenia majątkowe[39] oraz przez jaki okres przechowuje się na stronie BIP określonego rodzaju dokumenty (szczególnie przy ogłoszeniach różnego rodzaju na BIP.

Informacja czy podanie danych osobowych jest wymogiem ustawowym oraz czy osoba, której dane dotyczą, jest obowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych (art. 13 ust. 2 lit. e) RODO)

Wobec braku wyraźnego wskazania przez ustawodawcę jakiego rodzaju informacje dotyczące osoby pełniącej funkcję publiczną mogą być każdemu udostępnione bez jej wiedzy i zgody, trudno jednoznacznie jest określić zakres autonomii informacyjnej osoby.

Obowiązek jest zrealizowany, jeżeli administrator poinformuje, że przekazywanie danych następuje w celu wypełnienia obowiązku prawnego ciążącego na administratorze (patrz art. 6 ust. 1 lit. c) RODO). W żadnym wypadku odpowiedzialności za niewłaściwą realizację prawa do informacji nie będzie ponosić osoba, której dane dotyczące były przedmiotem wniosku o udostępnienie informacji publicznej. Osoba ta bowiem nie jest stroną postępowania i jedyną odpowiedzialność ponosi podmiot obowiązany, którym jest dana instytucja, nie zaś sama osoba pełniąca funkcję publiczną. Zatem konsekwencje niepodania tych danych, o czym mowa w art. 13 ust. 2 lit. e) RODO ciążyć zawsze będą na podmiocie obowiązanym do stosowania DostInfPubU w rozumieniu art. 4 ust. 1 i 2 DostInfPubU, a będzie to egzekwowane w formule skargi do WSA.

Poinformowanie o prawie do wniesienia sprzeciwu wobec przetwarzania (art. 13 ust. 2 lit. b) RODO)

Tego typu sytuacji nie sposób wykluczyć, wobec faktu braku jasnego określenia, jakiego rodzaju informacje dotyczące osób pełniących funkcje publiczne są wyłączone z zakresu autonomii informacyjnej. Może w praktyce zatem dojść do sytuacji, w której osoba neguje prawo administratora do przekazywania określonych informacji jej dotyczącej w trybie DostInfPubU. Obowiązująca DostInfPubU nie zawiera gwarancji tego typu. Jedynym przepisem jest art. 5 ust. 2 zd. 2, z którego wynika, że jeżeli wniosek obejmuje osoby niepełniące funkcji publicznych, to ich przekazanie wnioskodawcy może nastąpić tylko pod warunkiem uzyskania zgody tej osoby. W przepisie mowa jest o rezygnacji osoby fizycznej z przysługującego jej prawa do ochrony prywatności. Orzecznictwo sądowe potwierdza dualne podejście do osób określonych w art. 5 ust. 2 DostInfPubU.

ORZECZENIE

Zdaniem WSA w Białymstoku „informację publiczną stanowią również kwoty wypłaconych nagród, konkretnie wymienionych z imienia i nazwiska pracowników organu, z tym zastrzeżeniem, że dane dotyczące pracowników niepełniących funkcji publicznych i nie mających związku z pełnieniem tych funkcji, podlegają ochronie na podstawie art. 5 ust. 2 DostInfPubU, który wymaga zgody tych pracowników na udostępnienie informacji o wysokości jego wynagrodzenia [wyr. WSA w Białymstoku z 13.2.2018 r. (II SA/Bk 647/17, Legalis)].

ORZECZENIE

Podobnie WSA w Warszawie: „Należy zatem wyodrębnić dwie grupy pracowników, których sytuacja prawna w zakresie prawa do ochrony informacji o ich wynagrodzeniach jest różna. Pierwsza grupa to pracownicy, którzy pełnią funkcję publiczną i w stosunku do których wyłączona jest w tym zakresie ochrona ich prywatności, jeżeli żądana informacja pozostaje w związku z pełnioną funkcją, o czym stanowi art. 5 ust. 2 DostInfPubU. Drugą grupę stanowią natomiast pracownicy, którzy nie pełnią funkcji publicznej i wobec których możliwe jest zastosowanie przepisów chroniących ich prawo do prywatności [wyr. WSA w Warszawie z 10.10.2017 r. (II SA/Wa 369/17, Legalis)].

Poinformowanie o prawie do wniesienia skargi do organu nadzorczego (art. 13 ust. 2 lit. d) RODO)

W sytuacji zaistnienia poważnych wątpliwości, co do jawności informacji odnoszących się do osoby pełniącej funkcje publiczną, prawo do złożenia skargi do organu nadzoru może okazać się dość opiniotwórcze. Może to doprowadzić do ukształtowania się UODO [Urząd Ochrony Danych Osobowych] jako źródła ważnej opinii na temat granic jawności życia publicznego w kontekście granic jawności informacji o osobach pełniących funkcje publiczne. Opinie te brane są pod uwagę przez sądy administracyjne, podmioty obowiązane do stosowania DostInfPubU oraz przedstawicieli doktryny.

▶ Podstawa prawna

- art. 6 ust. 1 lit. a), lit. c), art. 13 ust. 2 lit. d), art. 17 ust. 1–3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1)
- art. 1 ust. 2, art. 4 ust. 1 i 2, art. 5 ust. 1 i 2, art. 6 ust. 1 pkt 3 lit. g), ust. 2, art. 10 ust. 1 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.)
- art. 61 ustawy z 2.4.1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. Nr 78, poz. 483 ze zm.)
- art. 115 § 19 ustawy z 6.6.1997 r. – Kodeks karny (t.j. Dz.U. z 2018 r. poz. 1600 ze zm.)

[39] W gminach, powiatach i województwach samorządowych oświadczenie majątkowe przechowuje się przez 6 lat – art. 24h ust. 6 ustawy z 8.3.1990 r. o samorządzie gminnym (t.j. Dz.U. z 2018 r. poz. 994 ze zm.).

Organizacje społeczne jako podmiot zobowiązany do udostępnienia informacji publicznej

dr Kazimierz Pawlik
Radca prawny, wykładowca akademicki, specjalizuje się w postępowaniu administracyjnym i zagadnieniach dostępu do informacji publicznej

Prywatyzacja zadań publicznych powoduje, że niektóre funkcje historycznie przypisane organom administracji publicznej przekazywane są podmiotom spoza kręgu tej administracji, do których mogą należeć m.in. fundacje i stowarzyszenia. Faktyczne wykonywanie zadania publicznego, z którym najczęściej wiąże się także przekazanie do dyspozycji pewnych składników majątku publicznego powoduje, że także te podmioty stają się zobowiązane do udostępniania informacji publicznej, w tym do rozpatrywania indywidualnych wniosków o udostępnienie takiej informacji.

Ogólne podstawy biernej legitymacji

Obowiązujące regulacje prawne, określając podmioty biernie legitymowane w postępowaniu o udostępnienie informacji publicznej, tj. dysponentów informacji publicznej zobowiązanych do jej udostępnienia, posługują się kryterium ustrojowym oraz kryterium funkcjonalnym. Zgodnie z art. 61 ust. 1 ustawy z 2.4.1997 r. – Konstytucja RP (Dz.U. Nr 78, poz. 483 ze zm.; dalej: Konst) prawo do informacji publicznej obejmuje prawo do uzyskania informacji o działalności organów władzy publicznej, osób pełniących funkcje publiczne, organów samorządu gospodarczego i zawodowego oraz o działalności innych podmiotów w takim zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Powyższy przepis poprzez wskazanie rodzajów informacji publicznej pośrednio wskazuje także podmioty zobowiązane do jej udostępnienia. W przypadku części z nich posługuje się przy tym kryterium ustrojowym (organy władzy publicznej, osoby pełniące funkcje publiczne, organy samorządu zawodowego i gospodarczego), zgodnie z którym sama przynależność do wskazanych grup podmiotów powoduje obowiązek udostępniania informacji. Natomiast w przypadku pozostałych podmiotów stosuje kryterium funkcjonalne, wiążąc obowiązek udostępnienia informacji z faktem wykonywania zadań władzy publicznej i dysponowaniem majątkiem publicznym.

Podobne kryterium zawarte zostało w art. 4 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.; dalej: DostInfPubU), gdzie ustawodawca w przykładowym katalogu podmiotów zobowiązanych wskazał z jednej strony na organy władzy publicznej oraz konkretne podmioty (art. 4 ust. 1 pkt 1–4 oraz art. 4 ust. 2 DostInfPubU), a z drugiej na podmioty reprezentujące inne

osoby lub jednostki organizacyjne, które wykonują zadania publiczne lub dysponują majątkiem publicznym (art. 4 ust. 1 pkt 5 DostInfPubU).

Regulacja szczególna

W związku z wątpliwościami dotyczącymi obowiązku udostępniania informacji publicznej przez organizacje społeczne od 9.11.2015 r. kwestia ta uregulowana została również w ustawie z 24.4.2003 r. o działalności pożytku publicznego i wolontariacie (t.j. Dz.U. z 2018 r. poz. 450 ze zm.; dalej: PożPubWolontU). Zgodnie z dodanym art. 4a PożPubWolontU organizacje pozarządowe, które wykonują zadania publiczne lub dysponują majątkiem publicznym, udostępniają informację publiczną na zasadach i w trybie określonym w PożPubWolontU. Ustawa ta w zakresie udostępniania informacji przez organizacje pozarządowe zawiera w większości powielenia rozwiązań przyjętych w DostInfPubU lub bezpośrednio do niej odsyła. W świetle art. 4b PożPubWolontU udostępnienie następuje w trybie bezwnioskowym, tj. przez publikację w Biuletynie Informacji Publicznej lub na stronie internetowej prowadzonej przez zobowiązaną organizację pozarządową lub na wniosek, który rozpatrywany jest na zasadach określonych w DostInfPubU. Praktyczna różnica polega zatem na tym, że ustawodawca przewidział możliwość publikacji informacji publicznych także na stronie internetowej nie będącej stroną BIP.

W zakresie samej legitymacji biernej do udostępnienia informacji publicznej powtórzono zapisy DostInfPubU poprzez powiązanie tego obowiązku z wykonywaniem zadania publicznego lub dysponowaniem majątkiem publicznym. Wyjaśnienie tych pojęć jest zatem kluczowe dla ustalenia, czy dana organizacja pozarządowa będzie zobowiązana do udostępnienia informacji publicznej. Należy przy tym pamiętać, że przesłanka wykonywania zadania publicznego jest autonomiczna względem przesłanki dysponowania majątkiem publicznym, co oznacza, że stwierdzenie wystąpienia którejkolwiek z tych przesłanek jest wystarczające dla stwierdzenia istnienia legitymacji biernej w zakresie udostępnienia informacji (por. wyr. NSA z 3.6.2015 r., I OSK 1603/14, Legalis).

Wykonywanie zadania publicznego

Zastosowanie w ustawach pojęcia „zadania publicznego" zamiast konstytucyjnego „zadania władzy publicznej" może oznaczać podkreślenie, że zadania publiczne, z którymi powiązany jest obowiązek informacyjny, mogą być wykonywane przez różne podmioty niebędące organami władzy i bez konieczności przekazywania tych zadań (por. wyr. WSA w Warszawie z 4.4.2017 r., II SAB/Wa 553/16, Legalis). Cechą zadań publicznych jest powszechność i użyteczność dla ogółu, a także sprzyjanie osiągnięciu celów określonych w Konstytucji lub ustawie. W przypadkach wątpliwych, przy ocenie obowiązku organizacji pozarządowej udostępnienia informacji publicznej, istotne może okazać się porównanie celów statutowych takiej organizacji z zadaniami realizowanymi zgodnie z ustawami ustrojowymi przez organy administracji publicznej, np. organy samorządu terytorialnego (por. wyr. WSA w Gorzowie Wielkopolskim z 31.8.2016 r., II SAB/Go 47/16, Legalis). W przypadku organizacji pozarządowych posiadających status organizacji pożytku publicznego przyjmuje się ponadto w orzecznictwie, że status ten potwierdza prowadzenie działalności pożytku publicznego, a tym samym wykonywanie zadań publicznych (por. wyr. WSA w Gorzowie Wielkopolskim z 24.11.2016 r., II SAB/Go 71/16, Legalis). Przy przyjęciu słuszności powyższej tezy należałoby zatem stwierdzić, że posiadanie takiego statusu wyłącza konieczność analizowania przedmiotu działalności organizacji, która z tego tytułu zalicza się do kręgu podmiotów, o których mowa w art. 4 ust. 1 pkt 4 DostInfPubU.

Dysponowanie majątkiem publicznym

Drugą przesłanką uzasadniającą ustalenie obowiązków informacyjnych organizacji pozarządowej jest dysponowanie majątkiem publicznym. Pod pojęciem tym należy rozumieć w szczególności korzystanie przez organizację pozarządową z dotacji finansowanych ze środków publicznych (por. wyr. WSA w Warszawie z 10.3.2017 r., II SAB/Wa 603/16, Legalis). Przekazanie takich środków oznacza, że organizacja pozarządowa staje się ich dysponentem, a środki te nie przestają mieć charakteru środków publicznych, co przesądza o szczególnych wymaganiach co do transparentności ich wydatkowania (por. wyr. WSA w Warszawie z 29.9.2016 r., II SAB/Wa 342/16, Legalis). W przypadku organizacji pozarządowych istotną kwestią jest fakt posiadania statusu organizacji pożytku publicznego także z perspektywy oceny zaistnienia przesłanki dysponowania majątkiem publicznym. Ze statusem tym wiąże się bowiem możliwość przekazywania – przez podatników podatku dochodowego od osób fizycznych – na rzecz organizacji, w oparciu o art. 27 PożPubWolontU, 1% podatku obliczonego. Otrzymane przez organizację środki finansowe pochodzące z 1% wskazanego podatku mogą być wykorzystane wyłącznie na prowadzenie działalności pożytku publicznego. Możliwość dysponowania tymi środkami o charakterze podatkowym w orzecznictwie uznawana jest za spełnienie przesłanki dyspo-

nowania majątkiem publicznym (por. wyr. WSA w Warszawie z 13.4.2016 r., II SAB/Wa 987/15, Legalis).

Ważne

Uznaje się, że dysponowanie choćby niewielką częścią mienia publicznego, nawet jeśli zdecydowana większość środków wykorzystywanych przez organizację ma charakter prywatny, jest wystarczające dla ustalenia istnienia obowiązku informacyjnego organizacji pozarządowej.

Zakres udostępnianych informacji

Sposób określenia podmiotów zobowiązanych do udostępnienia informacji publicznej nie ze względu na status, lecz na wykonywanie zadań publicznych lub dysponowanie majątkiem publicznym, może prowadzić do wniosku, że same obowiązki informacyjne m.in. organizacji pozarządowych są ograniczone. Wniosek taki wynika zwłaszcza z treści art. 61 ust. 1 Konst, który wskazuje z jednej strony na prawo dostępu do informacji o działalności (całej) organów władzy publicznej, a z drugiej w przypadku innych podmiotów stwierdza, że prawo do informacji przysługuje wyłącznie w zakresie, w jakim podmioty te wykonują zadania władzy publicznej lub dysponują majątkiem publicznym. Dlatego w orzecznictwie stwierdza się, że z uwagi na alternatywny sposób określenia legitymacji biernej żądanie w tym drugim przypadku informacji innych niż z zakresu wykonywania zadań publicznych lub dysponowania mieniem publicznym stanowiłoby nadmierną ingerencję w sferę informacyjną tych podmiotów, która wykraczałaby poza standard konstytucyjny (por. wyr. WSA w Gliwicach z 20.6.2017 r., IV SAB/Gl 115/17, Legalis). Organizacje pozarządowe są natomiast niewątpliwie zobowiązane do udostępnienia informacji o takiej własnej aktywności, która ukierunkowana jest na wypełnienie określonych zadań publicznych i realizowanie określonych interesów i celów publicznych (por. wyr. NSA z 29.6.2018 r., I OSK 2019/16, Legalis).

Legitymacja procesowa

Z legitymacją bierną w sprawie udostępnienia informacji publicznej wiąże się problem zdolności procesowej organizacji pozarządowych w postępowaniu przed sądami administracyjnymi. Można przyjąć, że skoro w świetle art. 4 ust. 1 pkt 5 DostInfPubU zobowiązany do udzielenia informacji publicznej jest każdy podmiot wykonujący wskazane funkcje, to w konsekwencji taki podmiot może być stroną postępowania sądowoadministracyjnego (por. wyr. NSA z 26.2.2014 r., I OSK 2135/13, Legalis). W szczególności podmiotowi zobowiązanemu do udostępnienia informacji publicznej nie można odmówić zdolności sądowej w postępowaniu wszczętym przeciwko niemu na skutek skargi o bezczynność w udostępnieniu informacji.

W takim przypadku podstawą prawną zdolności sądowej podmiotu zobowiązanego do udostępnienia informacji nie jest jednak art. 25 ustawy z 30.8.2002 r. o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2018 r. poz. 1302; dalej: PostAdmU), lecz art. 32 PostAdmU (por. wyr. NSA z 18.11.2016 r., I OSK 1941/16, Legalis). Wynika to z przyjęcia funkcjonalnej definicji organu, którym będzie również podmiot, przeciwko którego bezczynności w udostępnieniu informacji publicznej sformułowana jest skarga. W postępowaniu ze skargi na bezczynność takiego organu, sąd administracyjny w pierwszej kolejności zobowiązany jest do ustalenia, czy skarżony podmiot jest z perspektywy ustaw zobowiązany do załatwiania wniosków o informację publiczną, a dopiero w przypadku odpowiedzi twierdzącej do badania, czy faktycznie doszło do bezczynności w udostępnieniu informacji (por. wyr. WSA w Kielcach z 18.5.2017, II SAB/Ke 25/17, Legalis).

▶ Podstawa prawna

- art. 4 ust. 1, art. 4 ust. 2 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.)
- art. 4a, art. 4b, art. 27 ustawy z 24.4.2003 r. o działalności pożytku publicznego i wolontariacie (t.j. Dz.U. z 2018 r. poz. 450 ze zm.)
- art. 25, art. 32 ustawy z 30.8.2002 o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2018 r. poz. 1302)

Podsumowanie

Organizacje społeczne, które wykonują zadania publiczne lub dysponują majątkiem publicznym, należy uznać za podmioty zobowiązane do udostępnienia informacji publicznej. Dla istnienia tego obowiązku nie ma znaczenia podstawa wykonywania zadania publicznego (np. istnienie formalnego zlecenia wykonania) czy wielkość majątku publicznego, którym organizacja dysponuje. Natomiast obowiązek informacyjny nie dotyczy całej działalności takiej organizacji, ale sposobu wykonywania zadań publicznych lub zasad gospodarowania majątkiem publicznym.

Udostępnianie zanonimizowanych decyzji administracyjnych. Orzecznictwo i praktyka

Bartosz Wilk
Prawnik, wiceprezes stowarzyszenia Sieć Obywatelska Watchdog Polska

Realizacja wniosku o udostępnienie decyzji administracyjnych może wiązać się z koniecznością dokonania tzw. anonimizacji, czyli usunięcia danych pozwalających na zidentyfikowanie osób i podmiotów, które korzystają z ochrony prawnej. W związku z tym mogą pojawiać się wątpliwości, co do konieczności wydania decyzji o odmowie udostępnienia informacji publicznej oraz oceny wniosku pod kątem zakwalifikowania jej jako „informacji przetworzonej".

Decyzja administracyjna jako informacja publiczna

W ustawie z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.; dalej: DostInfPubU) znajduje się definicja informacji, które należy kwalifikować jako informacje publiczne, jak też otwarty (przykładowy) katalog informacji publicznych, które podlegają udostępnieniu. Zgodnie z art. 6 ust. 1 pkt 4 lit. a) DostInfPubU, udostępnieniu podlega informacja publiczna, w szczególności o danych publicznych, w tym treść i postać dokumentów urzędowych, zwłaszcza zaś – treść aktów administracyjnych i innych rozstrzygnięć. Aktami administracyjnymi są decyzje administracyjne, wydawane przez uprawnione do tego organy. Decyzje administracyjne stanowią także dokument urzędowy, którym jest – zgodnie z art. 6 ust. 2 DostInfPubU – treść oświadczenia woli lub wiedzy, utrwalona i podpisana w dowolnej formie przez funkcjonariusza publicznego w rozumieniu przepisów ustawy z 6.6.1997 r. – Kodeks karny (t.j. Dz.U. z 2018 r. poz. 1600 ze zm.), w ramach jego kompetencji, skierowana do innego podmiotu lub złożona do akt sprawy.

Definicja dokumentu urzędowego na gruncie DostInfPubU ma istotne znaczenie z punktu widzenia uprawnienia, określonego w art. 3 ust. 1 pkt 2 DostInfPubU. W przepisie tym określa się, że prawo do informacji publicznej zawiera uprawnienie do wglądu do dokumentów urzędowych. Zestawiając to z uprawnieniem do uzyskania informacji publicznej (art. 3 ust. 1 pkt 1 DostInfPubU), należy wskazać, że w przypadku decyzji administracyjnych może dojść do skorzystania z jednego z dwóch uprawnień:

1) wglądu do decyzji administracyjnej,
2) zawnioskowania o udostępnienie informacji publicznej, jaką jest decyzja administracyjna.

Do osoby korzystającej z prawa do informacji należy wybór jednej z form,

lub skorzystanie z obydwu. Niniejszy tekst dotyczy udostępnienia decyzji administracyjnych na wniosek.

Udostępnienie decyzji administracyjnych na wniosek

Problem z udostępnieniem decyzji administracyjnych może dotyczyć sytuacji, gdy – w ocenie adresata wniosku – udostępnienie decyzji administracyjnych naruszałoby dobra prawnie chronione, takie jak prywatność osób fizycznych lub tajemnica przedsiębiorcy.

PRZYKŁAD

Wniosek o udostępnienie informacji publicznej w postaci decyzji administracyjnej, która jest skierowana do osoby fizycznej, która nie pełni funkcji publicznej lub też funkcję tę pełni, ale decyzja nie ma związku z ich pełnieniem.

ORZECZENIE

W wyroku WSA w Opolu z 4.7.2018 r. (II SAB/Op 58/18, Legalis) wskazano, że: „Decyzja administracyjna wydana w indywidualnej sprawie (stanowiąca jeden z dokumentów włączonych do akt sprawy), co do zasady, podlega udostępnieniu na wniosek osoby niebędącej stroną postępowania administracyjnego złożony w trybie art. 10 DostInfPubU, gdyż jej treść należy do zakresu danych zaliczanych do zbioru informacji o sprawach publicznych. Nie oznacza to jednak, że wnioskujący o udostępnienie informacji publicznej musi automatycznie uzyskać informację o pełnej treści decyzji. Jeżeli postępowanie administracyjne pozostaje jawne tylko dla stron, organ uprawniony był do podjęcia czynności zmierzających do usunięcia z decyzji treści zawierających informacje pozwalające na zidentyfikowanie strony postępowania oraz konkretnej sprawy podlegającej rozpatrzeniu". Pojawić się mogą wówczas problemy związane z ograniczaniem dostępności informacji zawartych w decyzji administracyjnej. W praktyce następuje to wskutek dokonania tzw. anonimizacji, która polega na usunięciu (np. poprzez zamazanie lub zasłonięcie) tych informacji, które pozwalają na zidentyfikowanie osób fizycznych lub przedsiębiorców. Przedmiotem ochrony mogą być dobra prawnie chronione nie tylko adresata decyzji, ale także innych osób/podmiotów, których dane są zamieszczone w decyzji administracyjnej.

PRZYKŁAD

Może to być zakreślenie imienia i nazwiska adresata decyzji. Nie można jednak wykluczyć sytuacji, gdy – z uwagi na specyficzny stan faktyczny – zasadne będzie także wyłączenie innych informacji, pozwalających zidentyfikować konkretne osoby.

Warto w tej mierze wskazać, że do tego zagadnienia odnosi się motyw 26 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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) (DzUrz. UE L Nr 119, s. 1; dalej: RODO). Odróżnia on anonimizację od pseudonomizacji. Ta ostatnia polega na zastąpieniu danych osobowych innymi identyfikatorami lub określeniami w taki sposób, aby bez zestawiania z innymi danymi, nie było możliwe zidentyfikowanie osoby, której dane dotyczą. Anonimizacja z kolei polega na wykluczeniu w ogóle danych, pozwalających na zidentyfikowanie określonej osoby, zatem jest to czynność nieodwracalna (w odróżnieniu od pseudonomizacji). Zgodnie z motywem 26 RODO, zasady ochrony danych nie powinny więc mieć zastosowania do informacji zanonimowanych, gdyż te nie wiążą się z przetwarzaniem danych poszczególnych osób.

Dokonanie anonimizacji jest związane z zastosowaniem zasady proporcjonalności ograniczania konstytucyjnych wolności i praw (wynikającej z art. 61 ust. 3 w zw. z art. 31 ust. 3 Konstytucji RP), wśród których jest prawo do informacji. Zamiast całkowicie ograniczać dostępność informacji zawierających informacje podlegające ochronie, ogranicza się tylko dostępność konkretnych informacji, w minimalnym koniecznym zakresie.

Anonimizacja a wydanie decyzji o odmowie udostępnienia informacji publicznej

Praktyczny problem prawny sprowadza się do odpowiedzi na pytanie, czy w przypadku dokonania anonimizacji należy wydać decyzję o odmowie udostępnienia informacji publicznej. Problem ten nie istnieje wówczas, gdy wnioskodawca przedmiotem złożonego wniosku o udostępnienie informacji publicznej nie uczynił informacji poddanych anonimizacji, czyli gdy wprost wskazał, że nie zależy mu na uzyskaniu tych danych.

PRZYKŁAD

Wnioskodawca we wniosku zwraca się o „zasłonięcie wyłącznie danych dotyczących podatników, jak: dane osobowe, nazwa pod jaką prowadzona jest działalność gospodarcza, adres zamieszkania lub siedziby, PESEL, NIP" (przykład z wyr. WSA w Warszawie z 6.6.2014 r., II SA/Wa 437/14).

W tym przypadku wnioskodawca nie czyni przedmiotem wniosku informacji poddanych anonimizacji. Można więc przyjąć, że w tym zakresie nie dochodzi do potrzeby udostępnienia informacji publicznej. Nie jest też konieczne wydanie decyzji o odmowie jej udostępnienia.

Niemniej jednak w przypadku bardziej ogólnie sformułowanego wniosku, to do oceny organu należy ocena zakresu koniecznych wyłączeń informacji i dokonanej w tym zakresie anonimizacji. Kolejnym wyzwaniem jest ustalenie, czy w sprawie zachodzi potrzeba wydania decyzji o odmowie udostępnienia informacji publicznej. W tej mierze orzecznictwo wypracowało dwa stanowiska.

Stanowisko pierwsze – każda anonimizacja wymaga wydania decyzji administracyjnej o odmowie udostępnienia informacji publicznej

Wskutek anonomizacji dochodzi do ograniczenia dostępności części informacji. W świetle art. 16 ust. 1 DostInfPubU takie ograniczenie przybierze formę decyzji administracyjnej. Pierwsze z podejść opiera się na przyjęciu, że ograniczenie prawa do informacji polega nie tylko na odmowie przekazania informacji w jakimkolwiek zakresie, ale także na ograniczeniu udostępnienia jakiejś części informacji, która jest przedmiotem wniosku (dane podlegające anonimizacji).

ORZECZENIE

W wyroku WSA w Gorzowie Wielkopolskim z 24.1.2018 r. (II SAB/Go 126/17, Legalis), Sąd przyjął, że organ „wprawdzie udzielił wnioskowanej informacji, jednak w sposób nie w pełni realizujący oczekiwania skarżącego wynikające z jego wniosku (...), albowiem pomijając dane osobowe osób fizycznych – stron umów. Oznacza to, że organ nie rozpatrzył wniosku w całości, zgodnie z zawartym w nim żądaniem. Udzielenie informacji niepełnej, czy też niezgodnej z treścią żądania, należy oceniać jako bezczynność adresata wniosku o udostępnienie informacji publicznej". Z tego powodu sąd uznał, że w sytuacji, gdy „organ uważał, że żądane informacje podlegają ochronie na podstawie art. 5 DostInfPubU, to wówczas winien wydać na podstawie art. 16 ust. 1 DostInfPubU decyzję o odmowie udostępnienia informacji w tym zakresie. Nieudostępnienie pełnej treści żądanej informacji przy jednoczesnym niewydaniu decyzji odmownej stanowi o bezczynności organu".

ORZECZENIE

W wyroku WSA w Łodzi z 10.7.2015 r. (II SAB/Łd 69/15) wskazano, że: „Odmowa udostępnienia informacji z powodów określonych w art. 5 ust. 2 DostInfPubU powinna przybrać formę decyzji wydanej na podstawie art. 16 DostInfPubU, a nie dokonania anonimizacji dokumentów. W sprawie niezbędne było wydanie decyzji także z tego powodu, by strona mogła polemizować ze stanowiskiem organu wnosząc odwołanie, a następnie skargę do sądu administracyjnego (...). Konkludując powyższe uwagi dostrzec wypada, że ponownie rozpoznając sprawę organ, uznając, że w sprawie prawo do informacji publicznej podlega ograniczeniu stosownie do art. 5 ust. 2 DostInfPubU, będzie zobowiązany do wydania stosownej decyzji zgodnie z art. 16 DostInfPubU. Niewątpliwie organ w sprawie nie wydał takowej decyzji, co świadczy o tym, że powołując się na okoliczności art. 5 ust. 2 DostInfPubU pozostaje w bezczynności".

Gdy w sprawie nie wydano decyzji o odmowie udostępnienia informacji publicznej, to wnioskodawca może skorzystać ze skargi na bezczynność, w której powoła się na to, że nie została w całości udostępniona interesująca go informacja publiczna (zob. wyr. NSA z 2.6.2015 r., I OSK 1513/14, Legalis).

Omawiane podejście opiera się na przyjęciu, że anonimizacja ma nie tylko faktyczny wymiar (np. zamazanie określonych informacji), ale także prawny (związany z ograniczeniem prawa do informacji w formie decyzji). Takie rozwiązanie może być korzystne dla wnioskodawcy. Z jednej strony, otrzymanie decyzji administracyjnej pozwoli mu zrozumieć dokonane przez adresata wniosku wyłączenie części informacji, zarówno co do zakresu, jak i co do podstaw takiego rozstrzygnięcia. Z drugiej strony, jeżeli przedstawione argumenty nie przekonają wnioskodawcy, będzie on mógł zakwestionować dokonaną anonimizację poprzez skorzystanie ze ścieżki odwoławczej w toku postępowania administracyjnego oraz sądowoadministracyjnego. Przedmiotem sporu wówczas może być dokonanie anonimizacji, co do zasady, w danej sprawie, jak i co do dokonanego zakresu ograniczenia prawa do informacji.

W razie przyjęcia i zastosowania omawianego podejścia, wraz z przekazaniem zanonimizowanej decyzji administracyjnej (będącej przedmiotem wniosku o udostępnienie informacji publicznej) wnioskodawca otrzyma decyzję o odmowie udostępnienia informacji publicznej w zakresie zanonimizowanych fragmentów. Z uwagi na to, że do wnioskodawcy należy określenie sposobu i formy przekazania informacji, będącej przedmiotem wniosku, udostępnienie informacji oraz doręczenie decyzji administracyjnej może nastąpić w różnych formach.

PRZYKŁAD

Wnioskodawca wskazał we wniosku, że zanonimizowana decyzja administracyjna powinna być udostępniona w formie skanu, wysłanego na adres e-mail. Jeżeli wnioskodawca nie zawnioskował o doręczenie decyzji w formie elektronicznej (stosownie do art. 39[1] ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego; t.j. Dz.U. z 2017 r. poz. 1257 ze zm.; dalej: KPA), decyzja powinna być udostępniona w formie tradycyjnej papierowej na podstawie art. 39 KPA, natomiast zanonimizowana decyzja administracyjna – poprzez wysłanie za pośrednictwem poczty e-mail.

Wydanie decyzji administracyjnej o odmowie udostępnienia informacji publicznej jest możliwe tylko wówczas, gdy adresat wniosku posiada informacje niezbędne do wydania tejże decyzji (dane wnioskodawcy, takie jak imię i nazwisko, lub nazwa, oraz adres). W świetle ostatniego stanowiska sądów administracyjnych, w razie zaistnienia potrzeby wydania decyzji administracyjnej, adresat wniosku powinien także wezwać wnioskodawcę do podpisania wniosku (zob. *B. Wilk*, Kiedy wezwać do podpisania wniosku o udostępnienie informacji publicznej?, Informacja w Administracji Publicznej 2018, Nr 3, s. 55–58).

Gdy wnioskodawca nie poda swoich danych (np. złożył wniosek anonimowy), to wówczas adresat wniosku powinien zwrócić się do adresata o podanie danych niezbędnych do wydania decyzji oraz wezwać do podpisania wniosku (poprzez złożenie pod-

pisu elektronicznego lub tradycyjnego. W tym zakresie dobrą praktyką byłoby poinformowanie, że w razie braku spełnienia wezwania, niemożliwe będzie wydanie decyzji administracyjnej. Z drugiej strony, w tej sprawie nie powinno budzić wątpliwości, że dopuszczalne jest udostępnienie zanonimizowanej decyzji administracyjnej, której udostępnienie jest przedmiotem wniosku, bez wydawania w tym zakresie decyzji administracyjnej o odmowie udostępnienia informacji publicznej.

Drugie stanowisko – nie należy utożsamiać anonimizacji z odmową udostępnienia informacji publicznej

Wyrazem tego podejścia jest wielokrotnie przytaczany w orzecznictwie sądowoadministracyjnym wyrok NSA z 11.1.2013 r. (I OSK 2267/12, Legalis).

ORZECZENIE

„Z zestawienia tych dwóch wartości, tj. zasady jawności informacji publicznych oraz obowiązku ochrony prywatności, tajemnic przedsiębiorcy i danych osobowych osób fizycznych, można wyprowadzić wniosek, że możliwe jest udostępnianie informacji publicznej w sposób nienaruszający wskazanych dóbr chronionych. Służy temu m.in. zastosowana przez organ w rozpatrywanej sprawie tzw. anonimizacja danych wrażliwych. W takim wypadku nie zachodzi jednak potrzeba wydawania oddzielnej decyzji na podstawie art. 16 DostInfPubU, gdyż przepis ten może mieć zastosowanie tylko w wypadku odmowy udostępnienia informacji, a nie w przypadku jej udzielenia z zachowaniem zasady ochrony dóbr chronionych".

W wyroku tym wskazuje się także, że „ocenie Sądu rozpatrującego skargę na bezczynność organu w zakresie udostępnienia informacji publicznej, podlegać będzie sposób i zakres dokonanej przez organ anonimizacji, a w szczególności to, czy nie niweczy on pożądanego przez stronę rezultatu w postaci uzyskania informacji o konkretnie wskazanych sprawach publicznych" oraz że „wydanie decyzji odmownej na podstawie przepisu art. 16 DostInfPubU byłoby konieczne tylko w przypadku, gdyby istota żądanej informacji dotyczyła żądania ujawnienia chronionych prawem danych wskazanych osób lub danych wrażliwych innych podmiotów. Naczelny Sąd Administracyjny nie podziela poglądu, że w każdym wypadku, kiedy zachodzi możliwość ujawnienia «przy okazji» udostępniania informacji publicznej danych podlegających ochronie na podstawie przepisów ustawy o ochronie danych osobowych, należy całkowicie odmówić udzielenia informacji na podstawie przepisu art. 16 DostInfPubU, zwłaszcza, gdy strona nie jest sama zainteresowana ujawnieniem takich danych, żądając udzielenia informacji o konkretnych sprawach publicznych".

W wyroku NSA z 12.10.2017 r. (I OSK 537/17, Legalis), wskazano m.in., że anonimizacja może obejmować informacje, które „nie są objęte uzewnętrznionym we wniosku zainteresowaniem wnioskodawcy, które odnosi się do fragmentów irrelewantnych z punktu widzenia ochrony danych osobowych)". Wskazuje się przy tym, że: „Ocenę tę należy przeprowadzać przez pryzmat złożonego w sprawie wniosku i wskazanego w nim wyraźnie zakresu żądanych informacji" (por. wyr. NSA z 12.4.2017 r., I OSK 1928/15, Legalis).

Takie podejście znajduje też wyraz w orzecznictwie wojewódzkich sądów administracyjnych, w tym np. w wyroku WSA w Opolu z 16.1.2018 r. (II SA/Op 608/17, Legalis). Wskazano w nim, że: „Żaden też z przepisów ustawy nie nakazuje wydania decyzji o odmowie udostępnienia informacji publicznej w związku z dokonaniem anonimizacji udostępnianej informacji publicznej, natomiast udostępnienie zanonimizowanego dokumentu w związku ze złożonym wnioskiem nie oznacza pozostawania przez podmiot zobowiązany w bezczynności. Przewidziane w art. 5 ust. 2 DostInfPubU ograniczenie prawa do informacji publicznej nie oznacza bezwzględnego zakazu udostępnienia informacji zawierających tzw. dane wrażliwe. Nawet w sytuacji, gdy dokumenty zawierają takie właśnie dane, mogą one zostać udostępnione w kserokopii, z której usuwa się takie elementy".

W omawianym podejściu akceptuje się potrzebę wydania w sprawie decyzji o odmowie udostępnienia informacji publicznej wówczas, gdy organ odmawia udostępnienia całej informacji, objętej przedmiotem wniosku o udostępnienie informacji publicznej. W orzecznictwie wskazuje się bowiem, że w razie uznania, iż istnieje potrzeba ochrony prywatności określonej osoby lub osób, a celu tego w dostateczny sposób nie spełni anonimizacja danych wrażliwych osób uczestniczących w postępowaniu, to wówczas organ, do którego skierowano wniosek o udostępnienie informacji publicznej, powinien – na podstawie art. 16 DostInfPubU – wydać decyzję administracyjną odmawiającą udostępnienia informacji publicznej, powodując się na ograniczenia zawarte w art. 5 ust. 1 i 2 DostInfPubU (wyr. WSA w Białymstoku z 14.2.2013 r., II SA/Bk 967/12, Legalis; wyr. WSA w Łodzi z 6.8.2014 r., II SA/Łd 537/14, Legalis).

Ponadto, zgodnie z przedstawionymi w tym podejściu stanowiskami sądów administracyjnych, decyzję o odmowie udostępnienia informacji publicznej należy wydać wówczas, gdy wskutek dokonanej anonimizacji nie zostaną przekazane informacje, o których przekazanie wnioskodawca zwrócił się wprost we wniosku. Przedmiotem oceny sądów administracyjnych jest wówczas to, czy dokonana anonimizacja nie niweczy w istocie realizacji samego wniosku. Przykładem oceny przez sąd zakresu dokonanej anonimizacji w kontekście celu spełnienia funkcji informacyjnej może być przytoczony już wyrok WSA w Opolu

z 4.7.2018 r. (II SAB/Op 58/18, Legalis), w którym wskazano, że: „Udostępniony skarżącemu odpis pozwala na zapoznanie się z treścią decyzji, istotnymi elementami rozstrzygnięcia oraz podstawami faktycznymi i prawnymi jej wydania, a to oznacza zrealizowanie celu ustawy, którym jest zgodnie z art. 1 ust. 1 DostInfPubU informacja o sprawach publicznych, udostępniana w trybie ustawy, z ewentualnymi ograniczeniami (tu wynikającymi z art. 5 ust. 2 DostInfPubU)".

Drugie z omawianych podejść, polegające na uznaniu, że nie zawsze anonimizacja wiąże się z zaktualizowaniem obowiązku wydania decyzji o odmowie udostępnienia informacji publicznej, na pierwszy rzut oka może okazać się korzystne, gdyż zwalnia z wydania decyzji administracyjnej przy każdej anonimizacji. Niemniej jednak nie ogranicza ryzyka powstania sporu sądowoadministracyjnego, gdyż w razie uznania przez wnioskodawcę, że udostępniona decyzja administracyjna została poddana nieprawidłowej (zwłaszcza – zbyt daleko idącej) anonimizacji, będzie on mógł skierować skargę na bezczynność organu.

W praktyce określenie tego, co jest przedmiotem zainteresowania wnioskodawcy, może rodzić problemy. W razie sporu co do zakresu anonimizacji może spowodować to przedłużenie sporu sądowego. Wynika to z faktu, że wnioskodawca najpierw będzie kwestionował bezczynność organu (który nie wydał decyzjo i o odmowie udostępnienia informacji) i w razie udanego zaskarżenia – będzie zaskarżał wydaną decyzję o odmowie udostępnienia informacji publicznej (odmawiającą udostępnienia informacji objętych anonimizacją). Może to więc być rozwiązanie mniej korzystne z punktu widzenia wnioskodawcy.

Ponadto DostInfPubU nie przewiduje trybu zwrócenia się do wnioskodawcy o zajęcie stanowiska w przedmiocie potencjalnej anonimizacji i jej zakresu. Z tego też powodu, brak reakcji ze strony wnioskodawcy nie uprawnia adresata wniosku do niepodejmowania jakiegokolwiek działania. Wówczas wedle własnej oceny powinien przyjąć, czy udostępnia informację, czy też odmówi jej udostępnienia (lub jej części) w drodze decyzji administracyjnej.

Anonimizacja a przetworzenie informacji

Innym zagadnieniem, związanym z udostępnianiem zanonimizowanych decyzji administracyjnych, jest ocena wniosku dotyczącego tego typu informacji pod kątem tego, czy nie dotyczy on „informacji przetworzonej" w rozumieniu art. 3 ust. 1 pkt 1 DostInfPubU. Wówczas udostępnienie tej informacji uzależnione jest od spełnienia przesłanki „szczególnej istotności dla interesu publicznego". W orzecznictwie sądów administracyjnych przyjmuje się, że konieczność dokonania anonimizacji żądanych we wniosku informacji sama w sobie nie prowadzi do uznania, że wniosek dotyczy „informacji przetworzonej".

ORZECZENIE

W wyroku NSA z 30.9.2015 r. (I OSK 1746/14, Legalis) wskazano, że: „Informacja prosta poprzez sam proces anonimizacji, czyli czynność polegającą jedynie na przekształceniu, a nie przetworzeniu informacji nie zmienia się w informację przetworzoną. O przetworzeniu informacji nie stanowi też sięganie do materiałów archiwalnych. Informacja przetworzona w chwili złożenia wniosku w zasadzie nie istnieje. Jej wytworzenie wymaga przeprowadzenia przez podmiot zobowiązany pewnych czynności analitycznych, organizacyjnych i intelektualnych w oparciu o posiadane informacje proste".

Niemniej jednak w orzecznictwie można znaleźć przykłady sporów sądowych, związanych z uznaniem za „informację przetworzoną" zanonimizowanych dokumentów. W orzecznictwie bowiem wypracowano dwa podejścia związane z uznawaniem określonych informacji za „przetworzone", które określić można jako „jakościowe" i „ilościowe". Pierwsze z nich opiera się na stwierdzeniu, że informacją przetworzoną jest informacja nieistniejąca na dzień złożenia wniosku, która jednak może być przygotowana specjalnie dla wnioskodawcy w oparciu o inne informacje posiadane przez adresata wniosku, w wyniku podjęcia działań intelektualnych i wytworzenia nowej jakościowo informacji. Wskazuje się przy tym, że anonimizacja sama w sobie nie prowadzi do wytworzenia nowej jakościowo informacji.

Drugie z nich, ilościowe, opiera się na przyjęciu, że choć wniosek dotyczy w istocie „informacji prostej", to o zastosowaniu instytucji z art. 3 ust. 1 pkt 1 DostInfPubU może świadczyć szeroki zakres wniosku, wymagający zgromadzenia, zanonimizowania i sporządzenia wielu kserokopii określonych dokumentów, co może wymagać takich działań organizacyjnych i angażowania środków osobowych, które zakłócają normalny tok działania podmiotu zobowiązanego i utrudniają wykonywanie przypisanych mu zadań (np. wyr. NSA z 23.1.2015 r., I OSK 315/14, Legalis). Choć takie podejście w sposób istotny i niedookreślony ogranicza prawo wnioskodawców do uzyskania informacji, to znajduje ono szeroką reprezentację w orzecznictwie. Sądy oceniają wówczas wydane decyzje o odmowie udostępnienia informacji publicznej pod kątem tego, czy podane w uzasadnieniu decyzji argumenty i fakty uzasadniają przyjęcie, że w danej sprawie suma informacji prostych prowadzi do zakwalifikowania żądanej informacji jako „przetworzonej".

▶ Podstawa prawna

- art. 3 ust. 1 pkt 1, pkt 2, art. 5, art. 6 ust. 1 pkt 4 lit. a), ust. 2, art. 10, art. 16 ust. 1 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.)

Wzór zawiadomienia o podejrzeniu popełnienia przestępstwa nieudostępnienia informacji publicznej

Nieudostępnienie informacji publicznej jest penalizowane w art. 23 ustawy z 6.9.2001 r. o dostępie do informacji publicznej. Jest to przestępstwo ścigane z urzędu. Poniżej znajdą Państwo wzór zawiadomienia o podejrzeniu popełnienia przedmiotowego przestępstwa ze względu na nierozpoznanie terminowe wniosku o udostępnienie informacji publicznej.

Barbara Pietrzak-Kudelska
Radca prawny, pracownik samorządowy

Sprawca przestępstwa

Sprawcą przestępstwa z art. 23 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.; dalej: DostInfPubU) może być każdy, na kim ciąży obowiązek udostępnienia informacji publicznej. Może to być osoba kierująca podmiotem zobowiązanym wymienionym w art. 4 ust. 1 i 2 DostInfPubU, czyli np. wójt, burmistrz, prezydent miasta, wojewoda, minister, kierownik samorządowej lub państwowej jednostki organizacyjnej. Będą to również pracownicy podmiotów zobowiązanych, których obszar obowiązków obejmuje udostępnianie informacji publicznej. Zakres obowiązków może wynikać m.in. z umowy o pracę, regulaminu pracy, wewnętrznego regulaminu organizacyjnego czy też opisu stanowiska. Wskazany przepis dotyczy również osób zatrudnianych na podstawie umów cywilnoprawnych, jeżeli przedmiot umowy lub zakres wykonywanych czynności związany jest z udostępnianiem informacji.

Omawiane przestępstwo można popełnić jedynie umyślnie, z zamiarem zarówno bezpośrednim, jak i ewentualnym. Zamiar bezpośredni polega na tym, że sprawca chce popełnić czyn zabroniony. Natomiast zamiar ewentualny charakteryzuje się tym, że sprawca nie chce popełnienia czynu zabronionego, ale przewidując możliwość jego popełnienia, godzi się na to, czyli akceptuje mogący nastąpić stan rzeczy.

Kary za nieudostępnienie informacji publicznej

Przestępstwo nieudostępnienia informacji publicznej stanowi występek i jest zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności do roku. Grzywnę wymierza się w stawkach

dziennych, określając liczbę stawek oraz wysokość jednej stawki, przy czym najniższa liczba stawek wynosi 10, natomiast najwyższa 540. Stawka dzienna nie może być niższa od 10 zł ani też przekraczać 2000 zł. Ustalając stawkę dzienną sąd bierze pod uwagę dochody sprawcy, jego warunki osobiste, rodzinne, stosunki majątkowe i możliwości zarobkowe. Kara ograniczenia wolności trwa najkrócej miesiąc, najdłużej 2 lata. Kara ograniczenia wolności polega na: obowiązku wykonywania nieodpłatnej, kontrolowanej pracy na cele społeczne albo na potrąceniu od 10% do 25% wynagrodzenia za pracę w stosunku miesięcznym na cel społeczny wskazany przez sąd. Nieodpłatna, kontrolowana praca na cele społeczne jest wykonywana w wymiarze od 20 do 40 godzin w stosunku miesięcznym.

Wzór

.....
(*miejscowość, data*)

Zawiadamiający:

Jan Kowalski
.....
.....
(*adres*)

Prokuratura Rejonowa …**[1]**
.....
(*adres*)

ZAWIADOMIENIE
o podejrzeniu popełnieniu przestępstwa [2]

Na podstawie art. 304 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2018 r. poz. 1987 ze zm.) składam zawiadomienie **[3]** o podejrzeniu popełnienia przestępstwa nieudostępnienia informacji publicznej, tj. o czyn z art. 23 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.).

UZASADNIENIE

W dniu 24.5.2017 r. na adres poczty elektronicznej Urzędu Gminy …… złożyłem wniosek o udostępnienie informacji publicznej – umów i faktur związanych z realizacją inwestycji „Budowa drogi gminnej – ul. Jasnej na odcinku od ul. Kolorowej do ul. Ciemnej".

Dowód: wniosek o udostępnienie informacji publicznej

W dniu 20.6.2017 r. doręczono mi decyzję odmawiającą udostępnienia informacji publicznej. Przedmiotowa decyzja została przeze mnie zaskarżona do Samorządowego Kolegium Odwoławczego w … Samorządowe Kolegium Odwoławcze decyzją z 12.1.2018 r. uchyliło zaskarżoną decyzję i przekazało sprawę do ponownego rozpoznania wójtowi. Z treści uzasadnienia decyzji SKO wynika, że żądana przez mnie informacja stanowi informację publiczną oraz że nie zachodzą ustawowe przesłanki ograniczające prawo dostępu do informacji publicznej.

Dowód: decyzja SKO

Pomimo rozstrzygnięcia wydanego przez SKO do dzisiaj nie otrzymałem żądanej informacji, Wójt Gminy … nie wydał także kolejnej decyzji w przedmiocie mojego wniosku.

Zgodnie z art. 23 ustawy o dostępie do informacji publicznej „kto, wbrew ciążącemu na nim obowiązkowi, nie udostępnia informacji publicznej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia

wolności do roku". W przypadkach udostępniania informacji publicznej na wniosek, czynem zabronionym opisanym w tym przepisie może być m.in.: nierozpoznanie wniosku pomimo upływu terminów przewidzianych w ustawie, wydanie niezgodnej z prawem decyzji odmawiającej udostępnienia informacji, niezgodne z prawdą poinformowanie wnioskodawcy, że podmiot zobowiązany nie posiada żądanych informacji bądź, że nie stanowią one informacji publicznej.

W niniejszej sprawie doszło zarówno do wydania decyzji niezgodnej z prawem, o czym świadczy jej uchylenie przez organ II instancji, jak również do nierozpoznania wniosku w terminie.

Biorąc powyższe pod uwagę uzasadnione jest podejrzenie popełnienia przestępstwa nieudostępnienia informacji publicznej, tj. czynu z art. 23 ustawy o dostępie do informacji publicznej.

.....

(*podpis Zawiadamiającego*)

Załączniki:

1. Wniosek o udostępnienie informacji publicznej.
2. Decyzja SKO.

Objaśnienia do wzoru

[1] **Organ właściwy** – zawiadomienie składa się do prokuratora lub Policji.

[2] **Forma zawiadomienia** – Kodeks postępowania karnego nie przewiduje szczególnej formy zawiadomienia o podejrzeniu popełnienia przestępstwa. Zawiadomienie można złożyć zarówno pisemnie, jak i ustnie do protokołu.

[3] **Podmioty zobowiązane do złożenia zawiadomienia** – Kodeks postępowania karnego przewiduje społeczny i prawny obowiązek zawiadomienia o przestępstwie ściganym z oskarżenia publicznego. Obowiązek społeczny, nie jest obłożony żadną sankcją i spoczywa na każdej osobie posiadającej wiarygodną informację o przestępstwie ściganym z urzędu. Prawny obowiązek spoczywa natomiast na instytucjach państwowych i samorządowych, jeżeli w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu.

Podstawa prawna

- art. 33, art. 34, art. 35 ustawy z 6.6.1997 r. – Kodeks karny (t.j. Dz.U. z 2018 r. poz. 1600 ze zm.)
- art. 304 ustawy z 6.6.1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2018 r. poz. 1987 ze zm.)
- art. 4 ust. 1 i 2, art. 23 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.)

C·H·BECK
Beck Akademia
konferencje • szkolenia • e-learning

Tajemnica adwokacko-radcowska a prawa osoby, której dane dotyczą (Rozdział III RODO)

Katarzyna Kloc
Adwokat oraz partner w kancelarii Gawroński & Partners s.k.a., ekspert w obszarze ochrony danych osobowych

Maciej Gawroński
Opis

Wejście w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1; dalej: RODO) oraz wszelkie inne zmiany w zakresie regulacji dotyczących ochrony danych osobowych, takie jak wejście w życie nowej ustawy z 10.5.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.; dalej: OchrDanychU) oraz planowane zmiany w przepisach sektorowych są wyzwaniem zarówno dla organizacji, jak i dla doradzających im prawników. Ogólnikowość części przepisów RODO w połączeniu z imperatywnością pozostałych i brakiem reguł kolizyjnych prowadzą do licznych wątpliwości, jak przetwarzać dane osobowe zgodnie z prawem.

Wyzwaniem dla kancelarii prawnych jest implementacja wymogów RODO z uwzględnieniem szczególnych obowiązków nałożonych na radców prawnych i adwokatów przez przepisy prawa regulujących zasady wykonywania powyższych zawodów (ustawa z 26.5.1982 r. – Prawo o adwokaturze, t.j. Dz.U. z 2018 r. poz. 1184 ze zm.; dalej: PrAdw) oraz ustawa z 6.7.1982 r. o radcach prawnych (t.j. Dz.U. z 2017 r. poz. 1870 ze zm.; dalej: RadPrU), a przede wszystkim z uwzględnieniem obowiązku zachowania tajemnicy adwokacko-radcowskiej. Problem częściowo został przedstawiony w projektowanych zmianach w przepisach sektorowych[1]. Dostrzeżono, że stosowanie przepisów RODO przez kancelarie w pełnym zakresie skutkować będzie naruszeniem jednego z podstawowych obowiązków ciążących na adwokatach i radcach prawnych jako osobach zaufania publicznego, tj. obowiązku zachowania tajemnicy zawodowej. W projektowanych zmianach, m.in. w Prawie

[1] Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z 22.10.2018 r. opublikowany na stronie: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/149781_projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-zapewnieniem-stosowania-rozporzadzenia-2016-679.html.

o adwokaturze i w ustawie o radcach prawnych wprowadzono ograniczenia stosowania przez prawników niektórych przepisów RODO. Nie wyjaśnia to jednak wszystkich wątpliwości, a wręcz tworzy nowe. Co więcej, jak wynika z niniejszego artykułu, projektowane przez ustawodawcę rozwiązania dotyczące tajemnicy zawodowej są w znacznym stopniu zbędne[2].

Przetwarzanie danych w kancelarii prawnej – ogólne informacje

Przetwarzanie informacji, w tym danych osobowych, pozyskanych zarówno od klientów będących osobami fizycznymi, jak i od firm i innych organizacji, jest dla adwokatów oraz radców prawnych istotą ich działalności. Prawnicy zazwyczaj mają dostęp do danych szczególnie istotnych, zarówno z punktu widzenia jednostki, jak i firmy. Niekoniecznie muszą to być szczególne kategorie danych w rozumieniu art. 9 RODO, to jest dane takie jak informacje o stanie zdrowia, czy o poglądach politycznych. Specyfika działalności prawniczej powoduje, że często dane, w których posiadaniu są kancelarie prawne, to dane finansowe, dane stanowiące tajemnicę handlową, informacje o życiu rodzinnym czy informacje związane z podejrzeniem popełnienia przez klienta przestępstwa (obecnie wyłączone z katalogu szczególnych kategorii danych zgodnie z art. 9 i przetwarzane w oparciu o art. 10 RODO).

Ważne

Kancelaria musi zapewnić, niezależnie od ogólnych regulacji w zakresie ochrony danych osobowych, żeby procesy przetwarzania danych prowadzone były z poszanowaniem tajemnicy adwokackiej i tajemnicy radcy prawnego.

Kancelaria jako administrator

Zgodnie z art. 4 pkt 7) RODO „administrator" danych osobowych to „podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych".

To czy kancelaria świadcząca na rzecz klienta usługi prawne jest podmiotem przetwarzającym czy administratorem danych, zależy w pierwszej kolejności od tego, kim jest klient. W relacjach z konsumentami (tak zwane relacje B2C – ang. *business to consumer*) kancelarie są z definicji administratorami danych.

Natomiast przy świadczeniu usług na rzecz firm (relacje B2B) czy innych organizacji, rola kancelarii wymaga bliższej analizy. Jeżeli kancelaria świadczy usługi na rzecz innego administratora danych osobowych (przedsiębiorcy, innej instytucji), swoboda kancelarii w określaniu celów i sposobów przetwarzania danych jest ograniczona. Stąd zdania co do tego, czy kancelaria występuje jako administrator danych osobowych w sprawie klienta instytucjonalnego, są podzielone.

Ustawodawca za administrowaniem

W projektowanych zmianach w przepisach sektorowych zrezygnowano z bezpośredniego uregulowania statusu adwokatów i radców prawnych jako administratorów danych, co znalazło się we wcześniejszej wersji projektu. Pomimo tego, z uzasadnienia projektu można wywnioskować, że **ustawodawca popiera koncepcję administrowania danymi przez adwokatów i radców prawnych**. W jednej z pierwszych wersji projektu zmian pojawiła się regulacja nadająca każdemu adwokatowi, czy radcy prawnemu status odrębnego administratora danych, jednak na obecnym etapie z koncepcji tej zrezygnowano.

Celem przetwarzania danych osobowych w trakcie realizacji zlecenia dla klienta jest świadczenie usług prawnych na rzecz klienta w celu określonym przez klienta. Prawnik „certyfikowany" (adwokat, radca prawny) dysponuje wprawdzie pewną swobodą w doborze narzędzi prawnych (sposobów przetwarzania danych), ale nie ma w tym zakresie dowolności. Przy bardziej skomplikowanych sprawach, czy poradach prawnych, kancelaria faktycznie ma pewien margines swobody w zakresie decydowania, jakie dane i w jakim konkretnie celu pozyskuje od klienta, aby usługa została wykonana jak najkorzystniej. Przykładem takich sytuacji są skomplikowane spory sądowe, w których to prawnicy z reguły decydują, jaki zakres danych osobowych pozyskują od swojego zleceniodawcy, od świadków, przesłuchując świadków strony przeciwnej i w jaki sposób zostaną one w procesie wykorzystane. W takich sytuacjach zręczny prawnik „buduje" sprawę. Z drugiej strony wszystkie informacje pozyskane przez kancelarię należą do klienta i to klient ma ostatecznie prawo zdecydować, jak one zostaną wykorzystane. Prawnik w proteście może co najwyżej wypowiedzieć pełnomocnictwo.

Kancelaria jako podmiot przetwarzający

Z drugiej strony liczne głosy zwracają uwagę, że kancelaria nie decyduje ani o celach, ani o sposobach przetwarzania danych. W związku z tym, świadcząc usługi prawne na rzecz klienta – profesjonalisty (przedsiębiorcy lub innej instytucji, której przysługuje status administratora danych), kancelaria jedynie przetwarza w jego imieniu powierzone dane osobowe.

[2] Z wyjątkiem propozycji art. 16b PrAdw i art. 5b RadPrU, które przywracają tajemnicę zawodową względem Prezesa Urzędu Ochrony Danych Osobowych, usuniętą przez ustawodawcę w nowej ustawie o ochronie danych osobowych.

Obowiązki podmiotu przetwarzającego

W przypadku ukształtowania relacji z klientem na zasadzie powierzenia przetwarzania danych, konieczne będzie zawarcie odpowiedniej umowy powierzenia pomiędzy administratorem (klientem instytucjonalnym) a kancelarią. W umowie takiej strony muszą uregulować kwestie takie jak: przedmiot przetwarzania, czas trwania, charakter i cel przetwarzania, rodzaj powierzonych danych, kategorię osób, których dane dotyczą, obowiązki i prawa administratora oraz obowiązki podmiotu przetwarzającego. Kancelaria przetwarzająca dane w imieniu klienta jest obowiązana, zgodnie z art. 28 ust. 3 RODO, do:

1) przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora;
2) zapewnienia, aby osoby upoważnione zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy (zatem w przypadku kancelarii prawnej personel kancelarii posiadający dostęp do danych powinien zostać zobowiązany do zachowania tajemnicy);
3) zapewnienia danym odpowiedniego stopnia bezpieczeństwa (wdrożenia wszelkich środków wymaganych na mocy art. 32 RODO);
4) przestrzegania warunków dotyczących korzystania z usług innego podmiotu przetwarzającego (tj. dalsze powierzenie jedynie za zgodą administratora);
5) wsparcia administratora w procesie obsługi praw jednostki (w odniesieniu do danych, które przetwarza i z którymi związane są żądania osób);
6) wsparcia administratora w procesie zgłaszania incydentów naruszenia ochrony danych i w określonych przypadkach w procesie informowania o tych incydentach osób, których dane dotyczą;
7) usunięcia/zwrotu danych po zaprzestaniu świadczenia usług oraz
8) udostępnienia administratorowi (klientowi) wszelkich informacji niezbędnych do wykazania, że kancelaria przetwarza dane osobowe zgodnie z prawem oraz zawartą umową oraz umożliwienia przeprowadzenia przez administratora audytu.

Audyty „klienckie"

Podnoszone są przez niektórych prawników wątpliwości, co do możliwości poddania się przez kancelarię audytowi zgodności przetwarzania danych, gdy obowiązuje tajemnica zawodowa. Uznanie takiego argumentu prowadziłoby do wniosku, że prawo audytu z art. 28 ust. 3 lit. h) RODO jest niewykonalne w każdym przypadku. Każdego przedsiębiorcę (w tym np. firmy księgowe) obowiązuje tajemnica przedsiębiorstwa i tajemnica handlowa, w związku z którą nie mogą ujawniać jednemu swojemu klientowi danych przetwarzanych na rzecz drugiego. Stąd należy go uznać za nietrafny, natomiast sytuację kancelarii wcale nie za taką wyjątkową. Nie ma przeszkód formalnych ani praktycznych, aby z zachowaniem tajemnicy przetwarzania danych innych klientów umożliwić danemu klientowi weryfikację sposobu przetwarzania danych, które do tego klienta należą.

Weryfikacja podmiotów przetwarzających

Nowością na gruncie RODO jest obowiązek zweryfikowania przez administratora danych, czy podmiot przetwarzający zapewnia „wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą" (art. 28 ust. 1 RODO).

Oznacza to, że w przypadku uznania za słuszną koncepcji kancelarii jako podmiotu przetwarzającego, o jej wyborze nie powinien decydować tylko poziom świadczenia usług prawniczych i renoma, ale również gwarancja wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Chodzi tu przede wszystkim o bezpieczeństwo danych osobowych.

W praktyce, w decydowaniu o tym, czy kancelaria jest odrębnym administratorem danych czy podmiotem przetwarzającym, znaczenie mogą mieć okoliczności związane z danym zleceniem takie jak:

1) fakt, czy klient jest konsumentem, czy profesjonalistą;
2) charakter zlecenia (np. spór z konkretnym pracownikiem), ale także
3) wyraźne preferencje klienta.

Niezależnie od tego, czy kancelaria prawna w relacji z klientem jest administratorem danych, czy też podmiotem przetwarzającym, musi ona zadbać o to, aby przetwarzanie danych odbywało się w poszanowaniu tajemnicy zawodowej, czy to w umowie powierzenia przetwarzania danych, przy spełnianiu obowiązku informacyjnego, wdrożenia odpowiednich środków bezpieczeństwa i udokumentowaniu wszelkich procesów. Zatem status administratora/podmiotu przetwarzającego nie wpływa w żaden sposób na obowiązek zachowania tajemnicy zawodowej.

Prawnicy w kancelariach/ podwykonawstwo

Specyfika zawodów prawniczych powoduje, że często adwokaci czy rad-

cowie prawni nie są zatrudniani na podstawie umowy o pracę. W kancelariach prawnych prawnicy najczęściej świadczą usługi na podstawie umowy o współpracy, co wynika z konieczności zapewnienia prawnikom odpowiedniego stopnia niezależności przy świadczeniu przez nich usług prawnych, jak i w przypadku adwokatów z PrAdw (adwokaci nie mogą wykonywać zawodu pozostając w stosunku pracy). Nawet w organizacjach innych niż kancelaria adwokacka, czy radcowska prawnicy wewnętrzni często świadczą usługi na zasadzie umowy cywilnoprawnej z firmą. Jaka jest wówczas rola w procesie przetwarzania danych takiego adwokata, czy radcy prawnego? Czy każdy, kto współpracuje z kancelarią na zasadzie umowy o współpracę, prowadzi swoją własną działalność gospodarczą i świadczy usługi na rzecz klientów formalnie jest odrębnym administratorem danych osobowych?

Jak już wspomniano koncepcja, którą można nazwać „teorią totalnego administrowania", pojawiła się na etapie projektowania zmian w przepisach sektorowych. Następnie jednak została usunięta z ostatniej wersji dostępnego autorom projektu przepisów sektorowych. Regulacja, w której każdy współpracownik kancelarii będący adwokatem lub radcą prawnym byłby odrębnym administratorem danych, nie odpowiadałaby rzeczywistości oraz byłaby niepraktyczna. Każdy z licznych administratorów musiałby bowiem wykonywać obowiązek informacyjny wobec klienta, zgłaszać naruszenia ochrony danych, obsługiwać prawa jednostki, co prowadziłoby do chaosu i trudności ze sprostaniem obowiązkom wprowadzonym przez RODO.

PRZYKŁAD

Kancelaria X działająca w formie spółki komandytowej (Kancelaria X Iksiński sp.k.) zawarła umowę z klientem *Janem Kowalskim*, w jego sprawie spadkowej, nie związanej z działalnością zawodową lub gospodarczą. *De facto* zlecenie będzie wykonywane przez adwokat *Annę Nowak*, która współpracuje z Kancelarią X na podstawie umowy o współpracy o charakterze trwałym oraz dodatkowo prowadzi swoją własną kancelarię adwokacką. Administratorem danych osobowych *Jana Kowalskiego* będzie Kancelaria X, bo to ona decyduje o celach (przynajmniej formalnie) i sposobach przetwarzana danych. Mecenas *Nowak* nie będzie odrębnym administratorem, ponieważ w tym układzie działa jako upoważniony personel Kancelarii X. Inaczej sytuacja będzie wyglądała w przypadku klientów, których mec. *Anna Nowak* obsługuje samodzielnie i zupełnie niezależnie od Kancelarii X. w ramach swojej działalności gospodarczej. Wówczas mec. *Nowak* będzie administratorem danych swoich klientów i obowiązana będzie do spełnienia wszystkich obowiązków nałożonych przez RODO na administratorów.

Tajemnica zawodowa

Z uwagi na specyfikę wykonywanej działalności adwokata i radcy prawnego oraz zupełnie niezależnie od przepisów o ochronie danych osobowych, polski prawodawca w ustawach regulujących te zawody nałożył na prawników obowiązek zachowania tajemnicy zawodowej.

Zgodnie z art. 6 PrAdw **adwokat** ma obowiązek zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Obowiązek ten nie ma ograniczenia czasowego i adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się, udzielając pomocy prawnej lub prowadząc sprawę. **Jedynym wyjątkiem, gdy tajemnica adwokacka nie obowiązuje, są informacje udostępnianie na podstawie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu** (ustawa z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu; t.j. Dz.U. z 2018 r. poz. 723 ze zm.).

O tajemnicy adwokackiej mowa jest także w przepisach prawa procesowego karnego, cywilnego, a także administracyjnego oraz w aktach wewnętrznych organów samorządowych takich np. kodeks etyki adwokackiej.

Podobnie jak w przypadku adwokatów uregulowana jest kwestia obowiązkowego zachowania przez **radcę prawnego** w tajemnicy wszelkich informacji, o których dowiedział się w związku z udzielaniem pomocy prawnej. Zgodnie z art. 3 ust. 3–6 RadPrU, radca prawny ma bezwzględny, nieograniczony w czasie obowiązek zachowania w tajemnicy wszystkiego, o czym dowiedział się w związku z prowadzeniem sprawy klienta lub udzielaniu mu pomocy prawnej, z wyjątkiem informacji udzielanych w związku z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu.

Tajemnica zawodowa a RODO

Informacje, które adwokaci i radcowie prawni pozyskują od klientów, to przede wszystkim dane osobowe. Z uwagi na powyżej wskazane obowiązki do zachowania tajemnicy zawodowej, przetwarzanie informacji przez kancelarie prawne podlega więc dwóm reżimom prawnym:

1) przepisom o ochronie danych osobowych, tj. RODO i ustawie z 10.5.2018 r. o ochronie danych osobowych oraz
2) ustawom regulującym zasady wykonywania zawodu adwokata oraz radcy prawnego.

Istotne są również regulacje samorządowe adwokatów i radców prawnych, takie jak regulamin wykonywania zawodu adwokata[3] w kancelarii indywidualnej lub spółkach, czy regulamin

[3] Uchwała nr 54/2009 Naczelnej Rady Adwokackiej z 12.9.2009 r. ze zmianami wprowadzonymi uchwałą nr 72/2012 Naczelnej Rady Adwokackiej z 17.3.2012 r. i uchwałą 38/2015 z 27.6.2015 r.

wykonywania zawodu radcy prawnego[4], które to regulują między innymi zasady bezpiecznego przetwarzania informacji przez prawników z uwagi na tajemnicę zawodową adwokata czy radcy prawnego. Regulacje te nie stoją w konflikcie z przepisami RODO.

Stosowanie przepisów RODO przez kancelarie w pełnym zakresie w obszarze realizacji praw jednostki skutkować będzie jednak naruszeniem obowiązku zachowania tajemnicy zawodowej.

Realizacja praw jednostki

RODO wymienia następujące prawa osób, których dane dotyczą:

1) prawo do informacji przy pozyskiwaniu danych bezpośrednio (art. 13 RODO);
2) prawo do informacji przy pozyskiwaniu danych pośrednio (art. 14 RODO);
3) prawo do dostępu dodanych i do kopii danych (art. 15 ust. 1 i 3 RODO);
4) prawo do sprostowania i uzupełnienia danych (art. 16 RODO);
5) prawo do usunięcia danych (art. 17 RODO);
6) prawo do ograniczenia przetwarzania danych (art. 18 RODO);
7) prawo do informacji o odbiorcach danych (art. 19 RODO);
8) prawo do przenoszenia danych (art. 20 RODO);
9) prawo sprzeciwu (art. 21 RODO);
10) prawo do odwołania od decyzji automatycznej wywołującej skutki prawne lub podobne (art. 22 RODO).

Zmiany w przepisach sektorowych

W art. 90 RODO uregulowano kwestię konieczności wprowadzenia przepisów szczególnych regulujących obowiązki zachowania tajemnicy zawodowej, jeżeli jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy. Problem przy realizacji praw jednostki w zderzeniu z tajemnicą zawodową dostrzeżony został przez polskiego ustawodawcę, w związku z czym w projektowanych zmianach w PrAdw i RadPrU wprowadzono ograniczenia stosowania niektórych przepisów RODO związanych z realizacją praw osób, których dane dotyczą.

Projekt zmian do przepisów sektorowych, zakłada dodanie odpowiednio Działu IA w PrAdw oraz Działu 1a w RadPrU, których projektowane przepisy stanowią, że:

1) prawo dostępu do danych (art. 15 ust. 1 i 3 RODO);
2) ograniczenie przetwarzania danych (art. 18 RODO);
3) obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO)

– stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez adwokata lub radcę prawnego tajemnicy zawodowej.

Obowiązek wykonania prawa sprzeciwu przez adwokatów lub radców prawnych wynikający z art. 21 ust. 1 RODO w ogóle nie ma zastosowania w przypadku danych osobowych pozyskanych w związku z udzielaniem pomocy prawnej.

A co z pozostałymi prawami? Prawa osób, których dane dotyczą i do których obsługi obowiązany na gruncie RODO jest każdy administrator danych, to poza wskazanymi powyżej, to również prawa takie jak:

1) prawo do informacji (art. 13 i 14 RODO);
2) prawo do sprostowania danych (art. 16 RODO);
3) prawo do usunięcia danych (art. 17 RODO);
4) prawo do przenoszenia danych (art. 20 RODO);
5) prawo do odwołania od zautomatyzowanego przetwarzania danych o skutkach prawnych lub podobnych (art. 22 RODO), które jednak ze swej natury do przetwarzania danych osobowych przez prawników nie znajdzie zastosowania, zapewne aż do czasu, gdy kancelarie zaczną wykorzystywać sztuczną inteligencję

– dlatego również te prawa powinny być przedmiotem analizy, czy ich wykonanie nie naruszy obowiązku zachowania tajemnicy.

Warto zwrócić uwagę, że z bezpośrednim problemem konfliktu wykonywania praw jednostki z tajemnicą zawodową nie zderzy się kancelaria, która przetwarza dane osobowe dla klienta jako podmiot przetwarzający. W przypadku podmiotów przetwarzających dane, obowiązek współpracy przy wykonywaniu praw osób, których dane dotyczą, może wynikać z treści zawartej z administratorem umowy powierzenia przetwarzania danych (np. w zakresie wykonywania prawa dostępu do danych czy prawa do bycia zapomnianym – w sytuacjach, gdy tylko przetwarzający jest w faktycznym posiadaniu danych i bez jego pomocy administrator nie będzie w stanie wykonać żądania). Jednak podmiot przetwarzający może po prostu odesłać osobę do administratora danych.

Obowiązek informacyjny

Każdy administrator ma obowiązek poinformowania osób, których dane pozyskał o szczegółach przetwarzania, takich jak: kto jest administratorem i gdzie ma siedzibę, dane kontaktowe inspektora ochrony danych (jeżeli został powołany), cel i podstawa przetwarzania, kategorie danych, odbiorcy danych, przekazywanie danych do państwa trzeciego, okres retencji danych,

[4] Uchwała nr 94/IX/2015 KRRP z 13.6.2015 r. w sprawie Regulaminu wykonywania zawodu radcy prawnego.

prawa przysługujące osobie, której dane dotyczą. Obowiązek ten dotyczy zarówno danych pozyskiwania bezpośrednio od osoby, której dane dotyczą, jak i danych z innego źródła.

Pozyskiwanie danych pośrednio

Zgodnie z art. 14 ust. 3 RODO administrator podaje informacje o przetwarzaniu osobie, której dane pozyskał z innego źródła, jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji lub jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu, a w każdym przypadku najpóźniej w terminie miesiąca od ich pozyskania.

W świetle powyższych obowiązków adwokat czy radca prawny, który pozyskał dane przeciwnika procesowego klienta od tego klienta, byłby zmuszony najpóźniej w ciągu miesiąca powiadomić tę osobę o wszystkich wymaganych przez RODO szczegółach przetwarzania, np. o celu przetwarzania – przetwarzania danych w celu przygotowaniu pozwu lub wniosku o zabezpieczenie przeciwko osobie, które dane prawnik pozyskał. Prowadziłoby to wprost do konfliktu z tajemnicą zawodową i celem przetwarzania danych osobowych przez prawnika.

Z tego powodu już w samym RODO zagwarantowano wprost, że zgodnie z art. 14 ust. 5 lit. d) obowiązku informacyjnego „nie wykonuje się, jeżeli dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie UE lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnic".

Co więcej, jeżeli pozyskiwanie danych osobowych następuje w ramach konkretnego postępowania: cywilnego, administracyjnego, karnego – wtedy, zgodnie z art. 14 ust. 5 lit. c) RODO, przepisy danego postępowania stosuje się w całości, regulując uprawnienia osób zaangażowanych (np. świadków, podejrzanych, oskarżonych, stron, interwenientów).

Pozyskiwanie danych bezpośrednio

Obowiązek informacyjny przy pozyskiwaniu danych bezpośrednio od osoby, której dane dotyczą, został uregulowany w art. 13 RODO. W przepisie tym brak jest odpowiednika art. 14 ust. 5 lit. d) RODO. Jak więc godzić obowiązek poinformowania osoby, z którą prowadzi się komunikację, o tym po co się jej dane przetwarza, z tajemnicą zawodową? Rozwiązanie tkwi w etyce. Uznawszy, że pozyskiwanie danych podstępnie jest nieetyczne, należy poinformować osobę, od której pozyskuje się dane istotne dla sprawy (w szczególności świadka), o tym, po co te dane są zbierane. Aby zachować zgodność z tajemnicą zawodową, należy albo ograniczyć się do ogólnego opisania celu pozyskania danych i tożsamości administratora, a gdy to nie wystarczy uzyskać zgodę klienta na bliższe przestawienie sprawy albo powstrzymać się od wyłudzania informacji.

Prawo dostępu do danych

Prawo dostępu do danych, przewidziane w art. 15 RODO, odpowiada prawu do informacji. W obu przypadkach dochodzi do przekazania osobie, której dane dotyczą, szeregu szczegółowych informacji o procesie przetwarzania danych. Podstawowa różnica polega na tym, że prawo dostępu do danych wykonywane jest na żądanie osoby, a nie jak w przypadku obowiązku informacyjnego na mocy przepisów prawa oraz na tym, że w ramach wykonywania żądania dostępu do danych administrator może zostać obowiązany do wydania kopii danych.

W RODO nie przewidziano wprost możliwości wyłączenia stosowania prawa dostępu do danych z uwagi na tajemnice zawodowe. Dlatego kwestię realizacji prawa dostępu do danych i obowiązku zachowania tajemnicy zawodowej uregulowano wprost w projektowanych zmianach do przepisów sektorowych.

Zmiany zakładają, że adwokat lub radca prawny wykonuje żądanie osoby, której dane dotyczą w zakresie uzyskania od administratora potwierdzenia, czy przetwarza on jej dane osobowe, a jeżeli ma to miejsce, to udostępnia informacje, których zakres odpowiada zakresowi obowiązku informacyjnego tylko wtedy, jeżeli nie dojdzie przy tym do naruszenia tajemnicy zawodowej. Podobnie sprawa wygląda w przypadku obowiązku wydania kopii danych.

W przypadku udzielania dostępu do danych bezpośrednio klientowi, który sam przekazał kancelarii swoje dane osobowe, nie dojdzie do naruszenia tajemnicy zawodowej, zaś w przypadku, gdy do kancelarii z żądaniem uzyskania dostępu do danych zgłosi się osoba, która podejrzewa, że ktoś inny mógł jej dane przekazać, wykonanie takiego żądania naruszy tajemnicę zawodową.

PRZYKŁAD

Adwokat *Piotr Nowakowski*, prowadzący jednoosobową praktykę adwokacką jest administratorem wszystkich danych osobowych związanych ze sprawą rozwodową swojej klientki pani *Anny Kowalskiej*. Mąż pani *Anny Kowalskiej* podejrzewając, że żona korzysta z pomocy prawnej mecenasa Nowakowskiego, zgodnie z art. 15 ust. 1 RODO, zwraca się do niego z żądaniem uzyskania potwierdzenia, że mecenas *Nowakowski* jest w posiadaniu jego danych i zgodnie z art. 15 ust. 3 – otrzymania kopii wszystkich informacji związanych z jego osobą uzyskanych przez mecenasa od planującej wniesienie pozwu rozwodowego małżonki. Adwokat *Nowakowski*, z uwagi na obowiązującą go tajemnicę zawodową wobec swojej klientki, nie ma prawa przekazać panu *Kowalskiemu* informacji, które posiada w związku z prowadzoną sprawą.

Prawa do sprostowania i usunięcia danych

W projektowanych zmianach do PrAdw i RadPrU pominięto kwestię relacji prawa do sprostowania danych, prawa do usunięcia danych oraz prawa do przenoszenia danych do tajemnicy zawodowej.

Wskazuje to na powierzchowną analizę problemu pozyskiwania danych przez prawników. Żądanie sprostowania danych przy bezpośrednim pozyskiwaniu danych musi podlegać ocenie prawnika (np. zmiana „zeznań"). Gdyby natomiast do prawnika zgłosiła się osoba żądająca sprostowania tego, co o niej powiedziała inna osoba, prawnik nie może się do takiego żądania ustosunkować, gdyż naruszyłby tajemnicę zawodową. Podstawą odmowy rozpatrzenia takiego żądania sprostowania danych będzie więc ponownie art. 14 ust. 5 lit. d) RODO.

Projektowane zmiany w przepisach sektorowych przewidują ograniczenia w zakresie wykonywania prawa do ograniczenia przetwarzania (art. 18 RODO) oraz obowiązku powiadomienia odbiorców o sprostowaniu, usunięciu lub ograniczeniu przetwarzania (art. 19 RODO).

Jak wskazano w uzasadnieniu projektu, w sytuacji zgłoszenia żądania ograniczenia przez osobę trzecią, jeżeli jej dane osobowe zostały ujawnione adwokatowi czy radcy prawnemu przez klienta kancelarii, przyznawanie pierwszeństwa wykonaniu obowiązków określonych w powołanym przepisie nad obowiązkiem zachowania tajemnicy zawodowej (w tym obrończej), skutkować będzie naruszeniem praw i interesów klienta oraz podważeniem wiarygodności zawodu adwokata i radcy prawnego[5].

Prawo do przenoszenia danych

Zgodnie z art. 20 ust. 1 RODO osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

1) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) oraz
2) przetwarzanie odbywa się w sposób zautomatyzowany.

W relacjach, gdy dane objęte żądaniem pozyskane zostały bezpośrednio (od klienta), wykonanie prawa dostępu do danych nie naruszy tajemnicy zawodowej. W sytuacji, gdy z żądaniem wykonania prawa do przenoszenia danych wystąpi osoba, której dane kancelaria pozyskała pośrednio, kancelaria musiałaby najpierw potwierdzić, że przetwarza konkretne dane osobowe lub ujawnić te dane. Prawo do przenoszenia danych obowiązuje w relacjach bezpośrednich, a więc tylko z klientem.

Osoba, której dane dotyczą może wnieść sprzeciw wobec przetwarzania danych osobowych w określonych przypadkach. Obowiązek wykonania prawa sprzeciwu przez adwokatów lub radców prawnych, wynikający z art. 21 ust. 1 RODO, w ogóle nie ma zastosowania w przypadku danych osobowych pozyskanych w związku z udzielaniem pomocy prawnej.

Sprzeciw zgłoszony kancelarii może uniemożliwić przetwarzanie danych, a w konsekwencji zablokuje możliwość dochodzenia roszczeń na rzecz klienta lub uniemożliwi dalsze prowadzenie tego postępowania sądowego, prowadząc do jego przewlekłości.

Tajemnica zawodowa adwokata czy radcy prawnego ma szczególne znaczenie dla zawodów zaufania publicznego oraz ma pierwszeństwo przed wszystkimi innymi obowiązkami, które mogą się wiązać z ujawnianiem czy udostępnianiem informacji.

Analiza realizacji praw jednostki pod kątem naruszenia tajemnicy zawodowej przez adwokata/radcę prawnego prowadzi do generalnego wniosku, że problem ujawnienia tajemnicy nie występuje przy pozyskiwaniu danych bezpośrednio od osoby, której te dane dotyczą. Jak wskazano, danych nie należy pozyskiwać podstępnie.

Pozyskując dane z innych źródeł niż od osoby, której dane dotyczą, kancelaria z zasady nie powinna informować tej osoby o przetwarzaniu danych, jeżeli to przetwarzanie jest objęte tajemnicą zawodową (art. 14 ust. 5 lit. d) RODO). Przy realizacji jakichkolwiek praw jednostki wobec osób, których dane kancelaria otrzymała pośrednio, dojdzie do ujawnienia pozyskanych danych. Dlatego wnioski w odniesieniu do poszczególnych praw są następujące:

1) prawo do informacji przy pozyskiwaniu danych bezpośrednio – konflikt z tajemnicą zawodową rozstrzygany jest na polu etyki;
2) prawo do informacji przy pozyskiwaniu danych pośrednio – nie ujawnia się tajemnicy;
3) prawo do dostępu dodanych i do kopii danych – musielibyśmy ujawnić dane pozyskane pośrednio – więc nie ujawnia się tajemnicy;
4) prawo do sprostowania i uzupełnienia danych – musielibyśmy ujawnić dane pozyskane pośrednio – więc nie ujawnia się tajemnicy;
5) prawo do usunięcia danych – musielibyśmy ujawnić dane pozyskane pośrednio – więc nie ujawnia się tajemnicy;
6) prawo do ograniczenia przetwarzania danych – musielibyśmy ujawnić dane pozyskane pośrednio – więc nie ujawnia się tajemnicy;

[5] Uzasadnienie projektu zmian przepisów sektorowych z 22.10.2018 r.

7) prawo do informacji o odbiorcach danych – musielibyśmy ujawnić dane pozyskane pośrednio – więc nie ujawnia się tajemnicy;
8) prawo do przenoszenia danych – obowiązuje w relacjach bezpośrednich – a więc tylko z klientem (nie dotyka tajemnicy zawodowej);
9) prawo sprzeciwu – musielibyśmy ujawnić dane pozyskane pośrednio – więc nie ujawnia się tajemnicy;
10) prawo do odwołania od decyzji automatycznej wywołującej skutki prawne lub podobne – prawnicy na razie decydują nieautomatycznie.

Podstawa prawna

- art. 4 pkt 7), art. 9, art. 10, art. 14 ust. 5 lit. d), art. 21 ust. 1, art. 28 ust. 3, art. 32 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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.Urz. UE L Nr 119, s. 1)
- art. 6, art. 16b ustawy z 26.5.1982 r. – Prawo o adwokaturze (t.j. Dz.U. z 2018 r. poz. 1184 ze zm.)
- art. 3 ust. 3–6, art. 5b ustawy z 6.7.1982 r. o radcach prawnych (t.j. Dz.U. z 2017 r. poz. 1870 ze zm.)

Podsumowanie

Dogłębna analiza sytuacji, w których może się znaleźć adwokat lub radca prawny będący administratorem danych osobowych w przypadku skierowania do niego żądania opartego o przepisy Rozdziału III RODO (prawa jednostki), wskazuje, że kluczem w każdym przypadku pozostaje art. 14 ust. 5 lit. d) RODO. Przepis ten wprost zwalnia adwokata/radcę prawnego z obowiązku informacyjnego, tylko wtedy, gdy dane osobowe pozyskał od innej osoby, dokonując czynności objętych tajemnicą zawodową. Jednak do wykonania każdego z praw jednostki potrzebna jest wiedza o tym, czy kancelaria przetwarza konkretne dane osobowe lub ujawnienie tych danych. Stąd w oparciu o wspomniany przepis adwokat/radca prawny/kancelaria powinni odmówić wykonania każdego żądania osoby, które prowadziłoby do ujawnienia tych danych osobowych, które są objęte tajemnicą. W takiej sytuacji w odpowiedzi na konkretne żądanie należałoby odpisać: „W zakresie, w jakim Pani/Pana żądanie mogłoby doprowadzić do ujawnienia tajemnicy zawodowej, zgodnie z art. 14 ust. 5 lit. d) RODO, zostało ono pozostawione bez rozpoznania".

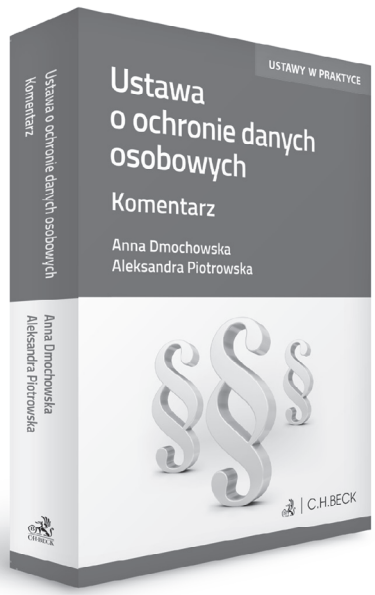
Jak więc wynika z powyższego, proponowane przez polskiego ustawodawcę przepisy dotyczące pogodzenia tajemnicy zawodowej z wykonywaniem praw jednostki mogą być uznane za zbędne.

C.H.BECK

Ustawa o ochronie danych osobowych
Komentarz

Praktyczny komentarz do ustawy o ochronie danych osobowych

- Przystępna i zrozumiała wykładnia przepisów ustawy o ochronie danych osobowych
- Praktyczne przykłady, dzięki którym Czytelnik jest w stanie lepiej zrozumieć zagadnienia obszaru ochrony danych osobowych
- Odwołania do wytycznych Grupy Roboczej Art. 29 oraz orzecznictwa,
- Wykładnia przepisów ustawy o ochronie danych osobowych w odniesieniu do wytycznych RODO



www.ksiegarnia.beck.pl
Zadzwoń: 81 46 13 300 • E-mail: kontakt@beck.pl

Różnice w nadawaniu uprawnień do dostępu do informacji niejawnych przetwarzanych w jednostkach samorządu terytorialnego – schemat postępowania

Po wejściu w życie ustawy z 5.8.2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2018 r. poz. 412 ze zm.; dalej: OchrInfU), zgodnie z postanowieniami jej art. 181, w jednostkach samorządu terytorialnego dokonano przeglądu wytworzonych materiałów zawierających informacje niejawne, w celu ustalenia czy spełniają one ustawowe przesłanki ochrony na podstawie wspomnianej ustawy.

Marek Anzel
Pełnomocnik ochrony, ekspert KSOIN ds. ochrony informacji niejawnych i bezpieczeństwa TI

Po przeprowadzeniu przeglądu okazało się, że w poszczególnych jednostkach samorządu terytorialnego przetwarzane są informacje niejawne o różnych klauzulach tajności. W Polsce funkcjonują jednostki organizacyjne, w których przetwarza się informacje niejawne o klauzuli „poufne" (są przypadki, że i „tajne") oraz takie, w których najwyższą klauzulą tajności przetwarzanych informacji jest „zastrzeżone".

Takie zróżnicowanie wynika z możliwości subiektywnej oceny klasyfikowanych informacji na podstawie definicji zawartych w art. 5 OchrInfU, jak również z powodu zróżnicowania klauzul tajności napływających materiałów niejawnych z urzędów wojewódzkich dotyczących opracowania „planów operacyjnych funkcjonowania organów samorządu terytorialnego".

Ważne

Klauzula tajności przetwarzanych informacji niejawnych ma bez-

pośredni wpływ na nadawanie uprawnień do dostępu do tych informacji. Im wyższa klauzula, tym oczywiście wyższe wymagania.

Różnice w nadawaniu określonych uprawnień wynikają nie tylko z zajmowanego stanowiska, z którym może się wiązać dostęp do informacji niejawnych, ale również ze ściśle określonych wymagań zdefiniowanych w OchrInfU.

Zgodnie z postanowieniami zawartymi w art. 4 ust. 1 OchrInfU, informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.

Warunkiem niezbędnym do dostępu do informacji niejawnych jest posiadanie dwóch dokumentów:

1) pisemnego upoważnienia uprawniającego do dostępu do informacji niejawnych o klauzuli „zastrzeżone" wydanego przez kierownika jednostki organizacyjnej lub odpowiedniego poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych o klauzuli „poufne" i wyżej, które może być wydane po przeprowadzeniu – odpowiednio – zwykłego lub poszerzonego postępowania sprawdzającego;
2) zaświadczenia o odbyciu szkolenia w zakresie ochrony informacji niejawnych.

Jak zaznaczono, w zależności od zajmowanego stanowiska oraz od klauzuli tajności informacji niejawnych, do których dana osoba będzie miała dostęp, wymagane są różne z wyżej wymienionych dokumentów.

W schemacie zaprezentowanym na końcu artykułu wyszczególniono trzy kategorie osób, które w jednostce samorządu terytorialnego legitymować się będą różnymi uprawnieniami.

Są to:

1) kierownik jednostki organizacyjnej (prezydent miasta, burmistrz, starosta, wójt);
2) pełnomocnik ds. ochrony informacji niejawnych;
3) osoby zatrudnione albo wykonujące czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych.

Ponadto każda z wyżej wymienionych osób funkcyjnych legitymować się będzie różnymi dokumentami uprawniającymi, zgodnie z postanowieniami OchrInfU, do dostępu do informacji niejawnych.

Należy nadmienić, że wzory zaświadczeń o odbyciu szkolenia przedstawiono w rozporządzeniu Prezesa Rady Ministrów z 28.12.2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (t.j. Dz.U. z 2015 r. poz. 205 ze zm.; dalej: ZaśwSzkolR). Zaświadczenia wydawane są przez uprawnione podmioty określone w art. 19 ust. 1 OchrInfU, zgodnie ze ściśle określonymi wzorami przedstawionymi w załącznikach nr 1, 2 i 3 do ZaśwSzkolR.

Najwyższa klauzula tajności informacji i wymagane uprawnienia do dostępu do informacji niejawnych

Zastrzeżone:

1) kierownik jednostki organizacyjnej:
   a) upoważnienie/poświadczenie – zgodnie z postanowieniami OchrInfU kierownik jednostki organizacyjnej jest podmiotem uprawnionym do wydawania pisemnych upoważnień do dostępu informacji niejawnych o klauzuli „zastrzeżone" przetwarzanych w podległej mu jednostce. W związku z powyższym bezzasadne jest wydawanie odrębnego pisemnego upoważnienia, w którym kierownik jednostki organizacyjnej sam siebie upoważniałby do tych informacji niejawnych.
   Biorąc powyższe pod uwagę, kierownik jednostki organizacyjnej, w której najwyższą klauzulą tajności przetwarzanych informacji niejawnych jest „zastrzeżone", ma zapewniony dostęp do tych informacji na mocy ustawy, bez konieczności wystawiania samemu sobie upoważnienia;
   b) zaświadczenie o przeszkoleniu – na mocy art. 19 ust. 2 pkt 3 OchrInfU – kierownik jednostki organizacyjnej powinien posiadać aktualne zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **wydane przez pełnomocnika ochrony**. Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 3 do ZaśwSzkolR.
   Zgodnie z postanowieniami art. 19 ust. 3 OchrInfU, zaświadczenie jest ważne do 5 lat od daty jego wydania;
2) pełnomocnik ochrony:
   a) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „poufne", **wydane przez ABW lub SKW** w ramach poszerzonego postępowania sprawdzającego – art. 14 ust. 3 pkt 3 OchrInfU;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **przeprowadzonym przez ABW albo SKW** – art. 14 ust. 3 pkt 4 OchrInfU. Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 1 do ZaśwSzkolR.

Zgodnie z art. 19 ust. 2 pkt 1 i 4 OchrInfU szkolenia wobec pełnomocników ochrony i ich zastępców oraz kandydatów na pełnomocników ochrony lub ich zastępców przeprowadza Agencja Bezpieczeństwa Wewnętrznego (w sferze cywilnej) lub Służba Kontrwywiadu Wojskowego (w sferze wojskowej);

3) osoby funkcyjne (pozostali pracownicy zatrudnieni na stanowiskach związanych z dostępem do informacji niejawnych):
   a) upoważnienie **wydane przez kierownika jednostki organizacyjnej** uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone", jeżeli dana osoba nie posiada poświadczenia bezpieczeństwa – art. 21 ust. 4 pkt 1 OchrInfU;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **wydane przez pełnomocnika ochrony** – art. 19 ust. 2 pkt 3 OchrInfU. Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 3 do ZaśwSzkolR.

Poufne:

1) kierownik jednostki organizacyjnej:
   a) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „poufne", **wydane przez ABW lub SKW** w ramach poszerzonego postępowania sprawdzającego – art. 22 ust. 1 pkt 2 lit. c) OchrInfU.

      Zasadniczo poświadczenia bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „poufne" wydaje pełnomocnik ochrony w ramach zwykłego postępowania sprawdzającego. Jednakże kierownik jednostki organizacyjnej jest wyjątkiem. Zgodnie z ww. cytowanym art. 22 OchrInfU postępowanie sprawdzające wobec kierownika jednostki organizacyjnej przeprowadza ABW lub SKW. Chodzi o to, aby uniknąć sytuacji, w której pełnomocnik ochrony będzie prowadził postępowanie sprawdzające wobec swojego pracodawcy.

      Wniosek o przeprowadzenie poszerzonego postępowania sprawdzającego wraz z wypełnioną ankietą bezpieczeństwa osobowego kierownik jednostki organizacyjnej przesyła do właściwej Delegatury ABW lub Wydziału Zamiejscowego Delegatury ABW. Wniosek, sam na siebie, podpisuje kierownik jednostki;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **wydane przez pełnomocnika ochrony** – art. 19 ust. 2 pkt 3 OchrInfU. Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 3 do ZaśwSzkolR;
2) pełnomocnik ochrony:
   a) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „poufne", **wydane przez ABW lub SKW** w ramach poszerzonego postępowania sprawdzającego – art. 14 ust. 3 pkt 3 OchrInfU;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **przeprowadzonym przez ABW albo SKW** – art. 14 ust. 3 pkt 4 OchrInfU.

      Zgodnie z art. 19 ust. 2 pkt 1 i 4 OchrInfU szkolenia wobec pełnomocników ochrony i ich zastępców oraz kandydatów na pełnomocników ochrony lub ich zastępców przeprowadza Agencja Bezpieczeństwa Wewnętrznego (w sferze cywilnej) lub Służba Kontrwywiadu Wojskowego (w sferze wojskowej). Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 1 do ZaśwSzkolR;
3) osoby funkcyjne (pozostali pracownicy zatrudnieni na stanowiskach związanych z dostępem do informacji niejawnych):
   a) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „poufne", **wydane przez pełnomocnika ochrony** w ramach zwykłego postępowania sprawdzającego – art. 22 ust. 1 pkt 1 OchrInfU.

      Zgodnie z postanowieniami art. 23 ust. 1 OchrInfU, pełnomocnik ochrony przeprowadza zwykłe postępowanie sprawdzające na pisemne polecenie kierownika jednostki organizacyjnej;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **wydane przez pełnomocnika ochrony** – art. 19 ust. 2 pkt 3 OchrInfU. Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 3 do ZaśwSzkolR.

Tajne:

1) kierownik jednostki organizacyjnej:
   a) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „tajne", **wydane przez ABW lub SKW** w ramach poszerzonego postępowania sprawdzającego – art. 22 ust. 1 pkt 2 lit. c) OchrInfU;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych. Szkolenie **przeprowadzają odpowiednio ABW lub SKW, wspólnie z pełnomocnikiem ochrony** – art. 19 ust. 2 pkt 2 OchrInfU. Zaświadczenie wydawane jest według

wzoru określonego w załączniku nr 2 do ZaśwSzkolR;

2) pełnomocnik ochrony:
   a) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „tajne", **wydane przez ABW lub SKW** w ramach poszerzonego postępowania sprawdzającego – art. 14 ust. 3 pkt 3 OchrInfU;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **przeprowadzonym przez ABW albo SKW** – art. 14 ust. 3 pkt 4 OchrInfU. Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 1 do ZaśwSzkolR;
3) osoby funkcyjne (pozostali pracownicy zatrudnieni na stanowiskach związanych z dostępem do informacji niejawnych):
   a) poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli „tajne", **wydane przez ABW lub SKW** w ramach poszerzonego postępowania sprawdzającego – art. 22 ust. 1 pkt 2 lit. a) OchrInfU.
   Zgodnie z postanowieniami zawartymi w art. 23 ust. 2 pkt 1 ABW albo SKW przeprowadzają poszerzone postępowania sprawdzające na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska lub zlecenia prac;
   b) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych **wydane przez pełnomocnika ochrony** – art. 19 ust. 2 pkt 3 OchrInfU. Zaświadczenie wydawane jest według wzoru określonego w załączniku nr 3 do ZaśwSzkolR.

Na następnej stronie przedstawiono schemat nadawania uprawnień do dostępu do informacji niejawnych, w zależności od klauzuli tajności informacji niejawnych przetwarzanych w danej jednostce organizacyjnej.

Podstawa prawna

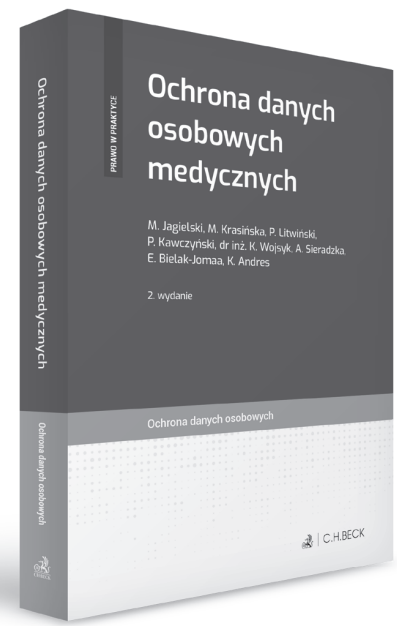
- art. 4 ust. 1, art. 5, art. 14, art. 19, art. 21 ust. 4 pkt 1, art. 22 ust. 1 pkt 2 lit. a), art. 23 ust. 2 pkt 1, art. 181 ustawy z 5.8.2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2018 r. poz. 412 ze zm.)
- załącznik nr 1, 2, 3 do rozporządzenia Prezesa Rady Ministrów z 28.12.2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (t.j. Dz.U. z 2015 r. poz. 205 ze zm.)

C.H.BECK

Ochrona danych osobowych medycznych

Uwzględnia specyfikę przetwarzania danych medycznych, które jako dane wrażliwe podlegają wielu ograniczeniom.

- Zasady przetwarzania danych osobowych i biometrycznych z uwzględnieniem nowej ustawy o ochronie danych osobowych.
- Nowe sankcje za nieprawidłowe przetwarzanie danych wrażliwych.
- Opisy procedur.



www.ksiegarnia.beck.pl | 22 311 22 22

Schemat różnic w nadawaniu uprawnień do dostępu do informacji niejawnych