SPIS TREŚCI

Aktualności

Ochrona danych osobowych

Opinie

Odpowiedzi na pytania

Wzór dokumentu

Schematy postępowań

Orzecznictwo

Dostęp do informacji publicznej

Opinie

Odpowiedzi na pytania

Wzór dokumentu

Schematy postępowań

Orzecznictwo

Tajemnice ustawowo chronione

Odpowiedzi na pytania

Schematy postępowań

informacja W ADMINISTRACJI PUBLICZNEJ

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

Cena: 110 zł w tym 5% VAT

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

Kamila Kędzierska
Redaktor naczelna

Szanowni Państwo,

chociaż lato i czas odpoczynku nadal w pełni, Redakcja Czasopisma Informacja w Administracji Publicznej nie ustaje w wysiłkach, by oddać w Państwa ręce kolejny numer kwartalnika, na łamach którego tradycyjnie przekazujemy najnowsze informacje dotyczące ochrony danych osobowych i tajemnic ustawowo chronionych, a także dostępu do informacji publicznej.

Aktualności koncentrują się na przepisach nowelizujących Kodeks postępowania administracyjnego oraz Prawo o postępowaniu przed sądami administracyjnymi – nasi specjaliści wskazują na te elementy znowelizowanych przepisów, które będą miały wpływ na przebieg postępowania o udostępnienie informacji publicznej.

Dział poświęcony ochronie danych osobowych otwierają teksty poświęcone zmianom w stosowaniu przepisów o ochronie danych osobowych, na jakie należy się przygotować w związku z rozpoczęciem stosowania w 2018 r. rozporządzenia ogólnego o ochronie danych osobowych. Nasi specjaliści wskazują na perspektywy współpracy Generalnego Inspektora Ochrony Danych Osobowych i Administratorów Bezpieczeństwa Informacji, a ponadto omawiają sposoby przygotowania jednostki do stosowania nowych przepisów, także w zakresie procedury identyfikowania i analizowania incydentów bezpieczeństwa informacji. Prezentujemy Państwu także szczegółowo omówiony schemat postępowania z wnioskiem o udzielenie informacji o przetwarzanych przez administratora danych osobowych. Zamieszczamy ponadto odpowiedzi na pytania Czytelników, dotyczące pozycji i zadań inspektora ochrony danych osobowych w jednostkach administracji oraz dokumentacji przetwarzania danych osobowych.

W ramach problematyki dostępu do informacji publicznej nasi eksperci podejmują zagadnienia związane z nowymi instytucjami wprowadzonymi w czerwcu 2017 roku do Kodeksu postępowania administracyjnego i ich wpływem na udostępnienie informacji publicznej. Publikujemy także aktualne informacje dotyczące rozwoju Centralnego Repozytorium Informacji Publicznych – portalu DanePubliczne.gov.pl. Przedstawiamy także tekst omawiający szczegółowo pojęcie osoby pełniącej funkcję publiczną. Prezentujemy również kolejny schemat – tym razem w zakresie bezwnioskowego trybu dostępu do informacji publicznej. W ramach tego działu przedstawiamy także najnowsze orzecznictwo w zakresie wzajemnego stosunku ustawy o dostępie do informacji publicznej oraz ustawy o ponownym wykorzystywaniu informacji sektora publicznego.

Dział poświęcony ochronie tajemnic ustawowo chronionych zawiera obszerne omówienie schematu postępowania z niejawną korespondencją przychodzącą i wychodzącą oraz prezentację orzecznictwa sądowego w zakresie ograniczenia dostępu do informacji niejawnych zawartych w aktach sprawy administracyjnej. Tradycyjnie Autorzy odpowiadają na nadesłane do Redakcji pytania – o udostępnianie protokołu z kontroli przedsiębiorcy oraz numeru rachunku bankowego przedsiębiorcy.

Zachęcam do wnikliwej lektury najnowszego numeru czasopisma i kierowania do Redakcji pytań w interesujących Państwa kwestiach związanych z szeroko pojętą informacją w administracji publicznej.

Kamila Kędzierska

Temat numeru

Nowa ustawa o ochronie danych osobowych – projekt

W dniu 14.9.2017 r. zostały opublikowane projekty nowej ustawy o ochronie danych osobowych (NUODO) wraz z projektem przepisów wprowadzających, które ustanawiają zmiany w ponad 130 ustawach. Oznacza to, że Ministerstwo Cyfryzacji zdecydowało się wdrożyć prawo unijne, kompleksowo, we wszystkich sektorach. Odeszło tym samym od praktyki innych państw członkowskich UE, w których najpierw udostępniane są ustawy o ochronie danych osobowych, a dopiero w dalszej kolejności podejmowane są prace zmieniające przepisy szczególne.

Nowa ustawa o ochronie danych osobowych

Podejście zaprezentowane przez resort ma dużo plusów. Najważniejszym jest nadanie nowego kierunku całemu systemowi ochrony danych osobowych w Polsce i wskazanie od razu zmian w przepisach sektorowych, co jest szczególnie istotne dla przedsiębiorców – umożliwia przygotowanie się do nowych regulacji już teraz. Poważnym ryzykiem takiej decyzji, jest jednak możliwość znacznego wydłużenia procesu legislacyjnego, co może opóźnić wejście w życie krajowych regulacji. Procesowanie ustawy o ochronie danych osobowych oddzielnie, względem zmiany 133 ustaw sektorowych, bez wątpienia przyśpieszyłoby przyjęcie tej pierwszej.

Trzeba oddać projektodawcy, że podszedł do zagadnienia europejskiej reformy danych osobowych rzetelnie i kompleksowo. Co prawda projekt ukazał się z opóźnieniem, bo według zapowiedzi Ministerstwa Cyfryzacji w czasie publikacji pierwszego projektu NUODO, pełny projekt miał być dostępny w okolicach czerwca 2017 r., a jesienią trafić do Sejmu. Z uwagi na poddanie projektu przepisów konsultacjom społecznym oraz uzgodnieniom międzyresortowym, treść projektowanych zmian na pewno ulegnie jeszcze mniejszym lub większym zmianom. Znamy już jednak kierunek podejścia polskiego ustawodawcy do reformy. W naszej ocenie projektodawca bardzo rzetelnie podszedł do wyzwania jakim jest wdrożenie RODO i po analizie przepisów NUODO wydaje się, że nie przekroczył kompetencji przyznanej państwom członkowskim.

Wyłączenia spod zakresu obowiązywania NUODO

Przepisy unijne zawarte w RODO przyznają państwom członkowskim swobodę w ograniczeniu stosowania przepisów względem niektórych sektorów. Z rozwiązania takiego skorzystał polski projektodawca, wyłączając zastosowanie ustawy względem:

1) działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych;
2) działalności literackiej;
3) działalności artystycznej;
4) wypowiedzi akademickiej.

Zgodnie z uzasadnieniem projektu NUODO, wyżej wymienione wyłączenia mają pierwszeństwo przed regulacjami RODO, o ile korzystanie z nich nie narusza istotnie praw lub wolności podmiotu danych – np. poprzez wykorzystanie danych faktycznie w innym celu niż wskazana twórczość dziennikarska, artystyczna lub literacka. Do wskazanych powyżej rodzajów działalności wyłączono tym samym stosowanie art. 13, art. 15 ust. 34, art. 18, art. 27 ust. 210 oraz art. 30 Rozporządzenia – czyli obowiązki administratora danych w zakresie:

1) informowanie osoby, której dane dotyczą o danych pozyskanych od tej osoby (art. 13),
2) dostarczania osobie, której dane dotyczą kopii danych (art. 15 ust. 3 oraz ust. 4),
3) ograniczenia przetwarzania na wniosek osoby, której dane dotyczą (art. 18),
4) wyznaczania swojego przedstawiciela w UE w przypadku, o którym mowa w art. 3 ust. 2 Rozporządzenia (art. 27 RODO – podmioty niemające jednostek organizacyjnych w UE przetwarzające),
5) powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu na podstawie umowy lub innego instrumentu prawnego (art. 28),
6) prowadzenia rejestru czynności przetwarzania danych osobowych (art. 30).

Zgodnie z art. 2 NUODO do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych, działalności literackiej oraz działalności artystycznej, nie będzie się stosowało następujących przepisów Rozporządzenia:

- 5 – zasady przetwarzania danych osobowych,
- 6 – przesłanki legalności przetwarzania danych osobowych,
- 7 – warunki wyrażania zgody przez osobę, której dane dotyczą,
- 8 – warunki wyrażania zgody przez dziecko w przypadku usług społeczeństwa informacyjnego,
- 9 – przetwarzanie szczególnych kategorii danych,
- 11 – przetwarzanie danych osobowych osoby niewymagającej identyfikacji,
- 14 – obowiązek podawania informacji w przypadku pozyskiwania danych nie od osoby, której dane dotyczą,
- 15 ust. 1 i 2 – prawo dostępu przysługujące osobie, której dane dotyczą,
- 16 – prawo do sprostowania danych,
- 19 – obowiązek powiadomienia odbiorcy danych o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,
- 20 – prawo do przenoszenia danych,
- 21 – prawo do sprzeciwu,
- 22 – zautomatyzowane podejmowanie decyzji w indywidualnych sprawach, w tym profilowanie.

Ochrona danych osobowych dzieci

Projektodawca NUODO, skorzystał z kompetencji przyznanej mu na mocy art. 8 ust. 1 RODO ustalając, że w wypadku realizacji usług internetowych, dzieci do lat 13 będą musiałby uzyskać zgodę rodzica na przetwarzanie ich danych (alternatywnie potwierdzenie przez rodzica zgody dziecka). Założeniem przyświecającym projektodawcy, jest jak się wydaje wyrównanie granicy wiekowej, gdy taka zgoda jest konieczna, z wynikającą z Kodeksu cywilnego granicą wiekową, gdy nabywa się ograniczoną zdolność do czynności prawnych. Jednak powstają pytania: w jaki sposób powinno się weryfikować tożsamość rodziców? Co stanie się ze zgodami, gdy osoba skończy 13 lat? Czy powinny być ponownie potwierdzane? Przepisy nie wskazują również, czy w razie cofnięcia zgody, może to zrobić dziecko samodzielnie, czy jej cofnięcie również wymaga aktywności rodzica.

Inspektorzy ochrony danych

W rozdziale 2 NUODO uregulowano warunki oraz tryb wyznaczania inspektorów ochrony danych osobowych (IOD), czyli nowych podmiotów, o kompetencjach zbliżonych do dzisiejszych Administratorów Bezpieczeństwa Informacji (ABI). W rozdziale określono w jakim terminie należy dokonać zgłoszenia inspektora ochrony danych organowi. Powinna być ona dokonana w terminie 14 dni od dnia wyznaczenia inspektora ochrony danych – w takim samym czasie informujemy o każdej zmianie danych, w tym o odwołaniu IOD. Projektodawca NUODO postanowił wprowadzić do projektu szeroką definicję podmiotów publicznych odnosząc się do definicji wskazanych w art. 5 § 2 pkt 3 ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (KPA), oraz podmioty publiczne wskazane w art. 9 ustawy z 27.8.2009 r. o finansach publicznych. Wskazana definicja nie powinna nastręczać wątpliwości interpretacyjnych i jest również rozwiązaniem racjonalnym i systemowo spójnym. Są nimi niemal wszystkie podmioty realizujące zadania publiczne z wyłączeniem spółek skarbu państwa oraz instytutów badawczych.

Prezes Urzędu Ochrony Danych Osobowych

NUODO wprowadza kluczową zmianę w zakresie funkcjonowania organu odpowiedzialnego za przestrzeganie przepisów o ochronie danych osobowych. Wraz z początkiem obowiązywania RODO, Generalny Inspektor Ochrony Danych Osobowych zostanie zastąpiony nowym organem jakim będzie Prezes Urzędu Ochrony Danych Osobowych (PUODO), który będzie swoje zadania realizował przy pomocy Urzędu Ochrony Danych Osobowych (UODO). PUODO będzie tym samym organem nadzorczym w rozumieniu RODO i „dyrektywy policyjnej".

Z uzasadnienia NUODO możemy odczytać, że wraz z początkiem obowiązywania RODO uchylona zostanie podstawa prawna działania GIODO. Nowy organ nadzorczy, z prawnego punktu widzenia, jest nowym organem państwowym, będącym następcą prawnym Generalnego Inspektora. Nazwa nowego organu również nie jest przypadkowa. Z uwagi na wprowadzenie w Rozporządzeniu funkcji inspektora ochrony danych osobowych, pozostawienie nazewnictwa organu w postaci Generalnego Inspektora Ochrony Danych Osobowych mogłoby wprowadzać w błąd w zakresie powiązania IOD (powołanych przez administratorów danych) z organem nadzorczym.

Procedura powołania PUODO jest zbliżona do powołania GIODO, ale oczywiście zawiera nowe rozwiązania. W stosunku do obowiązującej ustawy zmieniono kryteria, jakie powinien spełniać kandydat na Prezesa UODO. Zgodnie z art. 20 ust. 4 na stanowisko Prezesa UODO może być powołana osoba, która spełnia następujące warunki:

1) jest obywatelem polskim;

2) posiada tytuł naukowy doktora;
3) posiada wiedzę z zakresu ochrony danych osobowych;
4) przez okres co najmniej 5 lat wykonywała czynności bezpośrednio związane z ochroną danych osobowych;
5) korzysta z pełni praw publicznych;
6) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.

Warto wspomnieć o tym, że PUODO będzie mógł wykonywać swoje zadania przy pomocy trzech zastępców, powoływanych i odwoływanych przez Prezesa Rady Ministrów na wniosek ministra spraw wewnętrznych (jeden zastępca) oraz przez ministra cyfryzacji (dwóch zastępców). Jest to o tyle ciekawa konstrukcja, że na gruncie NUODO, w porównaniu do UODO, zwiększono niezależność PUODO poprzez przyznanie mu między innymi kompetencji do samodzielnego nadania statutu Urzędowi Ochrony Danych Osobowych (obecnie robi to Prezydent w formie rozporządzenia). Ponadto, przy Prezesie UODO działać będzie Rada do spraw Ochrony Danych Osobowych, w skład której wchodzić będzie 8 członków. Do zadań Rady zgodnie z art. 34 NUODO należeć będzie:

1) opiniowanie projektów dokumentów organów i instytucji UE dotyczących spraw ochrony danych osobowych;
2) opiniowanie przekazanych przez PUODO projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych;
3) opracowywanie propozycji kryteriów certyfikacji, o których mowa w art. 7;
4) opracowywanie propozycji rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych;
5) inicjowanie działań w obszarze ochrony danych osobowych oraz przedstawianie PUODO propozycji zmian prawa w tym obszarze;
6) wyrażanie opinii w sprawach przedstawionych Radzie przez PUODO;
7) wykonywanie innych zadań zleconych przez PUODO.

Powyższe wskazuje, że praca Rady do spraw Ochrony Danych Osobowych będzie dostarczała nam dużo informacji, które administratorzy będą mogli wykorzystać już na etapie systemów służących do przetwarzania danych jak również w codziennej działalności.

Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

Z projektu NUODO dowiadujemy się jak będzie wyglądało postępowania prowadzone przez PUODO. Będzie ono jednoinstancyjne i prowadzone w oparciu o przepisy KPA. NUODO wyposaża Prezesa UODO w szereg kompetencji kontrolnych takich jak:

1) prawo dostępu do wszelkich informacji niezbędnych do przeprowadzenia postępowania (z ograniczeniem w zakresie tajemnic prawnie ustawowo chronionych np. tajemnica radcowska, adwokacka);
2) możliwość żądania przedstawienia dowodów przez stronę oraz wykonanych na koszt kontrolowanego tłumaczeń dokumentów na język polski;
3) możliwość nałożenia grzywny za nieuzasadnione, niestawiennictwo jako świadek lub biegły oraz za bezzasadną odmowę zeznań, okazanie przedmiotu oględzin albo udziału w innej czynności urzędowej;
4) możliwość zobowiązania podmiotu, któremu zarzucane jest naruszenie danych osobowych, do ograniczenia przetwarzania danych, jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy, a dalsze ich przetwarzania może spowodować poważne i trudne do usunięcia skutki.

Decyzje PUODO będą podlegały natychmiastowemu wykonaniu. Ale co ważne, w projekcie przewidziano, że wniesienie przez stronę skargi do sądu, wstrzymuje wykonanie w odniesieniu do administracyjnej kary pieniężnej. Można dopatrzyć się w tym zakresie wątpliwości wyłącznie w zakresie celu wprowadzenia do projektu takiej regulacji. Zgodnie bowiem z art. 108 § 1 KPA, rygor natychmiastowej wykonalności może być nadany decyzji, od której służy odwołanie. W przypadku decyzji, od której odwołanie nie przysługuje – jak w projekcie Ministra Cyfryzacji – rygor taki nadawany jest więc z mocy samego prawa. Przepis pełni więc funkcję informacyjną.

Postępowanie kontrolne

Do NUODO wprowadzony został przepis dotyczący przeprowadzenia przez PUODO postępowania kontrolnego. Postępowania kontrolne prowadzone będą wg planu kontroli, na podstawie przeprowadzonych przez Prezesa UODO analiz, oraz na podstawie uzyskanych przez PUODO informacji – czyli w reakcji na tzw. donos. Zgodnie z art. 52 NUODO postępowanie kontrolne może być prowadzone również w toku postępowania w sprawie naruszenia przepisów o ochronie danych osobowych (uregulowanego w rozdziale 5 NUODO). Kontroli będą dokonywać upoważnieni pracownicy Urzędu Ochrony Danych Osobowych, którzy zostali wyposażeni w szereg kompetencji takich jak:

1) wstęp na grunt oraz do budynków, lokali lub innych pomieszczeń;
2) wgląd do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli;

3) przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
4) żądanie złożenia pisemnych lub ustnych wyjaśnień oraz wezwanie i przesłuchanie w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
5) możliwość przesłuchania w charakterze świadka pracowników kontrolowanego.

Postępowanie kontrolne nie może trwać dłużej niż miesiąc. Zgodnie z art. 74 NUODO postępowanie kontrolne rozpoczyna okazanie legitymacji i upoważnienia kontrolującego, a kończy podpisanie protokołu kontrolnego (art. 74 ust. 2 NUODO).

Postanowienie zabezpieczające

Projekt przewiduje uprawnienie Prezes UODO do wydania postanowienia zabezpieczającego skargę za naruszenie przepisów o ochronie danych. Prezes będzie mógł do momentu rozstrzygnięcia sprawy i wydania decyzji wydać postanowienie nakazujące przedsiębiorcy ograniczenie przetwarzania danych np. do ich posiadania. To znaczne wzmocnienie praw obywateli – będą mogli uzyskać natychmiastową ochronę swoich praw, i rozwiązanie mogące ogromnie wpłynąć na przedsiębiorców.

Odpowiedzialność cywilna i karna oraz administracyjne kary pieniężne

Projekt przewiduje trzy odrębne ścieżki dochodzenia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych. Co szczególnie ważne, każda z tych dróg może zostać wykorzystana niezależnie, a więc naruszenie będzie mogło być karane trzykrotnie – odpowiedzialność karna, cywilna i administracyjna.

Odnosząc się do odpowiedzialności administracyjnej, PUODO będzie uprawniony do nakładania administracyjnych kar pieniężnych na podstawie i warunkach określonych w art. 83 RODO. Kary będą nakładane w drodze decyzji administracyjnej. Projektodawca dokonał gruntownej zmiany względem projektu udostępnionego w marcu 2017 r. do konsultacji publicznej, przyznając PUODO uprawnienie do nakładania kary finansowej wobec wszystkich organów administracji publicznej. Z uwagi na obniżenie maksymalnego wymiaru kary nakładanej na administrację publiczną, projektodawca wzmocnił odpowiedzialność z tytułu naruszenia prywatności przez ten sektor poprzez nałożenie na niego obowiązku sprawozdawczego – każdy z adresatów decyzji wydawanych przez PUODO zobowiązany będzie do niezwłocznego wykazania sposobu ich wykonania. Administracyjne kary pieniężne będą stanowić dochód budżetu państwa, a ich 1% zasilał będzie nowo utworzony Fundusz Ochrony Danych Osobowych (FODO).

W przypadku, kiedy waga naruszeń jest znikoma, a strona zaprzestała naruszeń PUODO może udzielić upomnienia w drodze decyzji.

W projekcie znajduje się również możliwość dochodzenia roszczeń na drodze sądowej przed sądami cywilnymi (obok wszczęcia postępowania administracyjnego). Nie wyłącza to jednak możliwości jednoczesnego wystąpienia z roszczeniami z tytułu naruszenia przepisów NUODO wobec administratora danych osobowych. Praktyczne znaczenie tego uregulowania jest duże. Powołany przepis stanowi odrębną podstawę prawną dochodzenia roszczeń względem przewidzianej w art. 24 KC.

NUODO wprowadza obowiązek dla sądów o zawiadomieniu PUODO o każdym toczącym się postępowaniu, a także o każdym wyroku uwzględniającym powództwo w sprawach roszczeń cywilnych związanych z naruszeniem przepisów ochrony danych osobowych. Powyższe oznacza, iż podmiot danych będzie w stanie, na drodze cywilnej, uzyskać szeroką ochronę w razie naruszenia przepisów o ochronie danych.

W NUODO znalazły się również przepisy karne. Za udaremnienie lub utrudnienie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych grozi grzywna nakładana w parciu o przepisy Kodeksu postępowania w sprawach o wykroczenia; za przetwarzanie tzw. danych wrażliwych (art. 9 RODO) bez podstawy prawnej grozi grzywna, ograniczenie wolności lub pozbawienie wolności do roku – orzekane w trybie przepisów KK.

Podstawa prawna

- projekt z 12.9.2017 r. ustawy o ochronie danych osobowych, opublikowany na stronach Ministerstwa Cyfryzacji

Marek Kozica
Specjalista ds. Danych Osobowych
Aplikant radcowski Omni Modo

Tomasz Osiej
Radca Prawny. Firma doradcza
Omni Modo www.omnimodo.com.pl

Wywiad z dr. adw. *Pawłem Litwińskim* redaktorem naukowym komentarza do RODO

W związku z zakończeniem prac nad komentarzem do RODO, którego jest Pan redaktorem naukowym i który ukaże się na rynku w listopadzie tego roku, prosimy o przedstawienie naszym Czytelnikom eksperckich opinii dotyczących najbardziej nurtujących problemów.

Jak ocenia Pan zakres przygotowania administratorów danych do obowiązywania przepisów RODO?

Paweł Litwiński: Z tym bywa różnie. Duże podmioty z sektora prywatnego zazwyczaj są świadome nadchodzących zmian, a projekty wdrożenia RODO są w toku lub powoli zmierzają do końca, często jako projekty globalne. Wśród mniejszych podmiotów i, niestety, w części sektora publicznego implementacja RODO dopiero się zaczyna. A trzeba mieć świadomość tego, że np. niewielki startup, który przetwarza duże ilości danych o stanie zdrowia, może generować znacznie więcej problemów dla ochrony danych osobowych niż wielka firma produkcyjna. I od razu też trzeba podkreślić, że proces dostosowania do RODO w zasadzie nigdy się nie zakończy, a zapewnienie zgodności z RODO jest procesem dynamicznym, wymagającym stałej uwagi i stałego uwzględniania zmieniającego się otoczenia prawnego, technicznego i społecznego. To, co robimy teraz, to dopiero początek, tworzenie ram dla stałego zapewniania zgodności z RODO.

Jakie zadania, Pana zdaniem, wymagają najwięcej pracy ze strony administratorów danych w związku z RODO?

P.L.: RODO zrywa z 20-letnią praktyką znaną na gruncie ustawy o ochronie danych osobowych i rozporządzeń wykonawczych do niej, która sprowadzała proces zapewnienia zgodności z prawem do kilku czy kilkunastu konkretnych wymagań, które należało spełnić. Na gruncie RODO obowiązki, związane np. z zabezpieczeniem danych osobowych, sprowadzone zostały wyłącznie do ogólnej reguły, której wypełnienie pozostawiono już każdemu z podmiotów indywidualnie. I właśnie największą trudność – i najwięcej pracy – widzę w odniesieniu do takich obowiązków, co do których w RODO fundamentalnie zmienia się podejście. Wielkim problemem będą też obowiązki całkiem nowe, nieznane na gruncie dotychczasowych przepisów. Tutaj na pierwszy plan wybija się przeprowadzanie oceny skutków dla ochrony danych osobowych.

Jak zmienią się uprawnienia osób, których dane dotyczą?

P.L.: Uprawnienia podmiotów danych zmienią się dosyć radykalnie. Po pierwsze, pojawią się zupełnie nowe uprawnienia: prawo do przenoszenia danych i prawo do bycia zapomnianym. Po drugie, znane dotychczas uprawnienia – w szczególności uprawnienia o charakterze informacyjnym – ulegną zmianie co do treści i sposobu ich wykonywania. W przypadku każdego administratora danych powinno się dokonać przeglądu obecnie stosowanych procedur w tym zakresie i dostosować je do RODO, a także przygotować odpowiednie rozwiązania dla nowych uprawnień.

Jak zmieni się zakres obowiązków ABI, którzy 25.5.2018 r. zostaną powołani na stanowiska inspektów ochrony danych?

P.L.: Inspektorzy ochrony danych (IOD) z mocy prawa będą pełnić rolę punktu kontaktowego dla nowego organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych. Rola IOD będzie więc znacznie większa niż to jest obecnie, gdy mogą dokonywać na zlecenie GIODO sprawdzenia. Z drugiej strony, uwzględniając obowiązki IOD wynikające z RODO oraz ze względu na regułę *privacy by design*, IOD powinni być włączani we wszystkie procesy związane z przetwarzaniem danych osobowych. Z pewnością wzmocni to rolę IOD w organizacji.

Z jakimi konsekwencjami liczyć się muszą administratorzy danych, którzy nie zdążą wdrożyć nowych procedur przed 25.5.2018 r.?

P.L.: Przepisy RODO często sprowadzają się właśnie do konsekwencji, głównie finansowych, a to nie jest właściwe podejście. Oczywiście RODO przewiduje możliwość nakładania kar przez organ nadzorczy, ale skutki niewdrożenia RODO, to głównie skutki, których nie odczuje się od razu. Mam na myśli niedostosowanie organizacji do wymogów prawa, co będzie skutkować w przyszłości np. tym, że administratorzy danych nie będą mogli wykonywać żądań osób, których dane dotyczą – np. żądania przeniesienia danych, czy prawa do bycia zapomnianym. W rezultacie powstanie efekt kuli śniegowej i konsekwencje tego stanu rzeczy będą narastały.

Jakie najważniejsze zmiany należy poczynić w dotychczas prowadzonej dokumentacji przetwarzania danych, by zapewnić jej zgodność z RODO?

P.L.: Po pierwsze, trzeba ją zachować – i to mimo tego, że z RODO wprost nie wynika obowiązek prowadzenia dokumentacji. Po drugie, trzeba ją dostosować do RODO, czyli uwzględnić te nowe obowiązki, które właśnie z RODO wynikają. Szczegółowy zakres zmian zawsze jest wynikiem przeprowadzanego audytu.

Szczegółowe omówienie wszystkich poruszonych problemów, i nie tylko, znajdą Państwo w Komentarzu do Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, pod redakcją dr adw. *Pawła Litwińskiego*, autorstwa r.pr. *Pawła Barty* oraz dr adw. *Macieja Kaweckiego*.

Rekordowa liczba szkół w programie edukacyjnym GIODO

W roku szkolnym 2017/2018 w programie edukacyjnym GIODO dla szkół „Twoje dane – Twoja sprawa" będzie uczestniczyć blisko 340 placówek.

Dla przedstawicieli szkół 26 i 27.10.2017 r. Generalny Inspektor Ochrony Danych Osobowych (GIODO) zorganizował w Warszawie specjalne szkolenie, które oficjalnie zainaugurowało VIII edycję tego projektu.

Prawo i jego stosowanie w działalności szkoły

Pierwsza część spotkania poświęcona była przedstawieniu podstaw prawnych przetwarzania danych osobowych, ze szczególnym uwzględnieniem przepisów odnoszących się do sektora oświaty. Wykład wprowadzający w tematykę ochrony prywatności i danych osobowych wygłosił *Piotr Drobek*, zastępca dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej w Biurze GIODO. Z kolei szerzej o przepisach prawa regulujących przetwarzanie danych osobowych w sektorze oświaty mówiła kolejna ekspertka z Biura GIODO – *Barbara Gubernat*.

Osobne wystąpienie poświęcone było monitoringowi wizyjnemu w szkole. Zagadnienie to omówił *Paweł Makowski*, radca GIODO.

Pierwszy dzień spotkania zakończyły dwie prezentacje specjalistów, odnoszące się do zagadnień informatycznych. „Moja cyfrowa tożsamość – jak ją chronić, dlaczego warto i jak uczyć o ochronie danych osobowych?" to temat pierwszej z nich, przedstawionej przez *Grażynę Gregorczyk* reprezentującą Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie. Z kolei *Kamil Śliwowski* z Fundacji Katalyst Education, www. otwartezasoby.pl mówił o przyszłości w sprofilowanym świecie i o tym, jak przygotować się do niej w szkole.

Dobre praktyki

Drugi dzień szkolenia to warsztaty, podczas których prezentowane były konkretne projekty zrealizowane przez placówki oświatowe w czasie ubiegłorocznej edycji programu i nagrodzone w organizowanym przez GIODO konkursie na najlepszą inicjatywę edukacyjną.

Z kolei *Anna Janik*, nauczycielka od lat zaangażowana we współpracę przy Programie „Twoje dane – Twoja sprawa", prezentowała nową autorską inicjatywę. Wcześniejsza, wymyślona przez nią, Ogólnopolska Gra Planszowo-Edukacyjna nagrodzona przez GIODO w VI edycji programu i zaprezentowana podczas warsztatów otwierających VII jego edycję, spotkała się z tak dużym zainteresowaniem koordynatorów, że wielu z nich zdecydowało o włączeniu tej gry do programu swoich działań. Ostatecznie w roku szkolnym 2016/2017 w grze brały udział 34 placówki oświatowe. Nowe przedsięwzięcie spotkało się z równie życzliwym przyjęciem.

Spotkania warsztatowe były ponadto okazją do wymiany doświadczeń związanych zarówno z tym, jak w przystępny sposób uczyć dzieci zasad ochrony danych osobowych, jak i z tym, jak nauczyciele sami powinni postępować z danymi osobowymi uczniów i rodziców.

Wsparcie eksperckie

Podczas warszawskiego szkolenia czynny był też punkt konsultacyjny GIODO, w którym wszyscy zainteresowani mogli otrzymać informacje i porady dotyczące nurtujących ich problemów.

Ponadto każdy z uczestników spotkania otrzymał pakiet bezpłatnych materiałów edukacyjnych, w skład którego wchodzą: broszury informacyjne dotyczące zasad przetwarzania danych osobowych, scenariusze lekcji, prezentacje multimedialne i inne pomoce dydaktyczne ułatwiające realizację programu.

Temat numeru

Zgoda pracownika jako podstawa przetwarzania danych biometrycznych w RODO i w projekcie Przepisów wprowadzających ustawę o ochronie danych osobowych

dr hab., r. pr. Mariusz Krzysztofek
Director, Privacy Counsel – EMEA, Herbalife

Przetwarzanie danych pracowniczych w związku z zatrudnieniem należy do obszarów, w których RODO dopuszcza przyjęcie przez państwa członkowskie przepisów bardziej szczegółowych niż RODO (art. 88 RODO). Mogą one regulować przetwarzanie danych zwłaszcza do celów rekrutacji i wykonania umowy o pracę. Mimo przejścia od harmonizacji do ujednolicenia zasad ochrony danych w Unii Europejskiej, szczegółowe przepisy krajowe regulujące ich przetwarzanie w poszczególnych państwach członkowskich, nadal będą mogły się różnić w wybranych obszarach, ponieważ po pierwsze, nie wszystkie dziedziny podlegają prawu unijnemu, a po drugie, samo RODO dopuszcza odmienność regulacji krajowych we wskazanych w nim przypadkach. Jedną z tych dziedzin jest prawo pracy, a w jego ramach – zgoda pracownika jako podstawa przetwarzania danych, w tym również biometrycznych.

Projekt zmian w Kodeksie pracy z 12.9.2017 r. (projekt ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, opublikowany przez Ministerstwo Cyfryzacji) wprost dopuszcza przetwarzanie danych biometrycznych na podstawie zgody. Przestrzegam jednak przed traktowaniem tej podstawy jako wystarczającej i bezwarunkowej.

Korzystanie z danych biometrycznych przez pracodawców będzie na-

bierało coraz większego znaczenia wraz rosnącą popularnością tych technologii i spadkiem cen ich wdrażania. W szczególności, ale nie wyłącznie, w celu zabezpieczenia dostępu do chronionych pomieszczeń i urządzeń. Możliwość automatycznej identyfikacji ludzi na podstawie np. odcisków palców, układu naczyń krwionośnych, obrazu tęczówki oka lub głosu, zapewnia skuteczną ochronę przed dostępem osób nieuprawnionych, ale wiąże się z ryzykiem dla prawa do prywatności oraz dla innych praw i wolności.

Dotychczasowy stan prawny

Zgodę pracownika jako podstawę przetwarzania jego danych ponad zakres wskazany w ustawie, zakwestionował Naczelny Sąd Administracyjny w wyroku z 6.9.2011 r. (I OSK 1476/10, Legalis). Sąd podważył w tym wyroku zgodę pracownika jako podstawę do przetwarzania jego danych biometrycznych. Uznał wykorzystywanie odcisków palców do kontroli czasu pracy pracowników za nieproporcjonalne do tego celu przetwarzania. Zakwestionował również dobrowolność wyrażenia przez pracownika zgody, skoro do podstawowych cech stosunku pracy należy podporządkowanie pracownika pracodawcy. Skuteczność zgody osób, których dane dotyczą, wymaga pełnej swobody jej udzielenia i braku negatywnych konsekwencji odmowy.

Uzasadnieniem rozstrzygnięcia NSA było to, że w art. 22^1 § 1 i 2 ustawy z 26.6.1974 r. –Kodeks pracy (t.j. Dz.U. z 2016 r. poz. 166 zawarto zamknięty katalog danych osobowych, które może zbierać pracodawca. Artykuł 22^1 § 4 KP dopuszcza żądanie przez pracodawcę innych danych osobowych, jednak pod warunkiem, że obowiązek podania określonych danych wynika z odrębnych przepisów. Przyjęcie zgody jako podstawy przetwarzania danych nie uwzględniałoby więc ograniczenia kategorii danych osobowych, których przetwarzanie przez pracodawcę jest dopuszczalne na podstawie art. 22^1 KP[1].

Artykuł 22^1 § 5 KP odsyła do OchrDanychU w zakresie nieuregulowanym w art. 22^1 § 1–4 KP, jednak przepisy OchrDanychU nie są *lege speciali* w stosunku do art. 22^1 KP. Relacja między tymi przepisami jest odwrotna. To art. 22^1 KP, określając zamkniętą listę danych osobowych, których przetwarzanie przez pracodawcę jest dopuszczalne, jest przepisem szczególnym wobec zasady adekwatności. Rozszerzenie na podstawie zgody pracownika katalogu danych osobowych ponad zakres określony w art. 22^1 § 5 KP jest naruszeniem zasady adekwatności.

Zmiana stanu prawnego – wprowadzenie zgody pracownika jako podstawy przetwarzania

Projekt zmian w KP, będący elementem projektu przepisów wprowadzających ustawę o ochronie danych osobowych opublikowanego przez Ministerstwo Cyfryzacji, nie likwiduje zamkniętego katalogu danych osobowych, które może zbierać pracodawca (art. 22^1 § 1 i 2 KP), jednak w nowym art. 22^2 § 2 KP dopuszcza przetwarzanie danych biometrycznych (a nie należą do tego katalogu) na podstawie zgody pracownika. Nie należy jednak traktować zgody jako nowej podstawy do przetwarzania danych pracowniczych w oderwaniu od kluczowych zasad ochrony danych – proporcjonalności danych do celu przetwarzania i dobrowolności zgody.

Proporcjonalność korzystania z danych biometrycznych w stosunkach pracy

Projekt zmian w KP wymaga, aby zakres przetwarzania tych danych nie wykraczał poza dane osobowe pracownika dotyczące stosunku pracy.

ORZECZENIE

NSA w wyroku z 6.9.2011 r. (I OSK 1476/10, Legalis); dopuścił wykorzystywanie odcisków palców do kontroli dostępu do pomieszczeń chronionych, ale korzystanie z tych danych do kontroli czasu pracy pracowników uznał za nieproporcjonalne do tego celu przetwarzania. Podkreślił, że zgoda, nawet jeżeli w konkretnym przypadku dobrowolna, co pracodawca mógł wykazać, nie unieważnia zasady adekwatności i nie może rozszerzyć zakresu danych dopuszczonego wprost w ustawie. W dotychczasowym stanie prawnym sama zgoda nie mogła więc być podstawą przetwarzania danych biometrycznych, ale i np. danych o karalności pracownika.

Należy więc ustalić, czy wprowadzenie zgody jako podstawy przetwarzania danych biometrycznych pracowników oraz ograniczenie jej do zakresu dotyczącego stosunku pracy, pozwala na stosowanie tych danych do każdego celu, czy tylko do niektórych.

PRZYKŁAD

Czy akceptowalne będzie tylko zabezpieczanie dostępu do krytycznych systemów i pomieszczeń przez autoryzację z wykorzystaniem danych biometrycznych (z pewnością tak), czy również ewidencja czasu pracy (a ten właśnie cel został zakwestionowany w powyższym wyroku przez sąd, a wcześniej przez GIODO), a może wręcz nawet takie cele, jak monitorowanie jakości pracy biurowej? Uważam, że należy odrzucić podejście, jakoby zgoda mogła być podstawą przetwarzania danych biometrycznych niezależnie od celu.

Moim zdaniem, trzeba tu przywołać zasadę proporcjonalności zakresu danych do celu przetwarzania i uznać,

[1] *E. Kulesza*, Przesłanki przetwarzania danych osobowych pracowników przez pracodawcę, MoP 2012, Nr 7 – dodatek specjalny „Ochrona danych osobowych 2012", s. 30; *T. Wyka*, Rola Kodeksu pracy w systemie przepisów dotyczących ochrony danych osobowych pracownika (w:) Internet. Prawno-informatyczne problemy sieci, portali i e-usług, pod red. *G. Szpor*, *W. Wiewiórowskiego*, Warszawa 2012, s. 59; *G. Sibiga*, Przetwarzanie i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy, Radca Prawny 2005, Nr 2, s. 67.

że zgoda jej nie niweczy. Analogicznie – nowy art. 22^4 § 1 KP – dopuszczający monitoring wizyjny, ogranicza go do zapewnienia bezpieczeństwa pracowników lub ochrony mienia albo zachowania m.in. tajemnicy przedsiębiorstwa i wyklucza stosowanie tego środka do kontroli wykonywania pracy przez pracownika. Monitoring wizyjny nie jest środkiem bardziej ingerującym w prywatność niż monitoring z wykorzystaniem biometrii, więc należy – moim zdaniem – przyjąć, że analogiczne ograniczenie celów i proporcjonalność stosowanych środków są tu wymogiem.

Kiedy więc dane biometryczne pracownika dotyczą stosunku pracy, a korzystanie z nich jest proporcjonalne i nie jest nadmiernie inwazyjne, nie narusza prawa do prywatności i godności pracownika?

Ocena zawsze będzie zindywidualizowana, musi odnosić się do konkretnych okoliczności. Co więcej, zasada pozostanie stała, jednak jej interpretacja będzie ulegać ewolucji wynikającej z postępu technologicznego, także w kontekście społecznej akceptacji nowych praktyk w stosunkach pracy, a ponadto należy wziąć pod uwagę cel i jego wagę.

PRZYKŁAD

Elektroniczny monitoring temperatury ciała, czy częstotliwości mrużenia oczu mogą zapobiegać wypadkom spowodowanym zmęczeniem, więc zyskają aprobatę społeczną, gdy zostaną zastosowane w transporcie publicznym. Jednak technologie tego rodzaju mogą stać się też narzędziem inwigilacji, gdy zaczną służyć np. automatycznej analizie aktywności pracowników biurowych.

Potwierdzeniem tego podejścia do adekwatności danych w związku z zatrudnieniem jest również, przez analogię, projekt nowego przepisu Prawa bankowego (art. 13c ust. 2), który pozwala bankom żądać od pracowników danych biometrycznych, w szczególności odcisków palców, głosu, obrazu rogówki i sieci żył palców (ten katalog będzie ewoluował wraz z nowymi technologiami i ich dostępnością), jeżeli podanie takich danych jest konieczne ze względu na kontrolę dostępu do informacji przetwarzanych przez bank i pomieszczeń.

Dobrowolność zgody

Kolejnym czynnikiem wpływającym na dopuszczalność przetwarzania danych biometrycznych pracownika na podstawie jego zgody jest jej dobrowolność. Również obecnie KP nie wyklucza przetwarzania danych na podstawie zgody (choć nie w każdym przypadku – w szczególności nie danych o wyrokach karnych i danych biometrycznych, które mają szczególny charakter; zgoda może natomiast być podstawą do np. publikacji zdjęć pracowników w Internecie), jednak musi ona spełniać warunek dobrowolności. Dobrowolność jest kluczowym warunkiem ważności zgody, a motyw 155 RODO i nowy art. 22^2 § 2 KP, dopuszczający zgodę pracownika, nie usuną wątpliwości, czy zgoda kandydata do pracy lub pracownika jest w konkretnym przypadku dobrowolna.

Do podstawowych cech stosunku pracy należy podporządkowanie pracownika pracodawcy, udzielenie zgody przez pracownika na wniosek pracodawcy może następować w rzeczywistości pod nieformalną presją, dobrowolność wyrażenia przez pracownika zgody może więc zostać zakwestionowana. Skuteczność zgody osób, których dane dotyczą, wymaga pełnej swobody jej udzielenia i braku negatywnych konsekwencji odmowy.

Ważne

Projekt nowego art. 22^2 § 3 KP odnosi się do tego przez zastrzeżenie gwarancji, że brak zgody nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, w szczególności nie może uzasadniać odmowy zatrudnienia, wypowiedzenia stosunku pracy lub jego rozwiązania bez wypowiedzenia przez pracodawcę.

Rezerwę w podejściu do zgody jako podstawy przetwarzania danych pracowniczych, ze względu na ryzyko braku dobrowolności, zaleca Grupa Robocza Art. 29 (Opinia Grupy Roboczej 2/2017 z 8.6.2017 r. w sprawie przetwarzania danych osobowych w pracy, która uzupełnia wcześniejszą opinię Grupy Roboczej 8/2001 z 13.9.2001 r. w sprawie przetwarzania danych osobowych w kontekście zatrudnienia)[2].

ORZECZENIE

NSA orzekł analogicznie w wyroku z 1.12.2009 r. (I OSK 249/09, Legalis), podkreślając, że brak równowagi w relacji pracodawca – pracownik stawia pod znakiem zapytania dobrowolność wyrażenia zgody na pobieranie i przetworzenie danych osobowych (biometrycznych).

Rezerwa nie oznacza jednak, że dobrowolność zgody jest wykluczona. Dla oceny istotne są faktyczne okoliczności konkretnego przypadku. Po pierwsze, ustawodawca unijny zrezygnował w RODO (motyw 34 preambuły) z pierwotnego stwierdzenia, że stosunek zależności i wyraźny brak równowagi występuje w relacjach zatrudnienia i wpływa na dobrowolność, a więc ważność zgody pracownika. A jedno-

[2] Opinion 2/2017 adopted on 8 June 2017 on data processing at work, WP 249, s. 3 i 4: „Consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence", "It is important to state that employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship".

cześnie wprowadził motyw 155 preambuły, który z zastrzeżeniem wskazanych tu warunków, dopuszcza zgodę pracownika jako podstawę przetwarzania danych.

Po drugie, już obecnie KP przewiduje zgodę pracownika, a więc zakłada jej dobrowolność, ponieważ jest ona podstawowym warunkiem ważności oświadczenia woli (np. zgoda na potrącenie należności z wynagrodzenia pracownika – art. 91 § 1 KP, zgoda pracownicy w ciąży i pracownika opiekującego się dzieckiem do ukończenia przez nie 4. roku życia na pracę w określonym systemie czasu pracy – art. 178 § 1 i 2 KP).

Treść prób o zgodę

Ważna więc będzie treść próśb o zgodę – klarowne poinformowanie pracownika m.in. o celu zgody i jej dobrowolności, równie ważna będzie treść klauzul zgody. Ale przede wszystkim sfera faktyczna – wykazanie, że sama odmowa zgody na stosowanie biometrii nie spowodowała np. dyskryminacji w ustalaniu rocznych premii, czy w zakresie zadań pracownika. Jednak całkowity brak negatywnych skutków odmowy zgody może okazać się nieunikniony, jeżeli będzie wynikał z braku możliwości objęcia pracownika udogodnieniami, które zależały od jego zgody.

PRZYKŁAD

Gdy celem pracodawcy będzie skrócenie czasu oczekiwania pracowników na wejście i wyjście z firmy przez wprowadzenie bramek otwierających się po przyłożeniu palca, pracownicy którzy nie zostaną objęci tym systemem mogą być narażeni na opóźnienia wynikające np. z szukania w teczce karty magnetycznej przez osobę stojącą przed nimi w kolejce. To praktyczny problem, np. w instytucjach, które zatrudniają setki osób rozpoczynających i kończących pracę o tej samej porze.

Zgoda na przetwarzanie danych biometrycznych w firmach outsourcingowych

Ilustracją problemów interpretacyjnych dotyczących dobrowolności zgody jest dopuszczalność wskazania zgody jako warunku zatrudnienia przez firmę outsourcingową obsługującą zleceniodawców, którzy wdrożyli biometrię jako jedyny sposób uzyskania dostępu do biur. Wprawdzie projekt nowego art. 22^2 § 3 KP wyklucza odmowę zatrudnienia motywowaną wyłącznie odmową zgody pracownika na przetwarzanie danych biometrycznych, a wymóg udzielenia zgody jako warunek zatrudnienia brzmi jak takie właśnie niedopuszczalne ultimatum, ale uważam, że nie można w tej ocenie pomijać tego, iż w tym przypadku brak zgody wyklucza zatrudnienie ze względu na brak możliwości wykonywania działalności przez firmę outsourcingową, a więc wyklucza samo utworzenie stanowiska pracy. Pracodawcą jest tu firma świadcząca usługi w ramach outsourcingu na rzecz np. firm zarządzających biurowcami lub właścicieli biurowców.

Podkreślenie w ofercie pracy opublikowanej przez firmę outsourcingową, że niezbędna jest akceptacja korzystania z danych biometrycznych, nie musi, moim zdaniem, kolidować z zasadą dobrowolności zgody w sytuacji, w której korzystanie z danych biometrycznych do kontroli dostępu do pomieszczeń chronionych nie jest kwestią redukcji kosztów czy usprawnień organizacyjnych po stronie pracodawcy, lecz decyduje o technicznej możliwości wykonywania podstawowej działalności firmy.

Pracodawca zarządzający dostępem do swoich pomieszczeń może (nie odnoszę się tu do celowości i kosztów) utrzymywać równolegle np. system dostępu wykorzystujący dane biometryczne, a dla osób, które nie wyraziły na to zgody – karty magnetyczne. Taka praktyka bywa obecnie stosowana. Jednak firma outsourcingowa, której działalność wymaga regularnego dostępu do pomieszczeń jej zleceniodawcy, a dostęp ten został przez zleceniodawcę w pełni oparty na danych biometrycznych, nie ma alternatywy.

Przedstawienie przez firmę outsourcingową przejrzystej i rzetelnej informacji wskazującej tę zależność może sprawić, że kandydat do pracy uzna ją za logiczną, jego zgoda będzie rzeczywiście dobrowolna i będzie wynikała ze zrozumienia sytuacji, a organ nadzorczy i sądy zaakceptują to podejście w takim kontekście.

▶ Podstawa prawna

- art. 88 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 (Dz.Urz. UE L Nr 119 z 4.5.2016 r., s. 1–88)
- art. 22^1 § 1 – 5 ustawy z 26.6.1974 r. – Kodeks pracy (t.j. Dz.U. z 2016 r. 1666 ze zm.)

Temat numeru

Dane pracowników udostępnione na etapie rekrutacji a zasada celowości – obecne i projektowane zmiany w Kodeksie pracy

Magdalena Korga

Magister prawa, ABI, doświadczony trener i praktyk, audytor z doświadczeniem w zakresie wdrażania systemów zarządzania bezpieczeństwem danych osobowych, od ponad 10 lat zajmuje się doradztwem prawnym w zakresie ochrony danych osobowych

Do przetwarzania danych osobowych kandydata do pracy dochodzi na etapie rekrutacji. Przez składane do potencjalnego pracodawcy dokumenty rekrutacyjne, takie jak życiorys oraz list motywacyjny, kandydaci przekazują swoje dane osobowe, które w trakcie dalszego procesu rekrutacyjnego są przetwarzane przez przyszłego pracodawcę.

Zgodnie z art. 26 ust. 1 pkt 2 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922; dalej: OchrDanychU), administrator danych osobowych jest zobowiązany zapewnić, aby dane były zbierane w oznaczonych, zgodnych z prawem celach i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

Ustawodawca dopuszcza przetwarzanie danych osobowych w innych celach niż ten, dla którego zostały zebrane, jeśli nie narusza to praw i wolności osób, których dane dotyczą oraz następuje:

1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych;
2) z zachowaniem przepisów art. 23 i 25 OchrDanychU.

Powyższe zapisy OchrDanychU warto rozważyć w odniesieniu do praktyki wykorzystywania prywatnych numerów telefonów pracowników, udostępnianych przez nich w życiorysach składanych pracodawcy na etapie rekrutacji. Jak wskazuje praktyka, w wielu organizacjach życiorysy i listy motywacyjne pracowników są przechowywane w aktach osobowych, a zawarte w nich dane dotyczące prywatnego numeru telefonu bywają wykorzystywane do bieżących potrzeb związanych z zatrudnieniem.

Ważne

Takie postępowanie jest niezgodne z obecnymi przepisami prawa – Kodeksem pracy oraz OchrDanychU.

Pracodawca bowiem pozyskuje numer telefonu na potrzeby rekrutacji, a wykorzystuje go na potrzeby zatrudnienia. Pracownik będący na etapie rekrutacji, udostępnił w życiorysie prywatny numer telefonu (czy adres e-mail) w określonym celu, jakim jest kontakt w związku z rekrutacją. Wyrażona przez kandydata zgoda na przetwarzanie tych danych osobowych obejmowała korzystanie z danych wyłącznie na potrzeby rekrutacji.

Przetwarzanie danych kontaktowych zawartych w życiorysie w innych celach niż rekrutacja (np. w celu komunikowania się z pracownikiem w związku z pełnionymi przez niego obowiązkami służbowymi) jest zatem naruszeniem zasady celowości, o której mowa w art. 26 OchrDanychU.

Projektowane zmiany Kodeksu pracy

Projektowane zmiany Kodeksu pracy zmienią obecną sytuację w odniesieniu do zakresu żądanych od kandydata do pracy danych. Projekt zmian z 12.9.2017 r. dotyczący Przepisów wprowadzających ustawę o ochronie danych osobowych zakłada, że zgodnie ze znowelizowanym art. 22^1 § 1 KP, pracodawca żąda podania przez osobę ubiegającą się o zatrudnienie danych osobowych obejmujących adres poczty elektronicznej albo numer telefonu. Katalog danych został sprecyzowany w taki sposób, w którym pracodawca żąda od kandydata do pracy podania jednej z dwóch danych osobowych – adresu poczty elektronicznej albo numeru telefonu. Podstawą prawną przetwarzania tych danych w przyszłości będzie zatem przepis prawa (art. 6 pkt 1c RODO), a nie zgoda kandydata.

Ważne

Z katalogu danych, których żądać może pracodawca od kandydata, usunięta została pozycja dotycząca podania danych osobowych obejmujących miejsce zamieszkania (zastąpione adresem do korespondencji) oraz imiona rodziców.

Warto podkreślić, że na podstawie art. 22^1 § 5 KP, według proponowanego na dzień 12.9.2017 r. brzmienia, przetwarzanie danych osobowych obejmujących adres do korespondencji i adres poczty elektronicznej albo numer telefonu już **po nawiązaniu stosunku** pracy będzie możliwe tylko w przypadku, gdy pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej.

Jak wynika z powyższego, zmiany Kodeksu pracy, które mają wejść z życie z 25.5.2018 r., prawdopodobnie zmienią obecną sytuację w odniesieniu do danych osobowych kandydatów do pracy oraz pracowników, pod warunkiem, że zostaną przyjęte w brzmieniu zaproponowanym w projekcie ustawy wprowadzającej ustawę o ochronie danych osobowych z dnia 12.9.2017 r.

Podstawa prawna

- art. 23, 26 ustawy z 29.8.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922)
- art. 5 przepisów wprowadzających ustawę o ochronie danych osobowych; projekt z 12.9.2017 r.

Temat numeru

Ochrona danych osobowych w szkole w związku z rozpoczęciem stosowania RODO oraz nowej ustawy o ochronie danych osobowych

Krzysztof Dzioba
Radca prawny, Ernst & Young Law Tałasiewicz, Zakrzewska i Wspólnicy spółka komandytowa

Angelika Kosińska
Prawnik, Ernst & Young Law Tałasiewicz, Zakrzewska i Wspólnicy spółka komandytowa

Rozpoczęcie stosowania RODO i nowej ustawy o ochronie danych osobowych wpłynie na obowiązki dyrektorów szkół. Placówki oświatowe przetwarzają bardzo szeroki katalog informacji realizując cele nie tylko o charakterze edukacyjnym. Rozdzielenie różnych kategorii danych jest konieczne w celu wyboru i wdrożenia prawidłowych narzędzi w celu ich ochrony. Niespełnienie nowych wymagań wiąże się z ryzykiem kar pieniężnych.

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 (Dz.Urz. UE L Nr 119 z 4.5.2016 r., s. 1–88) (dalej: RODO), jako jeden ze swoich celów przyjmuje ochronę danych osobowych dzieci.

Nie pozostaje to bez znaczenia dla oceny nowych, wynikających z RODO, obowiązków po stronie szkół oraz prowadzących je podmiotów, w tym samorządów. W praktyce placówki oświatowe mają prawo przetwarzać dane uznawane za dane wrażliwe nie tylko w odniesieniu do swoich podopiecznych, ale także w odniesieniu do ich rodziców.

Przetwarzanie danych przez placówki oświatowe

Przetwarzanie ww. danych osobowych podlega obecnie rygorom określonym ustawą z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922; dalej: OchrDanychU). Ustawa ta rozwija, zagwarantowane w art. 51 ustawy z 2.4.1997 r. – Konstytucji Rzeczpospolitej Polskiej (Dz.U. Nr 78, poz. 483 ze zm. i sprost.), prawo do ochrony danych osobowych, określając zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane. Określone w OchrDanychU zasa-

dy znajdą zastosowanie w odniesieniu do danych znajdujących się w kartotekach, dziennikach lekcyjnych, wykazach i innych systemach informatycznych danej placówki.

Ustawa o ochronie danych osobowych oprócz zwykłych danych, takich jak: imię, nazwisko, adres zamieszkania itp. wyodrębnia dane szczególne chronione, których zamknięty katalog został określony w art. 27 ust. 1 OchrDanychU i których przetwarzanie możliwe jest tylko w określonych przypadkach. Dotyczy to np. kwestii medycznych, rasowych czy światopoglądowych.

Od strony podmiotowej gromadzone przez szkoły informacje stanowią w główniej mierze dane osobowe dotyczące dzieci, ich rodziców oraz opiekunów prawnych, czy też nauczycieli i innych pracowników. Od strony przedmiotowej placówki oświatowe przetwarzają szerokie spektrum danych, poczynając od danych teleadresowych dziecka i rodziców, a kończąc na informacjach o przebytych przez dziecko chorobach.

Analizując przetwarzanie danych przez szkoły, na gruncie OchrDanychU, można więc wyróżnić kilka kategorii tych danych. Po pierwsze, intuicyjnie – kategorię obejmującą dane przetwarzane w celach czysto edukacyjnych, tj. w szczególności zbieranych, utrwalanych, przechowywanych i usuwanych do realizacji zadań oświatowych. Do tej kategorii należą np. przetwarzane na podstawie ustawy o systemie oświaty dane osobowe dzieci przyjętych bądź nieprzyjętych do szkoły, dane niezbędne do określenia wysokości pobranej dotacji, listy obecności czy listy uczestników wypoczynku organizowanego przez placówkę.

Druga kategoria danych wymaga szerszego spojrzenia na zadania stojące przed szkołą jako instytucją oświatowo-wychowawczą. Ich katalog będzie obejmował m.in.: informacje udostępnione szkolnej pielęgniarce, szkolnemu ochroniarzowi w zakresie monitoringu, czy portierowi w obrębie działalności szkolnego sekretariatu. Przetwarzanie tych danych nie jest bowiem bezpośrednio związane z realizacją celów edukacyjnych – stanowiących realizację obowiązków ustawowych placówki (w tym ustawy o systemie oświaty). Co za tym idzie, podstawy ich zbierania, dostęp do nich oraz ich zakres należy zbadać pod kątem istnienia innej podstawy przetwarzania danych, zgodnie z przepisami OchrDanychU.

OPINIA GIODO

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych, potwierdzające wnioski z Opinii 2/2009 Grupy Roboczej Art. 29 ds. Ochrony Danych w sprawie ochrony danych dzieci (Ogólne wytyczne i szczególny przypadek szkół) „dane o stanie zdrowia powinny być przetwarzane jedynie przez lekarzy lub te osoby, które »bezpośrednio« zajmują się uczniami jak nauczyciele czy inni pracownicy szkoły związani tajemnicą zawodową. Przetwarzanie tego typu danych może się odbywać na podstawie bądź to zgody przedstawicieli prawnych dzieci lub ze względu na żywotne interesy dziecka w nawiązaniu do życia szkolnego" (opinia z 11.2.2009 r.)[1].

Pielęgniarki nie są najczęściej pracownikami szkoły, a jedynie świadczą na jej terenie gwarantowaną uczniom i wychowankom profilaktyczną opiekę zdrowotną. W celu zagwarantowania prawidłowości realizowanych zadań, a także zgodności z przepisami dotyczącymi obowiązku istnienia prawidłowej podstawy przetwarzania danych, niezbędne jest doprecyzowanie celu realizowanych świadczeń oraz wzajemnych zobowiązań w zakresie ochrony danych. Dotyczy to również pracowników ochrony, portierów czy pracowników stołówki. Nie jest więc dopuszczalny swobodny przepływ tej kategorii danych pomiędzy osobami pracującymi lub świadczącymi usługi na rzecz szkoły.

Trzecią kategorią danych przetwarzanych przez szkoły są dane pracowników. Podstawę przetwarzania oraz katalog informacji określają w tym przypadku takie ustawy, jak Kodeks pracy czy Karta Nauczyciela.

Obowiązki w zakresie danych osobowych

Placówka oświatowa przetwarzająca dane powinna dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, zobowiązana jest do zapewnienia, aby dane były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

Ministerstwo Cyfryzacji w projekcie z 12.9.2017 r. ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych opublikowanym na swojej stronie internetowej[2], zaproponowało wprost w szeregu aktów prawnych dotyczących oświaty wprowadzenie postanowień, zgodnie z którymi dane osobowe [przetwarzane na podstawie tych ustaw] podlegałyby zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu i były przechowywane wyłącznie przez okres niezbędny do realizacji zadań.

Powyższe stanowi realizację założeń RODO (m.in. Motyw 71 i 74 RODO), które w miejsce jasnych wytycznych dotyczących metod ochrony przetwarzanych danych wprowadza obowiązek stosowania rozwiązań adekwatnych. Warto zwrócić uwagę, że na konieczność stosowania przy przetwarzaniu danych osobowych, tzw. zasady adekwatności, wskazał już w 2005 r. Wojewódzki Sąd Administracyjny, który orzekł, iż:

[1] http://www.giodo.gov.pl/pl/259/2592

[2] https://www.gov.pl/cyfryzacja/konsultacje-spoleczne-projektu-przepisow-wdrazajacych-ogolne-rozporzadzenie-o-ochronie-danych-rodo-

ORZECZENIE

Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane (wyr. z 1.12.2005 r. II SA/Wa 917/05, Legalis).

Wynika z tego, że w szkole należy określić jakie kategorie danych są przetwarzane, na jakiej podstawie prawnej a następnie zastosować odpowiednie zabezpieczenia. Inne narzędzia będą służyć gromadzeniu danych teleadresowych, a inne kwestii medycznych czy światopoglądowych.

Realizacja zadań przetwarzania danych osobowych uczniów, w tym zapewnienie stosowania adekwatnych rozwiązań w celu ochrony tych danych jest przede wszystkim obowiązkiem administratora danych. Zgodnie ze stanowiskiem GIODO[3], to dyrektor reprezentuje szkołę, która jest administratorem danych osobowych uczniów. Oznacza to, że kierujący placówką i reprezentujący ją dyrektor odpowiada za właściwe prowadzenie i przechowywanie dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej, a także za zgodność wydawanych dokumentów z posiadaną w placówce dokumentacją oświatową.

Co więcej, dyrektor celem realizacji swoich obowiązków w tym zakresie, powinien zapewnić ochronę przetwarzanych danych osobowych, tj. zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym (nie posiadającym odpowiedniego upoważnienia), kradzieżą, przetwarzaniem danych z naruszeniem przepisów o ochronie danych osobowych (w tym regulacjom unijnym), a także przed ich zamianą, uszkodzeniem, zniszczeniem czy utratą.

Dyrektor obowiązany jest ponadto do przeprowadzania okresowo kontroli w zakresie prawidłowości zabezpieczania i przechowywania danych przez pracowników placówki, którą zarządza. Celem kontroli jest zapobieganie naruszeniom oraz ich identyfikowanie, a także osób za nie odpowiedzialnych.

W tym miejscu należy zwrócić uwagę na, wprowadzoną w art. 83 RODO i doprecyzowaną w Projekcie nowej ustawy o ochronie danych osobowych, odpowiedzialność finansową za naruszenie obowiązków dotyczących ochrony danych osobowych. Zgodnie z art. 83 Projektu, na podmioty publiczne, o których mowa a art. 9 pkt 112 i 14 ustawy o finansach publicznych (w tym jednostki budżetowe), będzie mogła być nałożona w drodze decyzji administracyjnej kara pieniężna w wysokości do 100 000 zł.

RODO kładzie nacisk na ochronę danych osobowych dzieci

Na marginesie można wskazać, że RODO **w Motywie 38, 58 i 75** kładzie szczególny nacisk na ochronę danych osobowych dzieci. Nowa regulacja przewiduje w tym zakresie znacznie bardziej restrykcyjne warunki niż w stosunku do osób dorosłych. Będzie to dotyczyć przede wszystkim administratorów danych osobowych, którzy świadczą usługi społeczeństwa informacyjnego oraz przetwarzają dane wyłącznie na podstawie zgody.

Uregulowanie RODO stawia w tym obszarze dodatkowo wymagania w dotyczące wieku dzieci. Wskazuje, że samodzielne wyrażenie zgody na przetwarzanie danych osobowych może nastąpić w momencie ukończenia przez dziecko 16. roku życia. Niemniej jednak, przepis art. 8 ust. 1 RODO odnosi się wyłącznie do usług społeczeństwa informacyjnego. W przypadku świadczenia innego rodzaju usług zastosowanie znajdą pozostałe przepisy RODO.

W projekcie ustawy opublikowanym przez Ministerstwo Cyfryzacji zaproponowany został odmienny od unijnego próg wiekowy. Polska regulacja wskazuje na przesłanki zgodne z art. 12 Kodeksu cywilnego, przewidując obniżenie wieku potrzebnego do wyrażenia zgody na przetwarzanie danych osobowych do lat 13 (art. 3 Projektu ustawy).

Powyższa kwestia ma znaczenie w przypadku kooperacji placówek oświatowych z podmiotami komercyjnymi. Prowadzenie akcji promocyjnych (związanych na przykład ze sponsoringiem szkół) czy organizacja konkursów przez taki podmiot może bowiem podlegać właśnie tej szczególnej regulacji art. 8 RODO. Nieprawidłowości w powierzaniu przetwarzaniu danych przez szkołę mogę za sobą pociągnąć wskazaną powyżej odpowiedzialność finansową.

Niezbędne dalsze kroki

Gromadzenie i przetwarzanie danych osobowych to wyzwanie zarówno dla szkół, jak i prowadzących je samorządów. RODO w swoich Motywach wskazanych wyżej oraz art. 8 zwraca uwagę na konieczność nakładania szczególnej staranności przy przetwarzaniu danych osobowych dzieci.

W praktyce nie zwraca się uwagi na takie sytuacje jak upamiętnianie imprez szkolnych, które następnie publikowane są jako fotorelacje w gablotkach szkolnych lub na stronach internetowych, czy na badania kontrolne (bilanse) przeprowadzane przez szkolną pielęgniarkę. Sama archiwizacja zwolnień lekarskich uczniów wymaga indywidualnego podejścia.

Zmiana przepisów dotyczących danych osobowych daje szansę na upo-

[3] https://men.gov.pl/wp-content/uploads/2017/04/poradnik-obowiazki-dyrektora-szkoly-z-zakresu-ochrony-danych-osobowych.pdf

rządkowanie działania szkół w tym obszarze. W pierwszym rzędzie, konieczne jest określenie liczby zbiorów danych i przyporządkowanie ich określonemu celowi. Drugim krokiem jest wskazanie, w jakim zakresie zbiory te są ze sobą połączone (np. przez przekazywanie informacji zebranych na potrzeby edukacyjne do celów zdrowotnych lub na odwrót).

Kolejnym etapem jest określenie podstawy przetwarzania danych w danych zbiorach. Część bowiem będzie miało podstawę ustawową (listy przyjętych do szkoły), a część będzie przetwarzana np. na podstawie zgody (do celów marketingowych, na potrzeby partnerów szkoły, do celów publikacji zdjęć na stronie internetowej placówki). Efektem powyższego kroku powinno być m.in. zaprzestanie przetwarzania danych poza zakres wyrażonej zgody lub wykorzystanie danych przetwarzanych na podstawie ustawy do innych celów niż wskazane w ustawie. Oznaczać to może np. konieczność usunięcia zdjęć uczniów ze strony internetowej.

Określenie zakresu danych oraz ich przepływów pozwoli również wskazać krąg osób mających dostęp do określonych danych.

PRZYKAD

Kwestie medyczne dotyczące dziecka nie powinny być powszechnie dostępne dla pracowników placówki. Konieczne jest zapewnienie, że tylko osoby realizujące określone cele przetwarzania danych mają do nich wgląd. W konsekwencji, jeżeli nie jest tak obecnie, konieczne może być przechowywanie danych w oddzielnych systemach informatycznych lub zbiorach papierowych i zapewnienie, że tylko wybrane osoby będą miały do nich dostęp.

Wnioski wynikające z powyższych kroków powinny się znaleźć w wewnętrznej dokumentacji placówki określającej zasady przetwarzania danych (polityce bezpieczeństwa, instrukcjach i regulaminach, w tym w regulaminie obiegu dokumentów). Dodatkowo dokumentacja powinna zawierać odzwierciedlenie, wynikających z RODO, nowych uprawnień osób, których dane są przetwarzane.

Ważne

Konieczne też może być wprowadzenie rozwiązań techniczno-organizacyjnych, takich jak stworzenie rejestru przetwarzania danych, określenia osoby odpowiedzialnej za informowanie organów nadzorczych w przypadku naruszenia bezpieczeństwa danych czy wprowadzenie zmian w systemie monitoringu.

Ostatnim etapem będzie przeprowadzenie szkoleń dla pracowników placówki na temat wprowadzonych zmian i nowych obowiązków.

Zakres poszczególnych kroków będzie zależał od wielkości danej placówki. Pełne przygotowanie do wdrożenia będzie wymagało prawdopodobnie około 3 miesięcy pracy. Biorąc pod uwagę, że obowiązki wynikające z RODO dotkną szkół jeszcze w maju 2018 r., tj. w trakcie roku szkolnego, wdrożenie ich może stanowić wyzwanie dla osób kierujących placówkami.

Powyższe kroki placówka może zasadniczo wykonać samodzielnie, w szczególności określenie zbiorów danych osobowych i podstaw przetwarzania oraz wprowadzenie zmian w dokumentacji. Niezbędna wydaje się jednak współpraca z jednostką samorządu terytorialnego prowadzącą placówkę. Działania z poziomu JST pozwolą na lepszą koordynację i oszczędności w razie korzystania z pomocy podmiotów zewnętrznych.

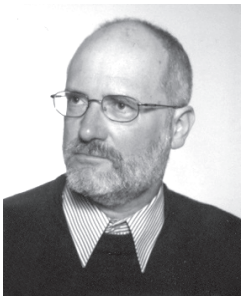
Powyższe działania powinny być przede wszystkim realizowane z uwzględnieniem ochrony danych osobowych dzieci.

▶ Podstawa prawna

- art. 27 ust. 1 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922)
- art. 8, 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)
- projekt z 12.9.2017 r. ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, opublikowany na stronach Ministerstwa Cyfryzacji
- projekt z 12.9.2017 r. ustawy o ochronie danych osobowych, opublikowany na stronach Ministerstwa Cyfryzacji

Temat numeru

Wybrane aspekty stosowania RODO oraz projektu nowej ustawy o ochronie danych osobowych



Marek Ujejski
Ekspert ds. bezpieczeństwa w COIG S.A. Wieloletni Dyrektor IT w sektorze publicznym i bankowym. W latach 2013–2015 przedstawiciel Polski z ramienia MCiA w eIDAS Expert Group działającej w DG CONNECT Komisji Europejskiej, współautor rozporządzeń wykonawczych w tym obszarze

Artykuł wyjaśnia nowe podejścia do obszaru bezpieczeństwa danych osobowych, wyrażanych deklaracyjnie przez terminy *Risk based approach* (podejście oparte na ryzyku), *Privacy by default* (domyślna ochrona danych) i *Privacy by design* (ochrona danych w fazie projektowania). Omówiono również istotne novum jakim jest kodeks postępowania i możliwość certyfikacji na zgodność z wymogami rozporządzenia, odnosząc się także do projektu ustawy o ochronie danych osobowych. Jest to wynik wielu dyskusji prowadzonych w różnych środowiskach, zarówno komercyjnych, jak i instytucji publicznych.

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 (Dz.Urz. UE L Nr 119 z 4.5.2016 r., s. 1–88; dalej: RODO) weszło w życie – zgodnie z brzmieniem artykułu 99 – 20. dnia po publikacji w Dzienniku Urzędowym Unii Europejskiej, a stosować się je będzie od 25.5.2018 r. Istotnym uzupełnieniem rozporządzenia są akty wykonawcze i delegowane. W rozporządzeniu wskazano obszary, w których KE ma możliwość wydania aktów wykonawczych oraz zakreślono obszary dla których kraje członkowskie Unii powinny wydać akty delegowane.

W przypadku Polski powstał projekt takiego aktu w randze ustawy[1]. Regulować ma on m.in. istotne z punktu praktycznego stosowania rozporządzenia procesy takie jak akredytacja i certyfikacja, niestety procesy te zostaną doprecyzowane dopiero przez planowany do powołania Urząd Ochrony Danych Osobowych.

Nowe podejście do regulacji

Już sama konstrukcja RODO ma wybitnie objaśniający charakter. W preambule szeroko omówiono cele i uzasadnienia wprowadzanej regulacji, świadczą o tym 173 punkty wspomnianej preambuły *versus* 99 artykułów samej regulacji. Zwraca również uwagę bardzo długi okres jaki minął od uzyskania opinii Europejskiego Inspektora Ochrony Danych[2] do przyjęcia RODO i rozpoczęcia jego stosowania. W odróżnieniu od dotychczas obowiązującej Dyrektywy i implementującej ją ustawy o ochronie danych osobowych,

[1] Projekt Ministerstwa Cyfryzacji z 12.9.2017 ustawa o ochronie danych osobowych.
[2] (172) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych, który wydał opinię 7.3.2012 r.

w polskim systemie prawnym w rozporządzeniu nie znajdziemy konkretnych wskazań, poza przykładowymi wyliczeniami, których spełnienie w literalny sposób świadczyłoby o tym, że dany podmiot wypełnia wszystkie wymagania RODO. Dotychczas obowiązująca ustawa z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922; dalej: OchrDanychU) i wydane z jej delegacji rozporządzenie MSWiA z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024) stawiało konkretne wymagania dotyczące organizacji procesu przetwarzania, posiadanych dokumentów, stosowanych zabezpieczeń kryptograficznych.

Jednak i w tym przypadku wiele procesów zabezpieczenia przetwarzania danych osobowych nie było do końca sprecyzowanych. Tak więc i obecne stosowanie zabezpieczeń ma charakter podlegający ocenie, zależnie od kontekstu występujących zagrożeń i wyboru adekwatnych środków do ich mitygacji. W konstrukcji RODO dokonano kolejnego kroku w kierunku przeniesienia większej odpowiedzialności na podmiot przetwarzający dane osobowe, przede wszystkim nakładając obowiązek szeroko rozumianej samooceny i działań wyprzedzających. Obwarowano to dodatkowo obowiązkiem udokumentowania jak ten proces jest prowadzony. Można dostrzec analogię do rozwiązań świata finansowego, gdzie takie podejście obowiązuje od dawna, a tzw. trzecia regulacja bazylejska[3] w zmodyfikowanym trzecim filarze *Market Discipline* narzuciła m.in. obowiązek szczegółowego przedstawienia metodyki jak bank oblicza swoje współczynniki kapitałowe podlegające regulacji. Również stosowane od dawna standardy amerykańskie wymagające własnej oceny ryzyka, w tym ryzyka operacyjnego (a do takiego można zaliczyć informatyczne przetwarzanie danych osobowych), takie jak COSO[4] niewątpliwie miały wpływ na taki kształt RODO.

Obowiązek uwzględnienia zapewnienia bezpieczeństwa przetwarzania danych już na początkowym etapie projektowania systemu przez administratora danych

Także podejście oparte na zasadzie koła Deminga „Plan-Do-Check-Act" (Zaplanuj-Wykonaj-Sprawdź-Popraw), szeroko stosowane w świecie standardów ISO dotyczących jakości, ma tu swoje odbicie. Ponadto istotną zmianę – w stosunku do stanu istniejącego – daje się zauważyć w obszarze projektowania nowych systemów informatycznych przetwarzających dane osobowe. Pojawia się tu wymóg uwzględnienia zasad ochrony prywatności już na początku procesu planowania systemu, wyrażony np. zasadą minimalizacji danych (art. 5 ust. 1 pkt c) RODO), czy też cały zakres art. 25 RODO, jednoznacznie wskazujący na obowiązek uwzględnienia zapewnienia bezpieczeństwa przetwarzania danych już na początkowym etapie projektowania systemu przez administratora danych. Ponieważ administrator danych bardzo często nie jest autorem projektu technicznego systemu informatycznego, który te dane będzie przetwarzał, jest konieczne aby przy przekazywaniu założeń lub definiowaniu kryteriów wyboru systemu do zaprojektowanego na poziomie logicznym procesu przetwarzania sformułował podstawowe wymagania bezpieczeństwa. Obowiązek ten, na mocy art. 25 ust. 1 i 2 RODO, jednoznacznie spoczywa na administratorze danych.

Certyfikacja

RODO nie precyzuje szczegółowo, jak ten stan – wymagany prawem – ma być osiągnięty, odsyła jedynie podmiot do procesu określonego w ust. 3 przywołanego art. 25 określonego jako certyfikacja (w całości art. 42 RODO). Mechanizm ten nie jest jedynym sposobem przedstawienia wiarygodnego zapewnienia spełnienia wymogów ustawodawcy, ale może być bardzo pomocny w wykazaniu zgodności z tymi wymaganiami. Certyfikacja w krajach UE może być wykonywana jedynie przez podmioty, które uzyskały akredytację w sposób określony w art. 43 RODO. Certyfikacja jest dobrowolna (art. 42 ust. 3 RODO) i nie stanowi o automatycznym uznaniu o wypełnieniu obowiązków wskazanych w omawianym rozporządzeniu, a w szczególności nie stanowi uszczerbku dla kompetencji kontrolnych organu nadzorczego.

Inną ścieżką zapewnienia bezpieczeństwa procesu (ale nie wykluczającą stosowania mechanizmu certyfikacji) jest opracowanie kodeksu postępowania (art. 40 RODO) przez wskazaną reprezentację podmiotów lub sam podmiot przetwarzający. Jednym z wskazanych w art. 40 ust. 2 RODO celów opracowania takiego kodeksu jest zapewnienie bezpieczeństwa przetwarzania w rozumieniu art. 32 RODO. Jest oczywiste, że początek procesu zapewnienia bezpieczeństwa zaczyna się w fazie projektowej, szczególnie w epoce masowego stosowania przetwarzania rozproszonego z dostępem zdalnym. Błędy popełnione w tej fazie w obszarze uwierzytelnienia użytkowników i autoryzacji do wskazanych zasobów oraz zapewnienia integralności kodu aplikacji[5] przetwarzającej dane osobowe są bardzo trudne do napra-

[3] http://www.bis.org/bcbs/basel3/b3summarytable.pdf.
[4] Ramy Kontroli Wewnętrznej dotyczące ustawy SOX w USA wydane przez Committee of Sponsoring Organizations of the Treadway Commission.
[5] Chodzi o zapewnienie braku możliwości modyfikacji kodu wykonywalnego przez złośliwe oprogramowanie.

wienia w fazie końcowej projektu lub wręcz w fazie eksploatacyjnej, wiążą się z koniecznością przebudowania znacznej części aplikacji jeśli nie wręcz z napisaniem jej od nowa w innej technologii.

Niewątpliwie jednym z istotnych problemów jest regres odpowiedzialności za niewłaściwe przygotowanie projektu, wybór technologii i wreszcie wykonanie technicznej realizacji systemu przetwarzającego dane osobowe w stosunku do podmiotu, który wykonał tę pracę na zamówienie administratora danych lub też, od którego administrator nabył część lub całość systemu. Rozporządzenie, poprzez dyspozycję zawartą w przywołanym już art. 25 RODO, jednoznacznie przypisuje odpowiedzialność za cały proces bezpieczeństwa administratorowi danych, tak więc jakakolwiek odpowiedzialność podmiotu tworzącego system informatyczny może być wywiedziona na zasadach odpowiedzialności cywilnej uregulowanej umową. Nie mamy tu bowiem współodpowiedzialności podmiotu, któremu powierzono dane lecz stosunek umowny, na bazie którego wykonano narzędzie mające prawidłowo wykonać zadanie, którego specyfikację przygotował administrator danych. Z drugiej strony, dbając o własną pozycję rynkową, nic nie stoi na przeszkodzie aby podmiot profesjonalnie zajmujący się budowaniem systemów informatycznych przetwarzających dane osobowe ustanowił kodeks postępowania, w którym zawarte zostaną zasady służące docelowo zadośćuczynieniu zasadzie *Privacy by design* i dobrowolnie rozciągnął stosowanie tej części kodeksu na systemy przetwarzające dane osobowe, które projektuje dla innych podmiotów.

Ważne

Należy jednak pamiętać, że dobrowolnie przyjęte zobowiązanie ma skutki obligatoryjne i niestosowanie się do nich przez podmiot, który zobowiązanie przyjął może pociągać skutki penalizacyjne wskazane w RODO.

Certyfikacja i kodeks postępowania jako deklaracja zgodności

Wskazany powyżej mechanizm deklaracji zgodności (*compliance*) wymaga podjęcia działań, a wcześniej ustanowienia szeregu instytucji wskazanych w RODO. Chcąc zatwierdzić lub zmienić już zatwierdzony kodeks postępowania, zrzeszenie podmiotów lub podmioty, które chcą przeprowadzić taki proces, muszą uzyskać zgodę organu nadzorczego ustanowionego w trybie art. 55 RODO. Taką ścieżkę wskazuje bezpośrednio art. 40 ust. 5 RODO. Organ nadzorczy ocenia projekt kodeksu lub przedłożonej propozycji zmiany i podejmuje decyzję o przyjęciu go do stosowania. W przypadku, gdy kodeks dotyczy działania w jednym z państw członkowskich i nie rozciąga się na działania w innych państwach (zdecydowana większość przypadków), organ nadzorczy dokonuje rejestracji tego kodeksu i publikuje jego treść (art. 40 ust. 6). W przypadku, gdy kodeks obejmuje działania podmiotu lub grupy podmiotów objętych postanowieniami tego kodeksu w kilku państwach UE, właściwy organ nadzorczy przedkłada projekt do zaopiniowania Europejskiej Radzie Ochrony Danych, która przedstawia stanowisko w sprawie, czy zabezpieczenia opisane w kodeksie są wystarczające dla zapewnienia odpowiedniego poziomu ochrony danych osobowych (art. 40 ust. 6). Od tego momentu droga do zatwierdzenia kodeksu postępowania przebiega w sposób odmienny od sytuacji, w której o zatwierdzenie kodeksu występował podmiot przetwarzający dane tylko w jednym kraju UE, a mianowicie opinia trafia do Komisji Europejskiej, która może przyjąć ten kodeks postępowania w drodze aktów wykonawczych po wypełnieniu procedury sprawdzającej (art. 93 ust. 2 RODO) i stwierdzić, że obowiązuje on w całej UE.

Od tej pory monitorowaniem przestrzegania postanowień kodeksu może się zajmować podmiot, który – na mocy art. 41 ust. 2 RODO – wypełnił wszystkie określone tam warunki i w celu wykonania tego zadania, został akredytowany przez właściwy organ nadzorczy. W przypadku stwierdzenia przez podmiot wykonujący proces monitorowania, że nastąpiło naruszenie przez konkretnego administratora zasad określonych w tym dobrowolnie przyjętym kodeksie, podmiot monitorujący może zawiesić lub wykluczyć tego administratora spośród podmiotów stosujących ten kodeks i podjąć inne stosowne działania, jednocześnie informując organ nadzorczy o stwierdzonych naruszeniach (art. 41 ust. 4 RODO). Należy przy tym cały czas pamiętać, że czynności te stosuje się bez uszczerbku dla uprawnień organu nadzorczego.

Na mocy art. 41 ust. 6 RODO monitorowania nie stosuje się do organów i podmiotów publicznych w związku z przetwarzaniem danych osobowych.

W odniesieniu do certyfikacji należy przypomnieć, że z założenia proces ten jest procesem prowadzącym do uzyskania wyróżnika potwierdzającego zgodność z przyjętymi kryteriami. Metoda ta jest powszechnie stosowana w zakresie przestrzegania standardów, w przypadku RODO potwierdza zgodność podmiotu w wymiarze prawnym, organizacyjnym i procesowym z wymaganiami określonymi przez RODO, włączając w to akty wykonawcze i delegowane. Certyfikacja, podobnie jak przyjęcie kodeksu postępowania, nie wpływa na obowiązek

przestrzegania wymogów RODO i nie stanowi uszczerbku dla uprawnień organu nadzorczego.

Do prowadzenia certyfikacji uprawnione są podmioty, które wypełniły warunki określone w art. 43 RODO lub bezpośrednio organ nadzorczy. Certyfikacji, podobnie jak to ma miejsce w obszarze certyfikacji na zgodność z wymaganiami ISO, udziela się na 3 lata, po czym proces wznowienia ważności tej certyfikacji trzeba powtórzyć. Informacja o pomyślnie przeprowadzonej certyfikacji jest gromadzona na poziomie Rady Ochrony Danych, która udostępnia tę informację publicznie.

Certyfikacja i kodeksy postępowań w projekcie ustawy o ochronie danych osobowych

Odnosząc się do drogi wskazującej organ właściwy do przeprowadzenia akredytacji trzeba stwierdzić, bazując na wspomnianym projekcie ustawy o ochronie danych osobowych z 12.9.2017 r., że Polska wybrała drogę wskazaną w art. 43 ust. 1 lit. a) RODO, czyli organ nadzorczy. W projekcie wspomnianej ustawy w art. 6 znajdujemy przepis wskazujący, że certyfikacji dokonuje Prezes Urzędu Ochrony Danych Osobowych, nowego organu, planowanego do powołania na mocy art. 20 ust. 2 nowej ustawy.

W obecnej sytuacji prawnej, gdy mamy dopiero projekt ustawy wypełniający delegację jaką krajom członkowskim UE dało rozporządzenie i braku konkretnych wymagań odnoszących się do kodeksów postępowań (te bowiem zostaną określone dopiero po powołaniu właściwego organu), trudno jest jednoznacznie stwierdzić, jakie formy zapisów zawartych w kodeksie postępowań zyskają uznanie właściwego organu.

Odnosząc się do certyfikacji – zajmie się tym w Polsce bezpośrednio organ jakim jest Prezes Urzędu Ochrony Danych Osobowych, a na podstawie art. 17 projektowanej ustawy monitorowaniem przestrzegania kodeksu postępowania zająć się może także podmiot akredytowany przez Prezesa Urzędu. Zważywszy, że planuje się też powołanie Rady ds. Ochrony Danych Osobowych, która będzie wśród swoich zadań miała m.in. składanie propozycji dotyczących kryteriów certyfikacji, o której mowa w art. 7 projektu ustawy, droga do określenia w sposób prawem wiążący tych kryteriów wydaje się odległa. Nieco lepiej wygląda sprawa dotycząca kodeksu postępowania. Co prawda powołanie podmiotów (lub podmiotu) zajmujących się monitorowaniem przestrzegania tych kodeksów wymaga decyzji Prezesa Urzędu, ale przecież nic nie stoi na przeszkodzie, aby w oparciu o znane w świecie praktyki (choćby wspomniane dobrowolne regulacje sektora finansowego) w oparciu o generalnie znane wymogi rozporządzenia, tzw. „dobre praktyki" i konkretną wiedzę operacyjną o zagrożeniach (także w oparciu o doświadczenie płynące z długoletniego stosowania ustawy o ochronie danych osobowych) tworzyć projekty takich kodeksów już dziś. W przekonaniu autora niniejszego artykułu dobrze przemyślany projekt kodeksu postępowania nie będzie wymagał dużych zmian w momencie, kiedy będzie możliwe jego zatwierdzenie przez planowany do powołania organ. Rozpoczęcie pracy z takim wyprzedzeniem pozwoli podmiotowi (lub grupie podmiotów), który zamierza taki kodeks utworzyć, przemyśleć dogłębnie wszystkie aspekty przetwarzania danych osobowych z szczególnym uwzględnieniem *Privacy by default* i *Privacy by design* stanowiących istotne *novum* w stosunku do stanu obecnego.

Podstawa prawna

- art. 25, art. 40, art. 41, art. 42, art. 55 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 (Dz.Urz. UE L Nr 119 z 4.5.2016 r., s. 1–88)

Prawo do przenoszenia danych

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

W artykule omówiona została konstrukcja prawna i zakres nowego uprawnienia przyznanego, w ogólnym rozporządzeniu o ochronie danych, osobie, której dane dotyczą – prawa do przenoszenia danych. Uprawnienie to służyć ma zapewnieniu osobie, której dane dotyczą, większej kontroli nad przetwarzaniem swoich danych, a jednocześnie umożliwiać swobodny przepływ danych.

W art. 20 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 (Dz.Urz. UE L Nr 119 z 4.5.2016 r., s. 1–88; dalej: RODO), wprowadzono nowe uprawnienie podmiotu danych – prawo do przenoszenia danych. Uprawnienie to służyć ma zapewnieniu osobie, której dane dotyczą, większej kontroli nad przetwarzaniem swoich danych, a jednocześnie umożliwiać swobodny przepływ danych. Dzięki możliwości skorzystania z omawianego uprawnienia, podmiot danych będzie mógł łatwiej zmienić dostawcę usługi, co może także przyczynić się do wzrostu konkurencyjności między podmiotami świadczącymi usługi (chodzi tu głównie o usługi świadczone z wykorzystaniem technologii informacyjnych i komunikacyjnych).

Ze względu na to, że uprawnienie do przenoszenia danych nie występowało dotąd w regulacjach prawnych dotyczących ochrony danych, warto przyjrzeć się konstrukcji prawnej tego uprawnienia, a także wskazać wątpliwości, jakie nasuwają się przy dokonywaniu wykładni art. 20 RODO oraz podjąć próbę ich wyjaśnienia. Analizując przepisy dotyczące prawa do przenoszenia danych warto również korzystać z pomocy, jaką stanowić może dokument opracowany przez Grupę Roboczą Art. 29 ds. Ochrony Danych pt. Wytyczne dotyczące prawa do przenoszenia danych[1], przyjęty 13.12.2016 r., ostatnio zmieniony 5.4.2017 r. Wprawdzie dokument ten nie ma mocy prawnie wiążącej, jednak wyjaśnienia i wskazówki w nim zawarte mogą przyczynić się do lepszego zrozumienia i łatwiejszego stosowania przepisu art. 20 RODO.

Przesłanki warunkujące możliwość skorzystania z uprawnienia do przenoszenia danych

Prawo do przenoszenia danych nie jest uprawnieniem, z którego może skorzystać każdy, czyje dane są poddawane przetwarzaniu, ponieważ możliwość realizacji tego uprawnienia została ograniczona przez wskazanie w art. 20 ust. 1 RODO przesłanek, jakie powinny być spełnione. Przesłanki te doty-

[1] WP 242 rew.01, polskie tłumaczenie dostępne na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych, pod adresem: http://www.giodo.gov.pl/pl/file/12455.

czą podstaw, na jakich opiera się przetwarzanie danych oraz sposobu, w jaki przetwarzanie jest dokonywane.

Jeśli chodzi o podstawy dopuszczalności przetwarzania danych, to w przepisie art. 20 ust. 1 lit. a) RODO przyjęto, że omawiane uprawnienie przysługuje jedynie, gdy przetwarzanie opiera się na zgodzie osoby, której dane dotyczą lub umowie, której stroną jest podmiot danych. Oznacza to, że przetwarzanie mające inną niż zgoda bądź umowa podstawę prawną[2] nie wiąże się z możliwością skorzystania z prawa do przenoszenia danych. Przyjęcie tego rodzaju ograniczenia jest związane z charakterem omawianego uprawnienia, z którego korzystać można wtedy, gdy podmiot danych decyduje o przetwarzaniu danych, natomiast w przypadku, gdy osoba, której dane dotyczą nie może samodzielnie decydować o przetwarzaniu (np. w sytuacji, gdy obowiązek przetwarzania danych wynika z przepisów prawa) uprawnienie do przenoszenia danych nie przysługuje.

Przesłanka odnosząca się do sposobu przetwarzania danych dotyczy wymogu, aby przetwarzanie odbywało się w sposób zautomatyzowany, tzn. z wykorzystaniem narzędzi automatycznych (np. komputerów), a nie w sposób tradycyjny (ręcznie – w zbiorach papierowych). Ta przesłanka jest również powiązana z charakterem omawianego uprawnienia, gdyż prawo do przenoszenia danych ma pozwolić na przenoszenie danych w celu ich dalszego zautomatyzowanego przetwarzania (przenoszenie danych między systemami informatycznymi), a nie przenoszenie danych przetwarzanych manualnie.

Wskazane powyżej przesłanki dotyczące podstawy prawnej i sposobu przetwarzania powinny być spełnione łącznie, tzn. nie wystarczy, że przetwarzanie opiera się na zgodzie lub umowie, konieczne jest aby równocześnie prowadzone było w sposób zautomatyzowany.

Treść i sposób realizacji uprawnienia do przenoszenia danych

Prawo do przenoszenia danych oznacza uprawnienie osoby, której dane dotyczą do otrzymania od administratora danych, które osoba ta dostarczyła administratorowi oraz uprawnienie do przesłania tych danych innemu administratorowi (art. 20 ust. 1 RODO). Uprawnienie to może być także realizowane inaczej – poprzez żądanie, by dane osobowe objęte omawianym uprawnieniem, zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe (art. 20 ust. 2 RODO). Dane osobowe powinny być przekazane „w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego".

Uprawnieniem do przenoszenia danych objęte są jedynie dane osobowe odnoszące się do osoby, która żąda przeniesienia danych. W zakresie tym mieszczą się także dane poddane pseudonimizacji, jeżeli można je powiązać z osobą, której dotyczą, natomiast nie mieszczą się dane anonimowe bądź dane osobowe, które nie dotyczą wnioskodawcy. Jeżeli administrator przetwarza dane wielu osób, jednak ich przetwarzanie dotyczy wnioskodawcy, wówczas dane te są objęte uprawnieniem do przenoszenia danych.

PRZYKŁAD

Jako przykład tego rodzaju danych Grupa Robocza wskazała rejestry połączeń telefonicznych, zawierające dane osób trzecich, stwierdzono przy tym, że abonenci powinni mieć możliwość otrzymania tych rejestrów w odpowiedzi na wnioski o przenoszenie danych, ponieważ rejestry dotyczą (także) wnioskodawcy[3].

Na tle tak sformułowanego przepisu nasuwa się wątpliwość o zakres danych objętych prawem do przenoszenia danych. Prawodawca unijny posłużył się sformułowaniem „dane osobowe jej dotyczące, które dostarczyła administratorowi". Takie sformułowanie może być rozumiane co najmniej dwojako: w znaczeniu węższym – jako dane, które osoba świadomie i dobrowolnie podała administratorowi (np. wpisała do formularza służącego gromadzeniu danych), albo w znaczeniu szerszym – jako dane, które osoba poprzez jakiekolwiek swoje działania dostarczyła administratorowi (np. odnoszące się do aktywności użytkownika w serwisie internetowym). W piśmiennictwie przedmiotu zaprezentowany został pogląd, który może być odczytywany jako uznający trafność ujęcia węższego, zgodnie z którym „wydaje się, iż rozsądne byłoby przenoszenie jedynie tych danych, które zostały pierwotnie uzyskane od osoby, której dane dotyczą, a nie tych będących efektem dalszych operacji przetwarzania"[4]. Odmienne stanowisko, wskazujące na szersze rozumienie określenia danych osobowych, które osoba dostarczyła administratorowi, zostało zaprezentowane w Wytycznych Grupy Roboczej Art. 29, w których stwierdzono, że „prawo do przenoszenia danych obejmuje dane przekazane świadomie i aktywnie przez osobę, której dane dotyczą, jak również dane osobowe wygenerowane poprzez jej działanie"[5]. Zakres ten nie obejmuje danych powstałych w wyniku opracowania (przetwarzania) przez administratora. Chodzi zatem o dane, które osoba dostarczyła administratorowi nie tylko przy gromadzeniu danych wraz z wy-

[2] Tj. realizacja obowiązku wynikającego z przepisu prawa; ochrona żywotnych interesów osoby, której dane dotyczą; wykonanie zadania realizowanego w interesie publicznym lub przetwarzanie danych w ramach sprawowania władzy publicznej powierzonej administratorowi; realizacja prawnie uzasadnionych interesów oraz inne niż zgoda podstawy dopuszczalności przetwarzania szczególnych kategorii danych.

[3] Por. Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 10.

[4] *M. Zadrożny* [w:] *A. Dmochowska, M. Zadrożny,* Unijna reforma ochrony danych osobowych. Analiza zmian, Warszawa 2016, s. 47.

[5] Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 3.

rażeniem zgody na ich przetwarzanie lub zawarciem umowy, ale równie na dalszych etapach przetwarzania, natomiast omawiane uprawnienie nie dotyczy danych wytworzonych przez administratora na własne potrzeby jako rezultat procesów przetwarzania danych, gdyż takie dane nie zostały dostarczone przez osobę, której te dane dotyczą. W Wytycznych Grupy Roboczej Art. 29 wyjaśniono, że dane wywnioskowane i dane wywiedzione tworzone są przez administratora danych na podstawie danych „przekazanych przez osobę, której dane dotyczą" (np. wynik oceny dotyczącej zdrowia użytkownika lub profil tworzony w kontekście zarządzania ryzykiem i regulacji finansowych) nie mogą jako takie być uznane za „przekazane przez" osobę, której dane dotyczą[6].

Gdy chodzi o sposób realizacji uprawnienia do przenoszenia danych, to prawodawca przewidział zasadniczo dwie drogi:

1) przekazanie danych podmiotowi danych,
2) bądź na jego wniosek przekazanie danych innemu administratorowi.

Przekazanie powinno nastąpić przez przesłanie danych drogą elektroniczną. Podmiot danych może zdecydować czy dane mają zostać przesłane do niego, czy też do innego administratora danych. W pierwszym przypadku podmiot danych może samodzielnie wykorzystywać przekazane mu dane bądź przesłać je dalej – kolejnemu administratorowi, a dotychczasowy administrator, zgodnie z art. 20 ust. 1 RODO, nie powinien stwarzać przeszkód w realizacji tych działań.

Prawo do przenoszenia danych realizowane jako uprawnienie do otrzymania od administratora danych na swój temat może służyć podmiotowi danych – na co zwrócono uwagę w Wytycznych Grupy Roboczej Art. 29 – w celu dalszego osobistego wykorzystania danych, a tego typu przechowanie może mieć miejsce na urządzeniu prywatnym lub w prywatnej chmurze, bez konieczności przesyłania ich innemu administratorowi danych, i stanowi uzupełnienie prawa dostępu do danych[7].

Druga możliwość dotyczy przekazania danych innemu administratorowi, czy to bezpośrednio (jeśli tego zażąda osoba, której dane dotyczą, wskazując administratora, któremu dane powinny zostać przesłane), czy też pośrednio – poprzez przekazanie osobie, której dane dotyczą, a ona sama prześle te dane nowemu administratorowi. W Wytycznych Grupy Roboczej Art. 29 wyjaśniono, że poza zapewnieniem uprawnień konsumentom poprzez zapobieganie „uzależnieniu" (ang. *lock-in*)[8], prawo do przenoszenia danych ma promować możliwości innowacji i wymiany danych osobowych między administratorami danych w bezpieczny sposób, pod kontrolą osoby, której dane dotyczą[9].

Przesłanie bezpośrednio innemu administratorowi jest uzależnione od faktycznych (technicznych) możliwości administratora, który realizuje uprawnienie do przenoszenia danych.

Ważne

Przepisy RODO nie nakładają na administratorów obowiązku zagwarantowania technicznych możliwości zautomatyzowanego przenoszenia danych (tzn. tworzenia aplikacji służących przenoszeniu danych), prawodawca unijny ograniczył się do wskazania, że dane powinny być przekazywane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

W motywie 68 preambuły do RODO wyjaśniono, że format danych powinien być „interoperacyjny" tzn. dane zapisane w takim formacie powinny być możliwe do przetwarzania w różnych systemach. Prawodawca unijny uznał, że należy zachęcać administratorów do opracowywania interoperacyjnych formatów, natomiast nie powinno się nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania.

Taka konstrukcja ma pozwalać na zautomatyzowane przetwarzanie, dzięki temu że „ustrukturyzowany format" będzie umożliwiał maszynowy odczyt danych, co w praktyce oznacza, że przesłane dane będą mogły być automatycznie „zaciągnięte" do innego systemu i tam poddawane dalszemu przetwarzaniu w sposób zautomatyzowany, bez konieczności ponownego „ręcznego" wprowadzania danych do systemu.

PRZYKŁAD

Przykładem formatu danych, który spełnia wymogi określone w art. 20 ust. 1 RODO jest format pliku .xml, tzn. dokumentu zapisanego w rozszerzalnym języku znaczników XML (ang. ***Extensible Markup Language***), który pozwala prezentować różne dane w ustrukturyzowany sposób, a przez to umożliwia wymianę danych pomiędzy różnymi systemami.

W Wytycznych Grupy Roboczej Art. 29 zwrócono uwagę na to, że administratorzy powinni ustanowić zabezpieczenia w celu zapewnienia, że będą rzeczywiście działać w imieniu osoby, której dane dotyczą (np. szczegółowe procedury dotyczące uzyskania potwierdzenia od osoby, której dane dotyczą albo przed przesłaniem albo

[6] Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 11.

[7] Por. Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 5. Jako przykład tego rodzaju wykorzystania prawa dostępu do danych Grupa Robocza wskazała żądanie udostępnienia danych w postaci listy odtwarzania (lub historii słuchanych utworów) z serwisu strumieniowej transmisji muzyki, aby dowiedzieć się, ile razy osoba ta słuchała określonych utworów w celu sprawdzenia, jaki utwór muzyczny chce nabyć lub jakiego utworu chce posłuchać na innej platformie. Podkreślono przy tym, że tego rodzaju przetwarzanie przekazanych danych wchodzi w zakres działalności domowej i w związku z tym nie podlega już RODO.

[8] Tzn. powstawaniu tzw. efektu zamknięcia polegającego na uzależnieniu się od jednego dostawcy.

[9] Por. Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 5–6.

wcześniej, gdy udzielana jest pierwotna zgoda na przetwarzanie lub gdy finalizowana jest umowa)[10].

Zastrzeżenia i ograniczenia w stosowaniu uprawnienia do przenoszenia danych

W przepisie art. 20 ust. 3 RODO stwierdzono, że wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych („prawa do bycia zapomnianym") uregulowanego w art. 17 RODO, a ponadto, iż prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Pierwsza część wskazanego powyżej przepisu określa relacje między prawem do przenoszenia danych a prawem do usunięcia danych; są to dwa uprawnienia zasadniczo od siebie niezależne, choć ze sobą powiązane. Opierając się na potocznym rozumieniu pojęcia „przenoszenie" można byłoby twierdzić, że administrator, który przesłał dane realizując to żądanie, powinien niejako automatycznie usunąć dane, gdyż przenoszenie polega zazwyczaj na zabraniu czegoś z jednego miejsca i umieszczeniu w innym miejscu (tu: danych od jednego administratora do drugiego). Jednak konieczność fizycznego zabrania dotyczy rzeczy materialnych, natomiast w przypadku informacji i prawa do przenoszenia danych kwestia ta nie jest tak prosta i jednoznaczna. Skorzystanie z uprawnienia do przenoszenia danych nie pociąga za sobą automatycznie konsekwencji w postaci usunięcia danych przez administratora, który realizuje uprawnienie do przeniesienia danych. Treścią uprawnienia do przenoszenia danych, jak zostało to wskazane powyżej, jest otrzymanie (przesłanie) danych, a nie ich usunięcie, a administrator może nadal przetwarzać dane przez okres niezbędny do realizacji celów przetwarzania. Oznacza to, że osoba korzystająca z prawa do przenoszenia swoich danych może domagać się usunięcia jej danych, jednak administrator nie będzie zobowiązany do realizacji żądania usunięcia danych, jeżeli zostaną spełnione przesłanki wskazujące na to, że dane nie powinny zostać usunięte. Taka sytuacja ma miejsce, zgodnie z art. 17 ust. 3 RODO, gdy dalsze przetwarzanie przekazywanych danych jest niezbędne:

1) do korzystania z prawa do wolności wypowiedzi i informacji;
2) do wywiązania się z prawnego obowiązku przetwarzania danych albo 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;
4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.

Ponadto, jak wyraźnie stwierdzono w art. 20 ust. 3 zd. 2 RODO, prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Oznacza to, że nawet w sytuacji, gdy przesłanki uprawniające do skorzystania z prawa do przenoszenia danych są spełnione (przetwarzanie odbywa się na podstawie zgody lub umowy w sposób zautomatyzowany), ale administrator realizuje zadania publiczne (np. gromadzi informacje w związku z zapobieganiem i zwalczaniem procederu prania pieniędzy) lub sprawuje władzę publiczną, to skorzystanie z uprawnienia do przenoszenia danych nie jest możliwe.

Grupa Robocza Art. 29 zasugerowała jednak w Wytycznych, że nawet jeżeli administratorzy nie mają obowiązku zapewniania przenoszenia danych, to opracowanie procedur automatycznego odpowiadania na wnioski o przenoszenie może być uznane za dobrą praktykę, a jako przykład tego rodzaju działań wskazano serwis rządowy zapewniający łatwe pobieranie wcześniej złożonych deklaracji podatkowych[11]. Tego rodzaju zalecenie nie powinno być odczytywane jako obowiązek, a w praktyce wydaje się, że realizacja konstrukcji prawa do przenoszenia danych w sektorze publicznym będzie rozwiązaniem rzadko spotykanym i wyjątkowym.

Może się również zdarzyć, że podmiot danych będzie chciał skorzystać z podobnych uprawnień przysługujących mu na podstawie szczególnych przepisów, a wówczas przepisy szczególne mogą powodować wyłączenie stosowania art. 20 RODO[12].

Dodatkowe zastrzeżenie odnoszące się do omawianego uprawnienia, zostało określone w art. 20 ust. 4 RODO. Zgodnie z tym przepisem, prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

PRZYKŁAD

Grupa Robocza Art. 29 wskazała jako przykład udostępnienie wykazu połączeń telekomunikacyjnych, zawierającego dane osób trzecich, wskazując, że jeżeli takie wykazy są następnie przesyłane nowemu administratorowi, ten nie

[10] Por. Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 6.
[11] Por. Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 9.
[12] Jako przykład takiej sytuacji wskazano wniosek osoby, której dane dotyczą, mający na celu zapewnienie dostępu do historii jej rachunku bankowego dla dostawcy usługi informacji o koncie, do celów wskazanych w 2. Dyrektywie w sprawie usług płatniczych (PSD2), taki dostęp powinien być zapewniony zgodnie z przepisami tej dyrektywy. Por. Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 8.

powinien ich przetwarzać w celu, który by negatywnie wpłynął na prawa i wolności stron trzecich (uniemożliwił stronom trzecim realizację ich praw jako osób, których dane dotyczą, na mocy RODO, np. praw do informacji, dostępu itp.).

W ocenie Grupy Roboczej Art. 29 prawa i wolności osób trzecich nie będą przestrzegane, jeżeli nowy administrator będzie wykorzystywał dane osobowe do innych celów, np. jeżeli administrator, który otrzymał dane osobowe osób trzecich wykorzystuje je do celów marketingowych[13]. Negatywny wpływ na prawa innych podmiotów może dotyczyć także danych objętych prawem własności intelektualnej (prawem autorskim) i tajemnicą handlową.

Podstawa prawna

- art. 20 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 (Dz.Urz. UE L Nr 119 z 4.5.2016 r., s. 1–88)

[13] Por. Wytyczne dotyczące prawa do przenoszenia danych, WP 242, s. 10, 12.

Podsumowanie

Prawo do przenoszenia danych jest nowym uprawnieniem, co sprawia, że jego realizacja, przy braku doświadczeń w tym zakresie, może być przyczyną licznych wątpliwości i problemów. W artykule przedstawiono zaledwie niektóre, wybrane zagadnienia, odnoszące się do omawianego prawa. Można wyrazić nadzieję, że zaprezentowane analizy, wsparte zaleceniami i opiniami Grupy Roboczej Art. 29, stanowić będą przyczynek do dyskusji nad optymalną praktyką realizacji prawa do przenoszenia danych, choć nie ulega wątpliwości, że jeszcze wiele kwestii z tego zakresu wymaga szczegółowego wyjaśnienia. Warto również zwrócić uwagę na to, że naruszenie przepisów dotyczących realizacji prawa do przenoszenia danych od 25.5.2018 r. będzie mogło pociągnąć za sobą negatywne konsekwencje w postaci nałożenia przez organ nadzorczy administracyjnej kary pieniężnej. Zagrożenie tego rodzaju powinno skłonić administratorów do ostrożności i dbałości o prawidłową realizację wymogów określonych w art. 20 RODO.

Zarządzanie ochroną danych osobowych oparte na ryzyku

Kamil Pszczółkowski
Ekspert ds. Bezpieczeństwa

Zarządzanie ryzykiem nie jest rewolucją a jedynie ewolucją przeniesioną z innych systemów zarządzania bezpieczeństwem. Stosowanie podejścia opartego na ryzyku zapewnia nam definiowanie adekwatnych mechanizmów bezpieczeństwa, dostosowanych do wielkości naszej organizacji, stosowanej technologii oraz wrażliwości i rodzajów operacji związanych z przetwarzaniem danych osobowych.

Stosowane podejście do definiowania wymagań w ochronie danych osobowych

Dotychczas w ochronie danych osobowych przyjęło się stosowanie zdefiniowanych wymagań organizacyjnych i technicznych, tj. Polityki Bezpieczeństwa Danych Osobowych i Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Wspomniane powyżej Polityka i Instrukcja definiowały wymagania, jakie należy zaimplementować w organizacji w celu zapewniania poufności, integralności i rozliczalności ochrony danych osobowych.

Wdrażanie zdefiniowanych na „sztywno" regulacji ma pewne zalety, np. ustandaryzowanie stosowanych zabezpieczeń między organizacjami, jednakże należy zwrócić uwagę na liczne wady, tj. brak dostosowania zabezpieczeń do operacji przetwarzania danych osobowych wykonywanych przez daną organizację oraz potrzeb stosowania ochrony, uwzględniającej warunki funkcjonowania organizacji.

Zagadnienie to zostało dostrzeżone, i na nowo zdefiniowane, w rozporządzeniu 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. L Nr 119 z 4.5.2016 r., s. 1–88; dalej: RODO), gdzie w celu określenia potrzeb organizacji w odniesieniu do wymagań związanych z ochroną danych osobowych oraz utworzenia skutecznego systemu ochrony danych osobowych potrzebne jest systematyczne podejście do zarządzania ryzykiem. W tym celu konieczne jest uwzględnienie stanu wiedzy technicznej, kosztów wdrażania zabezpieczeń oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Zarządzanie ryzykiem w ochronie danych osobowych

Zarządzanie ochroną danych osobowych oparte na ryzyku ma na celu:

1) zapewnienie zdolności do ciągłego zagwarantowania poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

2) definiowanie i wdrażanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku;
3) ocenę czy stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zarządzanie ryzykiem w ochronie danych osobowych jest procesem ciągłym, monitorującym adekwatność oraz skuteczność stosowanych zabezpieczeń organizacyjnych i technicznych, w celu utrzymania ryzyka na akceptowalnym poziomie.

Stosowana przez organizację metodyka zarządzania ryzykiem ma zapewnić porównywalne i powtarzalne rezultaty przez zastosowanie standaryzacji skal oceny oraz sposobu przeprowadzania analizy, niezależnie od tego, kto będzie przeprowadzał analizę i ocenę ryzyka danych osobowych w organizacji.

Ocena skutków dla ochrony danych osobowych powinna być przeprowadzona „przed przetwarzaniem" (art. 25, art. 35 ust. 1, art. 35 ust. 10, a także motywy 78, 90 i 93 preambuły RODO).

Ocena skutków powinna być uruchamiana na etapie projektowania operacji przetwarzania, nawet jeśli niektóre operacje przetwarzania są wciąż nieznane. Konieczne może być powtórzenie poszczególnych etapów oceny skutków w miarę postępu procesu projektowania, ponieważ wybór niektórych środków technicznych lub organizacyjnych może mieć wpływ na wagę lub prawdopodobieństwo wystąpienia zagrożeń związanych z przetwarzaniem danych osobowych.

Wymaganie aktualizacji przeprowadzonej oceny skutków dla ochrony danych osobowych po rozpoczęciu procesu przetwarzania nie jest ważnym powodem odłożenia lub braku realizacji oceny na etapie projektowania rozwiązania. W niektórych przypadkach ocena skutków będzie procesem ciągłym, np. gdy proces przetwarzania jest dynamiczny i podlega ciągłym zmianom.

Ważne

Zgodnie z dobrymi praktykami oraz opinią Grupy Roboczej ds. Ochrony danych, zaleca się by zarządzanie ryzykiem w ochronie danych osobowych zapewniało:

1) zidentyfikowanie operacji przetwarzania danych osobowych o wysokim ryzyku naruszenia praw lub wolności osób fizycznych;
2) oszacowanie ryzyka z punktu widzenia operacji przetwarzania, tzn. czy są niezbędne oraz proporcjonalne w stosunku do celów przetwarzania;
3) oszacowanie ryzyka z punktu widzenia ich skutków urzeczywistnienia ryzyka naruszenia praw lub wolności osób fizycznych oraz prawdopodobieństwa ich wystąpienia;
4) postępowanie z ryzykiem w celu zredukowania ryzyka;
5) informowanie o ryzyku interesariuszy i konsultacje eksperckie;
6) monitorowanie i przegląd ryzyka oraz procesu zarządzania ryzykiem.

Utrzymywanie zgodności ochrony danych osobowych z podejściem opartym na ryzyku nie jest obowiązkowe dla każdej operacji przetwarzania. Przeprowadzenie oceny skutków dla ochrony danych osobowych jest obowiązkowe jedynie wtedy, gdy przetwarzanie „może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 35 ust. 1, 3 i 4 RODO). Jest to szczególnie ważne w przypadku wprowadzania nowych technologii lub rozwiązań dotyczących przetwarzania danych.

W sytuacjach, gdy nie jest jasne czy ocena skutków dla ochrony danych osobowych jest wymagana, zaleca się jej wykonanie. Ocena skutków dla ochrony danych osobowych jest mechanizmem, który pomaga administratorom danych zachowanie zgodności z prawem.

Zgodnie z art. 35 ust. 3 RODO ocena skutków dla ochrony danych osobowych jest wymagana w szczególności w przypadku:

1) systematycznego opisu planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie do prawnie uzasadnionych interesów realizowanych przez administratora;
2) oceny czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
3) oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w art. 35 ust. 1 RODO[1];
4) środków planowanych w celu zaradzenia ryzyku, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.

[1] Art. 35 ust. 1 RODO: Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Znaczenie i rola niniejszego przepisu została wyjaśniona w motywie 84 preambuły RODO w następujący sposób: „Aby poprawić przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora danych do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym".

Otwarty katalog sytuacji wymagających oceny skutków dla ochrony danych osobowych

Warto zwrócić uwagę na wyrażenie „w szczególności" zawarte w zdaniu poprzedzającym wyliczenie w art. 35 ust. 3. RODO, które wskazuje na otwarty katalog sytuacji wymagających oceny skutków dla ochrony danych osobowych. Mogą zatem wystąpić operacje przetwarzania, które nie są objęte tą listą, ale jednocześnie stanowią podobne zagrożenia. Te operacje przetwarzania również muszą podlegać ocenie skutków dla ochrony danych osobowych.

Warto podkreślić, że ocena skutków dla ochrony danych, w rozumieniu RODO, jest narzędziem do zarządzania ryzykiem w kontekście ochrony praw i wolności osób fizycznych, których dane dotyczą. Natomiast w zarządzaniu ryzykiem bezpieczeństwa informacji skupiamy się na ryzykach i konsekwencjach dla organizacji, a nie na osobach fizycznych.

Artykuł 35 RODO odnosi się do prawdopodobnego wysokiego ryzyka „w odniesieniu do praw i wolności jednostek". Jak wskazano w opinii Grupy Roboczej ds. Ochrony Danych 29 14/EN WP 218, odniesienie do praw i wolności osób, których dane dotyczą, dotyczy przede wszystkim prawa do prywatności, ale może obejmować również inne podstawowe prawa, takie jak wolność słowa, wolność myśli, swoboda przemieszczania się, zakaz dyskryminacji, prawo do wolności sumienia i religii.

Metodyki zarządzania ryzykiem

Aktualnie tematyka zarządzania ryzykiem w ochronie danych osobowych jest nowym obszarem, w którym brakuje opracowań i praktycznych wskazówek dotyczących sposobu realizacji i oceny ryzyka.

W Europie identyfikuje się takie podejścia jak:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 201627. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798
- UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

W Polsce prace nad opracowaniem metodyki zarządzania ryzykiem w ochronie danych osobowych pod egidą Ministerstwa Cyfryzacji i Polskiego Komitetu Normalizacyjnego prowadzi Fundacja Bezpieczeństwa Informacji Polska.

Celem przedsięwzięcia jest bezpłatne udostępnienie metodyki (podręcznika), opisującego proponowany sposób spełnienia i realizacji wymagania dot. oceny skutków dla ochrony danych osobowych na zasadach licencji Creative Commons typu CC BY-NC-ND.

Dokument swoim zakresem będzie opisywać:

1) proces zarządzania ryzykiem w ochronie danych osobowych (w tym role i odpowiedzialności);
2) metodykę przeprowadzenia analizy i oceny ryzyka;
3) przykłady zastosowania metodyki w praktyce;
4) oddziaływanie przeprowadzonej oceny ryzyka na dobór adekwatnych zabezpieczeń organizacyjnych i technicznych;
5) monitorowanie, przeglądy i informowanie o ryzyka związanym z ochroną danych osobowych.

Przygotowywana metodyka jest konsultowana szeroko, dlatego też każdą zainteresowaną osobę zainteresowaną zaopiniowaniem dokumentu Fundacja zaprasza do współpracy.

Kontakt e-mail:
kamil.pszczolkowski@fbipolska.pl

Podstawa prawna

- art. 25, art. 35 ust. 1 i ust. 3–4, ust. 10 rozporządzeniu 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. L Nr 119 z 4.5.2016 r., s. 1–88)

PROJEKT „RODO 2018”

Lid krótkie wprowadzenie.

Autor
Opis autora

Z kim go zrealizować?

Wypełnienie postanowień europejskiego rozporządzenia o ochronie danych osobowych (RODO) to złożony i wieloetapowy proces wymagający określenia przez administratora danych zakresu prac, przewidywanych kosztów, czasu realizacji oraz niezbędnych zasobów.

Ze względu na interdyscyplinarny charakter RODO (połączenie wiedzy m.in. z dziedziny prawa, informatyki, ciągłości działania, zarządzania kryzysowego) okazuje się często, że posiadane zasoby ludzkie nie gwarantują sukcesu planowanego projektu. Organizacje stają wówczas przed trudnym pytaniem: kto może nam pomóc we wdrożeniu RODO?

Wybór rzetelnego partnera może nastręczać trudności, tym bardziej, że im bliżej 25.5.2018 r., tym coraz więcej firm oferuje usługi z zakresu ochrony danych osobowych.

Jak zatem wybrać właściwego konsultanta?

Oto elementy, które warto wziąć pod uwagę.

1. Doświadczenie w ochronie danych osobowych

RODO, inaczej niż obecne przepisy, nie zawiera gotowego katalogu obowiązków do „odhaczenia”. Po 25.5.2018 r. każda organizacja samodzielnie będzie decydować m.in. jak często zmieniać hasła do systemów informatycznych, jakie procedury znajdą się w polityce bezpieczeństwa i jak należy zabezpieczyć służbowe urządzenia mobilne.

Skuteczną implementację wymagań RODO w organizacji gwarantuje jedynie wyspecjalizowany podmiot mający odpowiednie doświadczenie w projektowaniu, wdrażaniu oraz utrzymaniu systemów ochrony danych osobowych. Tylko doświadczona firma doradcza jest w stanie zarekomendować adekwatne i racjonalne kosztowo środki ochrony danych.

2. Interdyscyplinarny zespół ekspertów

Projekt „RODO 2018” jest działaniem zespołowym, realizowanym na kilku płaszczyznach – zarządczej, prawnej oraz informatycznej.

Wielopoziomowość zmian sprawia, że profesjonalna firma doradcza wpierająca proces wdrożenia RODO musi dysponować interdyscyplinarnym zespołem ekspertów posiadających kompetencje, potwierdzone certyfikatami, m.in. w dziedzinie prawa, zarządzania bezpieczeństwem informacji, usługami informatycznymi, ciągłością działania oraz zarządzania kryzysowego.

Nawet najlepszy specjalista jednoosobowo nie przygotuje organizacji do stosowania RODO.

3. Metodyka prac

Projekt „RODO 2018" to ogromna ilość ludzkiej pracy, dlatego niezwykle ważne jest jej dobre zaplanowanie. Profesjonalna firma doradcza mająca wspierać wdrożenie RODO musi dostarczyć uznaną metodykę zarządzania projektami (zgodną np. z PRINCE2, COBIT, SCRUM), niezbędną do przeprowadzenia terminowego i efektywnego wdrożenia. Intuicyjne zarządzanie projektami może prowadzić do wydłużenia czasu wdrożenia, zwiększenia kosztów projektu oraz zniechęcenia uczestników do pracy.

4. Zakres wsparcia podczas wdrożenia

RODO wymaga zaangażowania się organizacji w budowę własnego systemu ochrony danych osobowych, adekwatnego do profilu prowadzonej działalności. Implementację jego (RODO) postanowień można przyrównać do budowy systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001. Profesjonalna firma doradcza zapewnia wsparcie na każdym z kolejnych etapów wdrożenia, tj.:

1) ustaleniu gotowości organizacji do stosowania RODO (audyt otwarcia);
2) przeprowadzeniu procesów analizy wpływu na prywatność (DPIA);
3) przeprowadzeniu procesu szacowania ryzyka;
4) przystosowaniu funkcjonujących procedur i polityk przetwarzania danych do wymagań RODO;
5) przystosowaniu środowiska teleinformatycznego do wymagań RODO;
6) szkoleniu dla personelu organizacji;
7) potwierdzeniu organizacji do stosowania RODO (audyt zamknięcia).

5. Czas realizacji projektu

Przygotowanie organizacji do stosowania RODO wymaga czasu i zależy od szeregu czynników, m.in. od wielkości organizacji, podejmowanych wcześniej działań w zakresie ochrony danych osobowych oraz świadomości i zaangażowania najwyższego kierownictwa. Ze względu na stopień skomplikowania projektu „RODO 2018" czas jego realizacji wynosi od kilku do kilkunastu miesięcy. Profesjonalna firma doradcza, podejmując się pomocy przy wdrożeniu RODO, powinna w sposób metodyczny oszacować czas potrzebny na realizację projektu (np. z wykorzystaniem metodyki PERT) oraz kontrolować postępy w jego realizacji (np. z wykorzystaniem wykresu Gantta).

6. Cena

Każda organizacja stara się osiągnąć maksymalny efekt przy minimalnym nakładzie środków, dlatego cena stanowi istotne kryterium wyboru firmy doradczej. Wybierając partnera należy jednak sprawdzić, jakie elementy wdrożenia objęte są zaproponowaną ceną oraz czy nie istnieją opłaty dodatkowe. Korzystna propozycja współpracy powinna obejmować dostosowanie wszystkich realizowanych przez organizację procesów przetwarzania danych osobowych, a nie jedynie ich część.

Powierzenia osobie – pełniącej funkcję sołtysa – obowiązku doręczania pism

„Czy sołtysi, którzy roznoszą mieszkańcom gminy decyzje o wymiarze podatku, powinni mieć nadane przez wójta upoważnienia do przetwarzania danych? Zaznaczę, że przekazywane sołtysom do dostarczenia decyzje nie są w żaden sposób pakowane/kopertowane, mają oni także dostęp do imion i nazwisk właścicieli i współwłaścicieli gruntów i budynków, kwot należnego podatku, wysokości ewentualnych zaległości, informacji dot. posiadanych nieruchomości (numery działek, powierzchnia itp.). Jeżeli należy im nadać upoważnienia, to rozumiem, że powinni zostać przeszkoleni z zakresu ochrony danych osobowych? Czy wtedy powinni zapoznać się także z polityką bezpieczeństwa funkcjonującą w urzędzie? Czy zakopertowanie tych decyzji pozwoliłoby uniknąć nadawania upoważnień i szkolenia ww. osób? Oczywiście w sytuacji zakopertowania decyzji sołtysi nadal będą mieli dostęp do imion i nazwisk właścicieli i współwłaścicieli nieruchomości oraz ich adresów zamieszkania."

ODPOWIEDŹ

Zgodnie z art. 144 § 4 ustawy z 29.8.1997 r. – Ordynacja podatkowa (t.j. Dz.U. z 2017 r. poz. 201 ze zm.) w przypadku, gdy organem podatkowym jest wójt, burmistrz (prezydent miasta), sołtys może doręczać, za pokwitowaniem, pisma w postępowaniu podatkowym. Przywołany przepis stanowi podstawę do powierzenia osobie – pełniącej funkcję sołtysa – obowiązku doręczania pism w postępowaniu podatkowym. Wskazana podstawa prawna nie znosi jednak ciążącego na administratorze danych obowiązku wydania odpowiedniego upoważnienia do przetwarzania danych osobowych w rozumieniu ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922; dalej: OchrDanychU).

Zgodnie z art. 37 OchrDanychU do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych. Dopuszczenie do przetwarzania danych osób nielegitymujących się wymaganym upoważnieniem może narazić administratora danych na zarzut niewłaściwego zabezpieczenia danych. Obowiązek nadania odpowiednich upoważnień jest niezależny od tego, czy dostęp do danych ma charakter stały lub czasowy.

Z punktu widzenia ochrony danych osobowych, sołtys powinien zostać upoważniony do przetwarzania danych osobowych niezależnie od tego czy doręczane dokumenty zostaną zapakowane w koperty, czy też nie. Niewątpliwie bowiem w obu przypadkach ma on dostęp do danych osobowych adresatów, choć w przypadku doręczania zapakowanej korespondencji zakres dostępu danych osobowych jest węższy.

Ze względu na ciążący na administratorze obowiązek zabezpieczenia danych osobowych skłaniać się należy do kopertowania przesyłek. Taka praktyka ogranicza ryzyko ujawnienia osobom trzecim, danych osobowych adresatów przesyłki wykraczających poza ich dane adresowe, np. w sytuacji doręczenia zastępczego przesyłki: sąsiadowi adresata, zarządcy domu lub dozorcy.

Realizując szkolenie z ochrony danych osobowych administrator danych nie ma obowiązku zapoznania sołtysów z całą dokumentacją ochrony danych przyjętą w urzędzie – obowiązek przeszkolenia sołtysów powinien zostać zrealizowany w zakresie odpowiadającym nałożonemu na nich obowiązkowi doręczania pism.

Adwokat Marta Kwiatkowska-Cylke
Lubasz i Wspólnicy
Kancelaria radców prawnnych

Podstawa prawna

- art. 144 § 4 ustawy z 29.8.1997 r. – Ordynacja podatkowa (t.j. Dz.U. z 2017 r. poz. 201 ze zm.)
- art. 37 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922)

Klauzula informacyjna o przetwarzaniu danych dla osoby, której dane dotyczą

Agnieszka Kręcisz-Sarna
Radca prawny

Od 25 maja 2018 r. stosowane przez administratorów danych klauzule informacyjne o przetwarzaniu danych powinny uwzględniać wymogi wynikające z ogólnego rozporządzenia o ochronie danych. Konieczne będzie nie tylko uzupełnienie dotychczas stosowanych klauzul o dodatkowe informacje, ale także ich przeformułowanie w taki sposób, aby zawierały zrozumiały i zwięzły przekaz dla osób, do których są kierowane. Dodatkowych trudności może nastręczać obowiązek dopasowywania zakresu przekazywanych informacji do konkretnego procesu przetwarzania danych osobowych.

Zakres informacji, które powinny być podawane osobie, od której administrator danych bezpośrednio pozyskuje dane określa art. 13 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 (Dz.Urz. UE L Nr 119 z 4.5.2016 r., s. 1–88; dalej: RODO). Katalog tych informacji jest znacznie szerszy niż wynika to z obecnie obowiązujących w Polsce przepisów.

Ważne

Mieszczą się w nim informacje, które administratorzy danych powinni przekazywać podmiotowi danych zawsze i niezależnie od okoliczności związanych z przetwarzaniem danych.

Ponadto są w nim informacje, których obowiązek przekazania powstaje dla administratorów z uwagi na okoliczności ich dotyczące, podstawę prawną przetwarzania danych czy zasady przetwarzania.

Przygotowany wzór klauzuli informacyjnej o przetwarzaniu danych dla osoby, której dane dotyczą obejmuje pełen zakres informacji wymaganych przez art. 13 RODO ze wskazaniem, które z nich i w jakich okolicznościach powinny być przez administratora danych uwzględniane.

Klauzula informacyjna o przetwarzaniu danych[1],[2],[3]

Na podstawie art. 13 ust. 1 i ust. 2 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 (dalej: RODO), informuję, że:

Administrator danych:

Administratorem Pani/Pana danych osobowych jest …… z siedzibą w ……, ul. ……, kod pocztowy ……, e-mail: ……, tel. ……..…

Przedstawiciel administratora danych[4]:

Nie dotyczy/Przedstawicielem administratora danych osobowych w Polsce jest …… Pani/Pan ……, ul. ……, …., e-mail: ……..…, tel. ……

Inspektor ochrony danych[5]:

Nie dotyczy./Dane kontaktowe inspektora ochrony danych w …… z siedzibą w …… (nazwa administratora danych) to: ul. ……, …., e-mail: ……..…, tel. ……

Cele przetwarzania danych osobowych oraz podstawa prawna przetwarzania:

Przetwarzanie Pani/Pana danych osobowych odbywać się będzie na podstawie art. …… RODO i wyłącznie w celu ……

Prawnie uzasadniony interes[6]:

Nie dotyczy/Prawnie uzasadnionym interesem, na który powołuje się administrator danych jest ……

Okres przechowywania danych osobowych[7]:

Pani/Pana dane osobowe będą przechowywane przez okres …… /do czasu ……

Prawo dostępu do danych osobowych[8]:

Posiada Pani/Pan prawo dostępu do treści swoich danych osobowych, prawo do ich sprostowania, usunięcia oraz prawo do ograniczenia ich przetwarzania. / Ponadto także prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, prawo do przenoszenia danych oraz prawo do wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych osobowych.

Prawo wniesienia skargi do organu nadzorczego:

Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. …… gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

Konsekwencje niepodania danych osobowych:

Podanie przez Panią/Pana danych osobowych jest wymogiem umownym/ustawowym/warunkiem zawarcia umowy ……, a ich niepodanie będzie skutkowało ……
……..…

Odbiorcy danych[9]:

1. Nie dotyczy/Pani/Pana dane osobowe nie będą przekazywane żadnym odbiorcom danych.

2. Odbiorcą Pani/Pana danych osobowych będzie ……

Przekazanie danych do państwa trzeciego/organizacji międzynarodowej[10]:

1. Nie dotyczy/Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

2.

a) Pani/Pana dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej …… na podstawie decyzji Komisji Europejskiej nr …… z dnia … stwierdzającej odpowiedni stopień ochrony.

b) Pani/Pana dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej …… Z uwagi na brak decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony administrator danych będzie stosował środki rekompensujące brak ochrony danych poprzez odpowiednie zabezpieczenie Pani/Pana danych osobowych za pomocą:
   - prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi w postaci ……;
   - wiążących reguł korporacyjnych …… zatwierdzonych przez Prezesa Urzędu Ochrony Danych Osobowych;
   - standardowych klauzul ochrony danych przyjętych przez Komisję Europejską ……;
   - standardowych klauzul ochrony danych przyjętych przez Prezesa Urzędu Ochrony Danych Osobowych i zatwierdzonych przez Komisję Europejską ……;
   - zatwierdzonego przez Prezesa Urzędu Ochrony Danych Osobowych kodeksu postępowania ……;
   - zatwierdzonego przez podmiot certyfikujący …… mechanizmu certyfikacji w postaci ……;
   - zezwolenia Prezesa Urzędu Ochrony Danych Osobowych na klauzule umowne ……;
   - zezwolenia Prezesa Urzędu Ochrony Danych Osobowych na postanowienia uzgodnień administracyjnych między organami lub podmiotami publicznymi ……;

c) Pani/Pana dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej …… na podstawie …… (jeden z wyjątków z art. 49 RODO).

d) Pani/Pana dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej …… ze względu na ważny prawnie uzasadniony interes realizowany przez administratora danych tj. …… Administrator danych zapewnia odpowiednie zabezpieczenia w zakresie ochrony Pani/Pana danych osobowych.

Kopię danych osobowych przekazywanych do państwa trzeciego może Pani/Pan uzyskać poprzez …… lub w miejscu udostępnienia danych ……

Zautomatyzowane podejmowanie decyzji, profilowanie[11]:

1. Nie dotyczy/Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany i nie będą profilowane.

2. Pani/Pana dane osobowe będą przetwarzane w sposób zautomatyzowany, co będzie odbywało się na zasadach …… Pani/Pana dane osobowe będą przetwarzane także w formie profilowania/wykorzystywane do tworzenia profili …… Konsekwencją wskazanych sposobów przetwarzania danych będzie …… co oznaczać będzie, że …… .

Objaśnienia

[1] Obowiązek informacyjny
Administrator danych zobowiązany jest podczas zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą do przekazania tej osobie informacji o zasadach przetwarzania jej danych. Forma oraz zakres udzielanych informacji określone zostały w art. 12 i 13 RODO. Administrator danych musi zadbać, aby przekazywana informacja zawierała wszystkie wymagane przez unijne rozporządzenie w danych okolicznościach faktycznych elementy, a także, by forma udzielanej informacji była zgodna z wytycznymi zawartymi w rozporządzeniu.

[2] Forma przekazania informacji
RODO zobowiązuje administratora danych do komunikowania się w sposób przejrzysty i zrozumiały z osobą, od której pozyskuje dane osobowe. W konsekwencji oznacza to, że informacja o zasadach przetwarzania jej danych osobowych, przygotowana przez administratora danych, powinna być zwięzła i jasna. Powinna być sporządzona w łatwo dostępnej formie i prostym językiem. W tym celu administrator danych może posłużyć się np. standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania danych (jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego). Pomocne w tym zakresie będą wskazówki Komisji Europejskiej, której przyznano uprawnienie do wydawania aktów delegowanych określających m.in. informacje przedstawiane za pomocą znaków graficznych i procedury ustanowienia standardowych znaków graficznych.

[3] Sposób przekazania informacji
Informacja może być udzielona w formie pisemnej lub w inny sposób np. elektronicznie. Można ją również przekazać ustnie, jeżeli osoba, której dane dotyczą, tego zażąda, o ile innymi sposobami potwierdzi się tożsamość tej osoby. Ważne aby administrator danych był w stanie wykazać, że dopełnił obowiązku informacyjnego.

[4] Przedstawiciel administratora danych
Obowiązek wskazania danych przedstawiciela dotyczy tylko takiego administratora danych, który nie posiada jednostki organizacyjnej na terenie Unii (np. w Polsce) i wyznaczył na terenie Unii (np. w Polsce) swojego przedstawiciela w celu podejmowania działań w jego imieniu w zakresie obowiązków administratora danych.

[5] Inspektor ochrony danych
Jeśli administrator powołał inspektora ochrony danych (art. 37 RODO) zobowiązany jest w zawiadomieniu o zasadach przetwarzania danych podać dane kontaktowe tej osoby.

[6] Prawnie usprawiedliwiony interes
Gdy podstawą przetwarzania danych osobowych jest prawnie usprawiedliwiony interes administratora danych lub strony trzeciej (art. 6 ust. 1 lit. f) RODO) w klauzuli informacyjnej należy wskazać ten interes np. dochodzenie roszczeń cywilnoprawnych z tytułu naruszenia dóbr osobistych, zapewnienie bezpieczeństwa osób i mienia w obszarze objętym monitoringiem.

[7] Okres przechowywania danych
W informacji przekazywanej podmiotowi danych należy wskazać okres przez jaki jego dane będą przetwarzane, a jeśli nie jest możliwe jego precyzyjne określenie należy wskazać kryteria ustalania tego okresu np. zakończenie realizacji umowy, zakończenie procesu rekrutacji.

[8] Prawa osoby, której dane dotyczą
Administrator ma obowiązek poinformowania osoby, której dane zamierza przetwarzać o przysługujących jej prawach, w szczególności o prawie dostępu do danych, sprostowania danych, ograniczenia przetwarzania i usunięcia danych. W zależności od podstawy, na jakiej administrator opiera proces przetwarzania danych osobowych może być zobowiązany do zawiadomienia podmiotu danych o kolejnych przysługujących mu na mocy unijnego rozporządzenia uprawnieniach. Jeżeli przetwarzanie danych odbywa się na podstawie zgody podmiotu danych administrator zobowiązany jest poinformować o prawie do cofnięcia zgody w dowolnym momencie. Przy czym powinien zastrzec, że cofnięcie zgody pozostaje bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Jeżeli przetwarzanie danych odbywa się na podstawie zgody podmiotu danych lub umowy oraz w sposób zautomatyzowany, to dodatkowo należy poinformować o prawie do przenoszenia danych. W przypadku zaś gdy przetwarzanie danych oparte jest o przesłanki z art. 6 ust. 1 lit. e) lub f) RODO, lub gdy dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, do celów badań naukowych, historycznych lub do celów statystycznych, administrator danych powinien dodatkowo

poinformować osobę, której dane dotyczą, o prawie do wniesienia sprzeciwu wobec przetwarzania dotyczących jej danych osobowych.

[9] Odbiorcy danych

Jeśli administrator danych przekazuje dane odbiorcom danych, to w klauzuli informacyjnej należy umieścić wzmiankę o odbiorcach danych osobowych lub o kategoriach tych odbiorców.

[10] Przekazanie danych do państwa trzeciego/organizacji międzynarodowej

Gdy administrator zamierza przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej to po pierwsze, powinien o tym zamiarze poinformować osobę, której dane dotyczą. Po drugie, powinien wskazać warunki transferu danych do państwa trzeciego, zgodnie z wymogami ogólnego rozporządzenia o ochronie danych. W szczególności może powołać się na decyzję Komisji stwierdzającą odpowiedni poziom ochrony (np. decyzja Komisji Europejskiej z 12.7.2016 r. dotycząca USA, tzw. Privacy Shield), a w razie braku takiej decyzji zadeklarować odpowiedni poziom ochrony danych za pomocą jednego z instrumentów wskazanych w art. 46 RODO. Istnieje także możliwość powołania się na jeden z wyjątków opisanych w art. 49 RODO lub na ważny prawnie uzasadniony interes realizowany przez administratora danych w okolicznościach opisanych w art. 49 ust. 1 zdanie drugie RODO.

[11] Zautomatyzowane podejmowanie decyzji, profilowanie

Administrator danych, który przetwarza dane stosując metodę zautomatyzowanego podejmowania decyzji, w tym profilowanie, zobowiązany jest przekazać osobie, której dane dotyczą istotne informacje o zasadach ich stosowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania danych w odniesieniu do osoby, której dane dotyczą.

▶ Podstawa prawna

- art. 12, art. 13, art. 44–49 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 z 4.5.2016 r. s. 1–88)

Obowiązek informacyjny administratora danych – schemat postępowania

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

Od momentu pozyskania danych osobowych na ich administratorze ciąży wiele obowiązków. Jednym z nich jest, wynikający z art. 24 i 25 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922; dalej: OchrDanychU), obowiązek informacyjny. Polega on na przekazaniu każdej osobie, której dane są przetwarzane, pewnych informacji dotyczących samego administratora danych, jak też prowadzonego przez niego procesu przetwarzania danych. Uprawnienie do uzyskania tych informacji jest niezależne od aktywności osoby, której dane dotyczą i wynika z samego faktu pozyskania jej danych przez administratora. Obowiązek ten jest zróżnicowany, w zależności od kogo administrator dane osobowe pozyskuje.

Legalne pozyskanie danych

Zanim administrator pozyska dane musi upewnić się jednak, że ich zebranie będzie w określonej sytuacji legalne i że jest on uprawniony do późniejszego przetwarzania tych danych. Tym samym musi on sprawdzić, czy legitymuje się jedną z przesłanek legalizujących proces przetwarzania danych, które są określone w art. 23 ust. 1 pkt 1–5 OchrDanychU (w stosunku do danych osobowych zwykłych takich jak: imię i nazwisko, adres zamieszkania, nr PESEL) oraz w art. 27 ust. 2 pkt 1–10 OchrDanychU (w stosunku do tzw. danych szczególnie chronionych, określonych w art. 27 ust. 1 OchrDanychU). Legalne pozyskanie danych jest podstawą do realizacji dalszych obowiązków administratora, wynikających z OchrDanychU.

Zebranie danych od osoby, której dane dotyczą

Jak stanowi art. 24 ust. 1 OchrDanychU, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować ją o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach bądź kategoriach odbiorców danych;
3) prawie dostępu do treści swoich danych oraz ich poprawiania;

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Przekazanie tych informacji może nastąpić w dowolnej formie. W praktyce administratorzy danych często stosują tzw. klauzule informacyjne, stanowiące element wszelkiego rodzaju formularzy, za pośrednictwem których osoby, których dane dotyczą, przekazują im swoje dane. Podpis zainteresowanego pod takim dokumentem ma dawać gwarancję, że zapoznał się on ze stosowną informacją. Takie rozwiązanie niewątpliwie spełnia wymogi cytowanego przepisu, lecz pamiętajmy, że nie jest jedynym dopuszczalnym. Przy wypełnianiu obowiązku informacyjnego chodzi bowiem o to, by informacja o administratorze danych faktycznie trafiła do zainteresowanej osoby, a nie by przybrała tę lub inną postać. Obowiązek ten może być zatem wypełniony także przez umieszczenie odpowiedniej informacji w regulaminie świadczenia usługi, przez złożenie stosownego oświadczenia, a w pewnych sytuacjach nawet przez wywieszenie odpowiedniej informacji (np. gdy dane gromadzone są w miejscu, gdzie informacja ta jest umieszczona w sposób zapewniający łatwe i odruchowe zapoznanie się z nią).

Jak wynika z cytowanego przepisu, administrator danych jest zwolniony z omawianego obowiązku jedynie wówczas, gdy:

1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub
2) osoba, której dane dotyczą, posiada informacje, o których mowa w art. 24 ust. 1 OchrDanychU.

PRZYKŁAD

Przykładem takiej sytuacji, który zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania, jest art. 17 ust. 2 ustawy z 16.3.2001 r. o Biurze Ochrony Rządu (t.j. Dz.U. z 2017 r. poz. 985 ze zm.), który daje tej służbie prawo do przetwarzania danych osobowych bez wiedzy i zgody osoby, której one dotyczą, o ile służy to realizacji zadań tej służby określonych w ustawie.

W drugim z omawianych przypadków administrator danych powinien mieć pewność, co do tego, że osoba zainteresowana posiada wszystkie informacje. Będzie miało to miejsce np. wtedy, gdy osoba zainteresowana „zna administratora danych, orientuje się co do celu zbierania danych, wie, czy jest zobowiązany przepisami prawa do udzielenia informacji”[1].

Pozyskiwanie danych z innego źródła

Obowiązek informacyjny wygląda inaczej, gdy administrator danych pozyskuje je nie bezpośrednio od osoby, której dane dotyczą, a z innego źródła. W pierwszej kolejności szerszy jest zakres informacji, jakie muszą być przekazywane zainteresowanemu. Zgodnie z art. 25 ust. 1 OchrDanychU w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
3) źródle danych;
4) prawie dostępu do treści swoich danych oraz ich poprawiania;
5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 OchrDanychU, czyli prawie do wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 OchrDanychU, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację oraz wniesienia w tych przypadkach sprzeciwu wobec przetwarzania jej danych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

Jak widać, w sytuacji, gdy administrator danych pozyskał je z innego źródła, osoba, której dane dotyczą, musi uzyskać dodatkowe informacje o tym skąd administrator ma jej dane oraz jakie uprawnienia przysługują jej na podstawie przepisów ustawy.

W omawianym przypadku pozyskania danych ważny jest też moment przekazania informacji przez administratora. Z ustawy wynika, że powinno to nastąpić bezpośrednio po utrwaleniu danych. Wydaje się, że może się to odbyć przy okazji pierwszej operacji na danych (ich wykorzystania), w tej jednak sytuacji operacja ta powinna być przeprowadzona w możliwie minimalnym odstępie czasu od zgromadzenia danych.

Forma przekazania informacji jest właściwie dowolna (tak jak przy pozyskaniu danych od osoby, której dane dotyczą) ważne jest jedynie, by administrator danych umiał dowieść, że omawiany obowiązek wypełnił.

Administrator danych jest zwolniony z tego obowiązku informacyjnego tylko wówczas, gdy:

1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;
2) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich prze-

[1] *J. Barta, P. Fajgielski, R. Markiewicz*, Ochrona danych osobowych. Komentarz, wyd. III, Kraków 2004, s. 317.

twarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań informacyjnych wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;

3) dane są przetwarzane przez administratorów danych, będących organami państwowymi, organami samorządu terytorialnego oraz państwowymi i komunalnymi jednostkami organizacyjnymi, jak też podmiotami niepublicznymi realizującymi zadania publiczne, na podstawie przepisów prawa;
4) osoba, której dane dotyczą, posiada omawiane informacje.

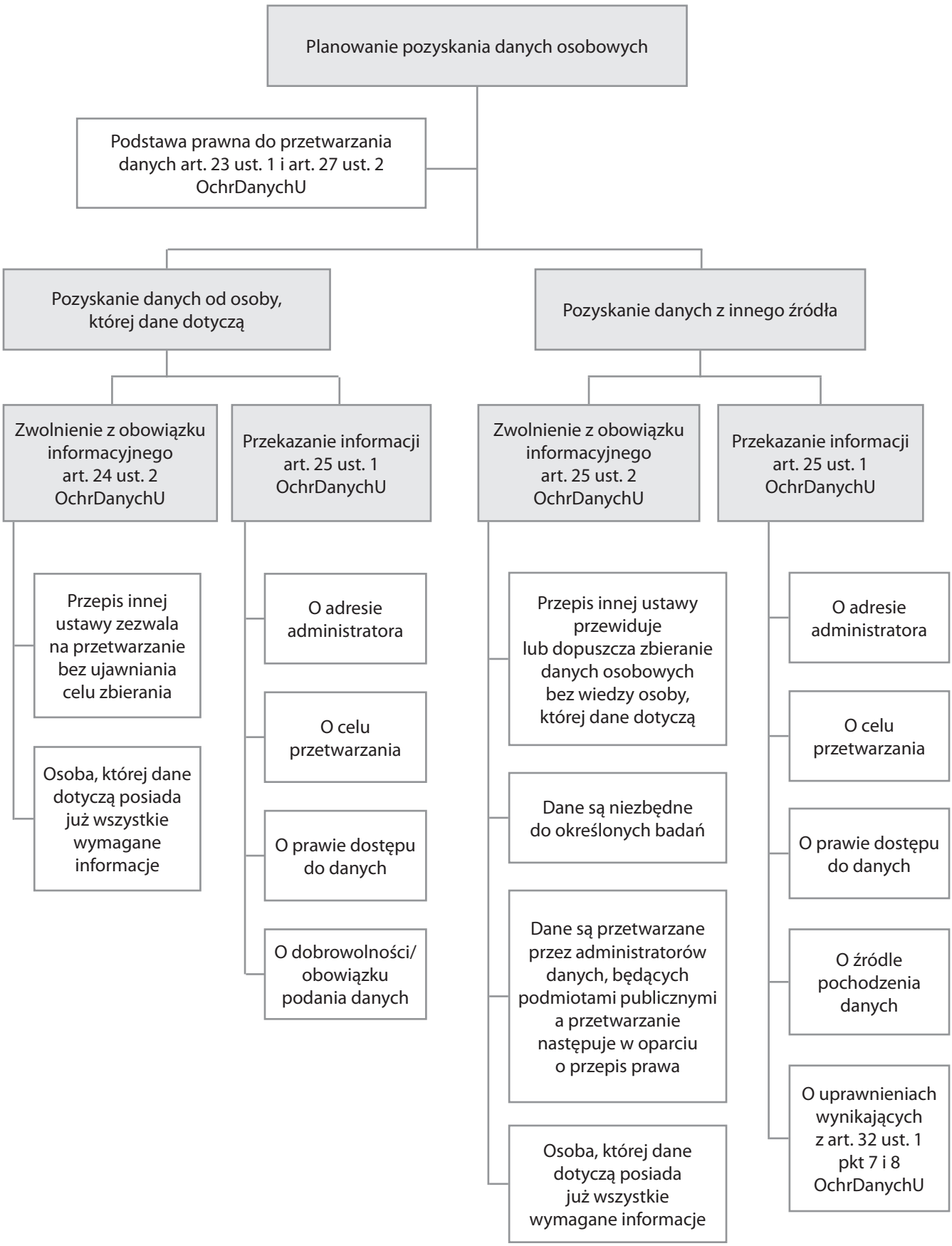
Jak widać katalog zwolnień został rozszerzony, w porównaniu z sytuacją zbierania danych od osoby, której dane dotyczą. Warto zwrócić uwagę na zwolnienie dotyczące prowadzenia określonych badań, gdy spełnienie obowiązku informacyjnego byłoby nadmiernym obciążeniem i zagrażałoby realizacji celu badania. Jest to ciekawe rozwiązanie, gdyż ustawodawca zapewnia, by ochrona danych nie blokowała rozwoju nauki rozumianej jako pewne dobro wspólne.

Zwolnione z realizacji omawianego obowiązku są również podmioty publiczne i podmioty niepubliczne realizujące zadania publiczne, o ile przetwarzają dane osobowe w oparciu o przepisy prawa. W praktyce, by podmiot taki mógł skorzystać ze zwolnienia, powinien oprzeć proces przetwarzania danych na przesłance legalności określonej w art. 23 ust. 1 pkt 2 OchrDanychU. Zakres tego wyłączenia jest bardzo obszerny. Zwolnienie to chroni podmioty realizujące zadania publiczne przed rygoryzmem ustawy i stawia interes ogółu nad ochroną praw jednostki.

Podstawa prawna

- art. 24, art. 25 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922)

Schemat: obowiązek informacyjny administratora danych



Czy istnieje obowiązek podania numeru rejestracyjnego pojazdu podczas zakupu biletu w parkomacie

dr Jowita Sobczak
Ekspert ds. bezpieczeństwa informacji,
wykładowca Społecznej Akademii Nauk

Artykuł opisuje stanowisko WSA w Warszawie z 13.4.2017 r. (VII SA/Wa 1069/16, Legalis) zgodnie z którym numery rejestracyjne pojazdów samochodowych stanowią dane osobowe, a obowiązek podania ich podczas zakupu biletu w parkomacie jest łamaniem przepisów prawa, w tym naruszeniem wolności wynikającej z Konstytucji RP. Zdaniem sądu bilet można opłacić bez podania numeru rejestracyjnego pojazdu.

Powyższe stanowisko sądu ma niezwykle istotne znaczenie dla praktyki realizacji obowiązków przez administrację publiczną w tym obszarze oraz osób, których dane są przetwarzane w tym zakresie.

Stan faktyczny

Rada Miasta [...] w dniu [..] czerwca 2008 r. podjęła uchwałę nr [...] w sprawie ustalenia strefy płatnego parkowania, wysokości stawek opłaty za parkowanie pojazdów samochodowych na drogach publicznych w strefie, wysokości opłaty dodatkowej oraz określenia sposobu pobierania tych opłat (Dz.Urz. Woj. Maz. Nr 138, poz. 4868).

W dniu [...] kwietnia 2016 r. *M.S.* złożył do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na ww. uchwałę Rady Miasta. Stwierdził on, że przedmiotowa uchwała została wydana z naruszeniem przepisów prawa. *M.S.* zakwestionował w ww. uchwale wymóg określający, że w przypadku zakupu biletu w parkomacie wyposażonym w klawiaturę, należy obowiązkowo podać numer rejestracyjny parkującego pojazdu. Zarzucił naruszenie następujących przepisów prawa:

1) art. 23 ust. 1 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922, dalej: OchrDanychU) polegające na nałożeniu w Uchwale obowiązku podania danych osobowych, w postaci numeru rejestracyjnego pojazdu, w sytuacji, gdy brak jest ustawowej podstawy przetwarzania tego rodzaju danych, a w szczególności, (…)
2) art. 47 oraz art. 51 ust. 1 i 2 ustawy z 2.4.1997 r. – Konstytucja

Teza

Uchwała Rady Miasta Stołecznego Warszawy, w której nakazano kierowcom, uiszczającym opłatę w parkomatach nowego typu – posiadających klawiaturę, podawać numery rejestracyjne samochodów, została wydana z naruszeniem prawa. W ocenie sądu organ nie wykazał prawnej podstawy do przetwarzania danych osobowych w postaci numerów rejestracyjnych aut.

Rzeczypospolitej Polskiej (Dz.U. Nr 78, poz. 483 ze zm. i sprost.; dalej: KonstU) polegające na naruszeniu prawa do prywatności poprzez zobowiązanie w Uchwale, do podania danych osobowych w postaci numeru rejestracyjnego parkującego pojazdu, podczas gdy zobowiązanie do ujawniania takich informacji może wynikać tylko z ustawy oraz powinno być zgodne z zasadą proporcjonalności, wynikającą z art. 31 ust. 3 KonstU oraz pozyskiwanie i gromadzenie tych informacji przez władzę publiczną powinno być niezbędne w demokratycznym państwie prawnym.

W odpowiedzi na skargę Rada Miasta [...] wniosła o jej oddalenie.

Obowiązek podania numeru rejestracyjnego pojazdu

Rada Miasta wskazała, że podanie numeru rejestracyjnego pojazdu na bilecie kontrolnym stanowi niepodważalny dowód na to, że dokonano opłaty za parkowanie danego pojazdu, a brak numeru oznacza, że jest wielce wątpliwe, czy takiej opłaty dokonano za parkowanie konkretnego pojazdu.

Ponadto według Rady Miasta, fakt zapisania na bilecie kontrolnym numeru rejestracyjnego pojazdu i wyłożenie biletu za przednią szyba pojazdu, nie narusza prawa do ochrony danych osobowych, bowiem dane te zostały przez skarżącego wcześniej udostępnione-upublicznione przez umocowanie na tym pojeździe tablicy z tym samym numerem rejestracyjnym.

Czy numer ewidencyjny pojazdu to dane osobowe?

Zgodnie z OchrDanychU za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Natomiast zgodnie z art. 7 pkt 2 OchrDanychU przetwarzanie danych to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Ponadto zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie z 9.4.2013 r. (II SA/Wa 211/13, Legalis) i wyrokiem z 25.4.2014 r. (II SA/Wa 30/14, Legalis) numer rejestracyjny pojazdu może prowadzić do identyfikacji osoby, a zatem może on stanowić dane osobowe w rozumieniu art. 6 OchrDanychU. W szczególności podkreślić należy, że Straż Miejska posiada prawo dostępu do danych zawartych w Centralnej Ewidencji Pojazdów i Kierowców, ma więc możliwość prostego ustalenia tożsamości właściciela pojazdu, posiadając numer rejestracyjny pojazdu.

Gromadzenie danych o numerach rejestracyjnych przez radę miasta

Rada Miasta stwierdziła, że uchwała nie nakłada na organ obowiązku podejmowania czynności polegających na gromadzeniu, czyli przetwarzaniu danych osobowych właścicieli pojazdów, bowiem fakt wydrukowania biletu z umieszczonym w jego treści numerem rejestracyjnym pojazdu nie musi oznaczać, że organ te numery gromadzi.

Sąd nie podzielił tego stanowiska.

Odnosząc się do stanowiska Rady Miasta należy odpowiedzieć na pytanie, czy parkomaty posiadają możliwość gromadzenia lub przesyłania wprowadzonych do niego danych. Odpowiedzią na to pytanie jest informacja umieszczona na parkomatach wyposażonych w klawiaturę do wprowadzania danych. Na każdym z nich zawarto informacje co do adresu siedziby i pełnej nazwy organu gromadzącego dane (administratora danych), w celu zbierania danych, prawie dostępu do treści swoich danych oraz ich poprawiania. Umieszczenie takich informacji jest obowiązkowe w przypadku zbierania danych osobowych i wynika z art. 24 ust. 1 OchrDanychU.

Należy podkreślić także, że Zarząd Dróg Miejskich zgłosił na podstawie art. 40 i nast. OchrDanychU zbiór danych osobowych o nazwie „Strefa Płatnego Parkowania". Do tego zbioru należą również informacje o numerach rejestracyjnych pojazdów parkujących w Strefach Płatnego Parkowania.

Rada Miasta wskazała, że podstawę wydania zaskarżonej uchwały upatruje m.in. w przepisach art. 23 ust. 1 OchrDanychU.

PRZYKŁAD

Przepis art. 23 ust. 1 pkt 3 OchrDanychU dopuszcza przetwarzanie danych, gdy jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną, lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. Jednak w ocenie Sądu w przypadku pobierania opłat za parkowanie w strefie płatnego parkowania nie dochodzi do zawierania umowy.

Przede wszystkim obowiązek uiszczania opłaty wynika z ustawy o dro-

gach publicznych, a nie z umowy. Poza tym, opłata za usługę stanowi daninę publiczną, a windykacja należności polegającej na obowiązku wniesienia opłaty dodatkowej z powodu nieuiszczenia opłaty, jest przeprowadzana w trybie egzekucji administracyjnej.

Co na to Konstytucja?

Nie można w tej sprawie nie dostrzec problemu konstytucyjnego. Zgodnie z brzmieniem art. 31 ust. 3 KonstU, ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw (tu prawa do decydowania o ujawnieniu swoich danych – art. 51 ust. 1 KonstU) mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Z przepisu tego wynika, że każdy obywatel może korzystać z konstytucyjnych wolności i praw w granicach zakreślonych przez ustawę, albowiem chroniąc sferę wolności obywatelskich, KonstU dopuszcza także ograniczenia w zakresie korzystania z konstytucyjnych praw i wolności, stanowiąc, że „mogą być ustanawiane tylko w ustawie" (*P. Barta*, *P. Litwiński*, Ustawa o ochronie danych osobowych. Komentarz, Legalis 2015).

Odnosząc się do cytowanego powyżej przepisu KonstU (art. 51), należy podkreślić przede wszystkim, że ustępy 2 i 3 tego przepisu ustanawiają m.in. fundamentalną zasadę przetwarzania danych przez władze publiczne tylko w zakresie niezbędnym w demokratycznym państwie prawa.

Artykuł 51 ust. 2 KonstU daje władzom publicznym uprawnienie do pozyskiwania, gromadzenia i udostępniania informacji o obywatelach. Dopuszczalny zakres przetwarzanych informacji wyznacza ich „niezbędność w demokratycznym państwie prawnym". Przy czym, nie ma ściśle wytyczonej granicy między informacją „niezbędną" a „zbędną". Trybunał Konstytucyjny odnosząc się do tego zagadnienia wskazał, że przesłanka „niezbędności" nie jest w art. 51 ust. 2 KonstU samodzielnie zdefiniowana. Nie powinno budzić wątpliwości, że pojęcie to nawiązuje do art. 31 ust. 3 KonstU (zasada proporcjonalności) – chociaż pełni tu rolę czynnika samoistnie ograniczającego wprost zakres gwarancji konstytucyjnej, podczas gdy zasada proporcjonalności uzasadnia ingerencję w treść samego prawa, niezależnie od jego ujęcia w normie konstytucyjnej. Pojęcie „niezbędności" powinno w konsekwencji uwzględniać co najmniej te same elementy, które KonstU wskazuje dla ustalenia, jakie wartości mogą w demokratycznym państwie uzasadniać konieczność ingerencji w sferę gwarantowanych konstytucyjnie praw i wolności, a mianowicie bezpieczeństwo, porządek publiczny, ochrona środowiska, zdrowia i moralności publicznej, a także wolności i prawa innych osób (wyr. TK z 12.11.2002 r., SK 40/01, Legalis).

Za niezbędne należało by więc uznać takie informacje, których posiadanie i udostępnianie jest warunkiem istnienia i efektywnego działania demokratycznego państwa prawnego; odpowiednio zbędne są informacje, które co prawda interesują administrację, ale bez których może ona działać i wypełniać swoje kompetencje.

Artykuł 51 ust. 1 KonstU potwierdza prawo jednostki do samodzielnego decydowania o ujawnianiu informacji o sobie. Obowiązek ujawnienia informacji o sobie stanowi ograniczenie autonomii informacyjnej. Ograniczenie takie może zostać wprowadzone tylko w drodze ustawy, przy czym nałożenie takiego obowiązku powinno mieścić się w granicach ingerencji państwa w sferę konstytucyjnych wolności i praw człowieka oraz obywatela, wyznaczonych przez art. 31 ust. 3 KonstU.

W ocenie sądu nałożenie takiego obowiązku w drodze uchwały rady miasta narusza art. 51 ust. 1 i 2 KonstU.

W świetle powyższych rozważań można przyjąć, że gromadzenie danych o numerach rejestracyjnych samochodów w związku z pobieraniem opłat za parkowanie w strefach płatnego parkowania niestrzeżonego nie jest niezbędne do efektywnego działania demokratycznego państwa prawnego.

Wojewódzki Sąd Administracyjny w Warszawie uznał, że skarga *M.S.* na uchwałę Rady Miasta jest zasadna. W ocenie Sądu stanowisko Rady Miasta w tym zakresie nie jest prawidłowe, gdyż realizacja wskazanego wyżej uprawnienia byłaby możliwa także bez przetwarzania informacji o numerach rejestracyjnych pojazdów.

Należy w tym miejscu wskazać, że Rada Miasta uzasadnia konieczność gromadzenia danych o numerach rejestracyjnych pojazdów potrzebami stosowania norm sankcjonujących. Jednak z norm sankcjonujących nie można wyprowadzać normy kompetencyjnej (kompetencji do gromadzenia i przetwarzania danych osobowych).

Z tych powodów zdaniem sądu art. 23 ust. 1 OchrDanychU nie może mieć zastosowania do uchwały w zaskarżonym zakresie, bowiem przetwarzanie żądanych danych osobowych nie jest niezbędne do zrealizowania uprawnienia Rady Miasta w zakresie ustalenia strefy płatnego parkowania oraz określenia sposobu pobierana opłaty za postój pojazdów samochodowych na drogach publicznych w strefie płatnego parkowania niestrzeżonego.

Podstawa prawna

- art. 23 ust. 1 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922)
- art. 47 oraz art. 51 ust. 1 i 2 ustawy z 2.4.1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. Nr 78, poz. 483 ze zm. i sprost.)

Temat numeru

O co chodzi z otwartością danych publicznych?

Anna Gos
Naczelnik Wydziału Polityki Otwartości Danych, Departament Rozwoju Usług Cyfrowych i Otwartości Danych w Ministerstwie Cyfryzacji

W najnowszym rankingu OECD Open, Useful, Reusable Government Data (OURDATA INDEX), opublikowanym w raporcie Government at a Glance 2017, Polska zajęła 20. miejsce na 31 badanych państw, przy uwzględnieniu dostępu i otwartości danych publicznych oraz rządowego wsparcia dla możliwości ponownego wykorzystywania informacji sektora publicznego[1]. Awansowaliśmy o 8 miejsc w stosunku do rankingu z 2015 r.

W 2015 r. na słabą pozycję Polski miało wpływ przede wszystkim podejście do udostępniania danych publicznych typu *top-down*, co oznaczało, że udostępniane są te dane, które administracja chce przekazać, a które niekoniecznie pokrywają się z potrzebami ze strony zainteresowanych danymi publicznymi, a także brak postrzegania otwartych danych publicznych jako siły napędowej lepszych usług publicznych czy tworzenia nowych produktów biznesowych.

W innej ocenie przeprowadzonej w ramach zleconego przez Komisję Europejską badania Open Data Maturity in Europe 2015 – Insights into the European state of play, Polska została zakwalifikowana do grupy *followers*[2]. Oznaczało to, że podstawy otwierania danych są ustanowione, istnieje portal otwartych danych, ale podejście do udostępniania danych publicznych nadal cechuje wysoka „silosowość" i wciąż pozostaje ono ograniczone. Raport rekomendował przede wszystkim opracowanie dokumentu strategicznego poświęconego otwieraniu danych, który będzie stanowił zarówno podstawę współpracy dla samej administracji publicznej, jak i wspomoże dalsze zaangażowanie potencjalnych podmiotów wykorzystujących dane, tworzenie wytycznych poświęconych priorytetowym obszarom otwierania danych publicznych oraz częstotliwości udostępniania zbiorów danych, które mogą pomóc wspólnotom lokalnym oraz tworzenie mierników do podejmowanych działań otwierania danych, które pomogą zidentyfikować korzyści i obszary do poprawy.

Odpowiedzią na zalecenia OECD oraz badanie Komisji Europejskiej jest m.in. Program Otwierania Danych Publicznych (dalej: PODP), opracowany w Ministerstwie Cyfryzacji i przyjęty 20.9.2016 r. przez Radę Ministrów (uchwała nr 107/2016, niepubl.)[3].

Nadrzędnym celem PODP jest poprawa jakości i liczby zasobów informacyjnych udostępnianych w Centralnym Repozytorium Informacji Publicznej (serwis dane publiczne.gov.pl).

[1] http://www.oecd-ilibrary.org/governance/government-at-a-glance-2017_gov_glance-2017-en;jsessionid=296ooao95k4l8.x-oecd-live-02.
[2] http://www.europeandataportal.eu/en/content/open-data-maturity-europe.
[3] http://mc.bip.gov.pl/programy-realizowane-w-mc/programu-otwierania-danych-publicznych.html.

Otoczenie międzynarodowe

Przy opracowaniu PODP przede wszystkim wzięto pod uwagę następujące inicjatywy unijne:

1) Dyrektywę 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego[4] zmienioną dyrektywą 2013/37/UE Parlamentu Europejskiego i Rady z 26.6.2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego[5];
2) Wytyczne Komisji Europejskiej opublikowane w formie komunikatu 2014/C 240/01 z 24.7.2014 r. w sprawie zalecanych licencji standardowych, zbiorów danych i opłat za ponowne wykorzystanie dokumentów[6];
3) Międzynarodową Kartę Otwartych Danych G8[7];
4) Partnerstwo na Rzecz Otwartego Rządu[8];
5) Open Data Guidelines[9].

Ważne

Dane publiczne – liczby i pojedyncze wydarzenia lub obiekty na możliwie najniższym poziomie agregacji, które nie zostały poddane przez administrację publiczną przetworzeniu do postaci raportów, wykresów itp. oraz nie został im nadany odpowiedni kontekst lub interpretacja (PODP).

Diagnoza barier

Większość rejestrów publicznych, w których gromadzi się dane publiczne o dużym potencjale dla ponownego wykorzystywania, powstało wiele lat temu i nie odpowiada współczesnym rozwiązaniom technologicznym, zapewniającym automatyzację procesów pobierania i przetwarzania danych publicznych.

Obecnie dane publiczne o największym potencjale do ponownego wykorzystywania prezentowane są w serwisach internetowych na kilka sposobów: przez udostępnienie na stronie resortu statycznych plików w formatach utrudniających ich ponowne wykorzystywanie, przez udostępnienie w formatach otwartych, ale o ograniczonej liczbie rekordów, czy też przez wyszukiwarkę informacji (pojedynczych rekordów) według podanych przez użytkownika słów kluczowych lub wyrażeń.

Przeprowadzona w ramach PODP inwentaryzacja w zakresie Systemu Informacji Systemów Teleinformatycznych (SIST), która objęła 371 rejestrów instytucji realizujących POPD pokazała, że w 137 przypadkach istnieje kontrola jakości danych, w 56 nie przewidziano takiej kontroli, w pozostałym zakresie brak danych.

W serwisie danepubliczne.gov.pl otwarty dostęp do zasobów informacyjnych ogranicza nadmierne stosowanie formatów nieprzeszukiwalnych i o zamkniętym dostępie do danych publicznych (np. format PDF dla danych liczbowych), niska jakość przygotowania danych publicznych, np. pozostawienie złożonej struktury nagłówka tabeli właściwego dla zbioru tekstowego lub wydruku, zamiast przygotowania arkusza danych w standardzie CSV, niewykonanie czynności weryfikacji i czyszczenia danych publicznych. Kolejnymi problemami są: niewielka liczba API do istniejących baz danych prowadzonych przez instytucje publiczne oraz niestosowanie formatu XML o najwyższym stopniu otwartości i użyteczności dla maszynowego wyszukiwania, pobierania i ponownego wykorzystywania.

Warto także wskazać na wyniki ankiety przeprowadzonej w 2015 r. przez Ministerstwo Cyfryzacji, diagnozującej bariery i potrzeby w dostępie do danych. Według respondentów (wpłynęły 154 odpowiedzi) do najistotniejszych barier w dostępie do danych publicznych należą:

1) brak danych kompletnych (74,7%),
2) brak danych w internecie (71,4),
3) zamknięty format danych uniemożliwiający automatyczne przeszukiwanie i import danych (63,0%),
4) brak dobrej woli urzędów (57,1%),
5) obecnie obowiązujące przepisy prawne (46,1%).

Filary otwartości

Międzynarodowe inicjatywy, tj. Międzynarodowa Karta Otwartych Danych G8 oraz komunikat 2014/C 240/01 dostrzegły, że zarówno podaż, jak i popyt na ponowne wykorzystywanie danych publicznych podlega ograniczeniom technicznym, które odgrywają fundamentalną rolę w zmniejszeniu lub maksymalizacji potencjalnej wartości danych publicznych dla społeczeństwa i gospodarki.

W celu ułatwienia ponownego wykorzystywania danych publicznych opracowano zalecenia, które powinny mieć wpływ na podniesienie wartości danych w ten sposób, że zwiększona zostanie ich dostępność, jakość, użyteczność i interoperacyjność.

Tożsame zalecenia są również kluczowym elementem PODP. Podmioty działające zgodnie z PODP muszą przestrzegać 8 zasad stanowiących podstawę uznania danych publicznych za otwarte.

[4] Dz Urz. UE L 345 z 31.12.2003 r., s. 90 ze zm. – Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 32, s. 701 ze zm.
[5] Dz.Urz. UE L 175 z 27.6.2013 r., s. 1.
[6] Obwieszczenie Komisji Europejskiej 2014/C 240/01 – Wytyczne w sprawie zalecanych licencji standardowych, zbiorów danych i opłat za ponowne wykorzystanie dokumentów (Dz.Urz. UE C 240 z 24.7.2014 r., s. 1).
[7] https://www.gov.uk/government/publications/open-data-charter.
[8] http://www.opengovpartnership.org/.
[9] http://sunlightfoundation.com/opendataguidelines/.

8 zasad stanowiących podstawę uznania danych publicznych za otwarte, według tych zasad dane powinny być:	
1.	**dostępne** – udostępnione bez żadnych ograniczeń szerokiemu gronu użytkowników (w szczególności: obywatelom, firmom, uczelniom, instytucjom) do dowolnych celów
2.	**upublicznione w wersji źródłowej** – dostępne w oryginalnej i niezmienionej formie, nie w postaci np. analiz, podsumowań, skrótów czy streszczeń, tak aby możliwe było np. łączenie danych z różnych źródeł
3.	**kompletne** – udostępnione w całości
4.	**aktualne** – udostępnione na tyle szybko, aby zachować wartość tych danych
5.	**odczytywalne maszynowo** – udostępnione w formatach przeznaczonych do odczytu maszynowego i formacie otwartym. Przykładem takich formatów jest CSV, XML, arkusz kalkulacyjny. Zazwyczaj trudne do maszynowego odczytu są formaty PDF, HTML czy plik tekstowy, które stają się użyteczne do ponownego wykorzystywania dopiero po przełożeniu ich na jeden z formatów otwartych
6.	**udostępnione niedyskryminująco** – dostępne dla każdego bez konieczności rejestracji, weryfikacji tożsamości poprzez podawanie hasła, loginu czy podpisywania jakichkolwiek umów
7.	**dostępne bez ograniczeń licencyjnych** – dane nie są przedmiotem praw autorskich, patentów, znaków towarowych lub tajemnicy handlowej i mogą być wykorzystywane w dowolnych celach bez konieczności ubiegania się o jakąkolwiek zgodę na ich używanie
8.	**niezastrzeżone** – dostępne w formacie powszechnie stosowanym, który nie jest kontrolowany przez żaden podmiot

Miejscem, w którym zapewniony zostaje dostęp do danych publicznych spełniających filary otwartości jest serwis danepubliczne.gov.pl.

Jakość danych

Idea otwartości danych publicznych to nowy paradygmat w porównaniu z jawnością informacji. Otwarte dane przede wszystkim są uporządkowane strukturalnie w taki sposób, żeby można je było dalej analizować, przetwarzać lub wykorzystywać do budowy usług, produktów lub aplikacji, tak więc tworzyć wartość dodaną.

Kluczowym elementem PODP w tym kontekście jest zbiór wytycznych mających na celu poprawę jakości danych publicznych (załącznik nr 1 do PODP). Wymagania dotyczące jakości danych obejmują:

1) aktualność;
2) kompletność;
3) poprawność formalną (kontrola danych, reguły poprawności);
4) wiarygodność;
5) jednorodność (te same typy danych są zapisywane w tym samym standardzie formalnym, np. data, waluta, liczby);
6) brak redundancji (nadmiarowości/powtórzeń);
7) naturalny język danych (gdy ma znaczenie);
8) format przeznaczony do odczytu maszynowego.

Do najbardziej pożądanych formatów plików do maszynowego odczytu zalicza się (w kolejności od najbardziej preferowanych): dane ustrukturyzowane JSON, XML, GML, CSV, SHP; XLSX, ODS, XLS; dane niestrukturyzowane: DOCX, ODT, RTF, DOC, TXT, PDF (dla plików zawierających graficzne odwzorowania dokumentów), JPG, TIF, PNG (dla plików zawierających dokumenty graficzne), archiwa skompresowane (dla pakietów przygotowanych do pobrania jako całość) dostępnych w serwisie danepubliczne.gov.pl był format XLS lub XLSX. PODP udziela wskazówek jak prawidłowo przygotować pliki i jakie operacje na danych są niedopuszczalne.

Ponadto PODP uwzględnia inne ważne standardy interoperacyjności i otwartości danych publicznych, które dotychczas były rozproszone w wielu dokumentach. Choć PODP realizują członkowie Rady Ministrów, po dokument może sięgnąć każdy, kto poszukuje wiedzy na temat przygotowania danych publicznych, a także organizacji i lokalizacji źródeł danych, standaryzacji i formatów plików danych, publikacji danych oraz standardu metadanych.

Pełnomocnictwo ds. otwartości danych

Ze względu na ramy niniejszego artykułu warto wspomnieć o jednym z ważniejszych rozwiązań instytucjonalnych PODP – pełnomocnikach ds. otwartości danych. Pełnią oni kluczową funkcję operacyjną w dbaniu o jakość i użyteczność danych publicznych w instytucjach objętych realizacją programu. Powodzenie w otwieraniu danych publicznych i upowszechnianiu standardów w głównej mierze zależy od operatywności i zaangażowania oraz merytorycznym przygotowania osób, które w urzędach zajmują się zagadnieniem otwartości danych publicznych.

Działanie pełnomocników ds. otwartości ma bezpośrednie oddziaływanie na statystyki serwisu danepubliczne.gov.pl. W okresie od września 2016 r. do września 2017 r. można zauważyć znaczący wzrost udziału danych ustrukturyzowanych (CSV, XML, JSON, XLS, XLSX) do 6565 danych – przyrost o 14%; oraz liczby zbiorów udostępnionych przez API – 187 (przyrost o 340%).

Warunki ponownego wykorzystywania informacji sektora publicznego

Dominik Sybilski
Asystent w Zakładzie Prawa Administracyjnego,
Instytut Nauk Prawnych PAN

Podmioty zobowiązane, udostępniając informacje sektora publicznego za pośrednictwem systemów teleinformatycznych, czy przekazując informacje na wniosek o ponowne wykorzystywanie mogą określić warunki dalszego korzystania z tych informacji. Nie mogą one jednak w nieuzasadniony sposób uniemożliwiać ponownego wykorzystywania. Precyzyjnie określone warunki chronią zarówno podmioty sektora publicznego udzielające informacji, jak i użytkownika informacji.

Ustawa z 25.2.2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2016 r. poz. 352 ze zm.; dalej: InfSekPublU) wprowadziła zmiany w zakresie przepisów regulujących warunki ponownego wykorzystywania informacji. Przypomnijmy, że obowiązująca od 16.6.2016 r. InfSekPublU dokonała, w swoim zakresie, wdrożenia do polskiego porządku prawnego postanowień dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego zmienionej dyrektywą 2013/37/UE[1]. Ustawodawca zaproponował nowy sposób wdrożenia zmienianej dyrektywy w krajowym systemie prawnym, który miał zapewnić, że rozwiązania dotyczące ponownego wykorzystywania będą bardziej przejrzyste i łatwiejsze w stosowaniu[2]. Zakładał on wyodrębnienie przepisów o ponownym wykorzystywaniu z ustawy z 6.9.2001 r. o dostępie do informacji publicznej (Dz.U. z 2016 r. poz. 1764; dalej: DostInfPubU) i uregulowanie zasad oraz procedury ponownego wykorzystywania w nowej ustawie, czyli InfSekPublU. Ustawa określa zasady i tryb udostępniania i przekazywania informacji sektora publicznego (dalej: ISP) w celu ponownego wykorzystywania, podmioty zobowiązane, które udostępniają lub przekazują te informacje[3], warunki ponownego wykorzystywania oraz zasady ustalania opłat. Dla omawianej tematyki istotne jest, że w InfSekPublU uwzględniono podstawową zmianę wynikającą z dyrektywy 2013/37/UE, czyli poszerzenie zakresu przedmiotowego ponownego wykorzystywania o zasoby będące w posiadaniu bibliotek, archiwów

[1] Dyrektywa 2013/37/UE Parlamentu Europejskiego i Rady z 26.6.2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.Urz. UE L 175/1).

[2] Uzasadnienie do rządowego projektu ustawy o ponownym wykorzystywaniu informacji sektora publicznego, Druk nr 141, http://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=141.

[3] W art. 5 InfSekPublU rozróżniono dwa tryby udzielenia ISP do ponownego wykorzystywania. „Udostępnienie" ISP odnosi się do bezwnioskowego udzielenia ISP poprzez systemy teleinformatyczne (w szczególności BIP i CRIP), z kolei „przekazanie" obejmuje wyłącznie udzielenie ISP na wniosek.

i muzeów. Treści będące w posiadaniu tych podmiotów na gruncie dyrektywy 2003/98/WE podlegały wyłączeniu z ponownego wykorzystywania.

Podstawy prawne dla ustalania warunków ponownego wykorzystywania informacji zostały ujęte w Rozdziale 3 InfSekPublU. Przepisy te mają zastosowanie przy udostępnianiu ISP za pośrednictwem systemów teleinformatycznych takich, jak Biuletyny Informacji Publicznej (dalej: BIP) czy centralne repozytorium informacji publicznej (dalej: CRIP)[4], jak i w sytuacji przekazywania ISP na wniosek o ponowne wykorzystywanie. Odstępstwa od ogólnych zasad dotyczących warunków będą mogły mieć miejsce w przypadku ponownego wykorzystywania zasobów bibliotek, archiwów i muzeów.

Bezwarunkowe ponowne wykorzystywanie

Podmiot zobowiązany udzielając ISP, tak w trybie wnioskowym, jak i bezwnioskowym za pośrednictwem swojego systemu teleinformatycznego – zgodnie z art. 13 ust. 1 z InfSekPublU – może podjąć decyzję o nieokreślaniu warunków ponownego wykorzystywania. Wówczas użytkownik może wykorzystywać ISP bez spełniania jakichkolwiek warunków, zgodnie ze swoimi potrzebami.

Podjęcie decyzji o braku warunków ponownego wykorzystywania będzie uzależnione od rodzaju informacji. Udzielenie ISP bez określenia warunków może dotyczyć tych informacji, które jednocześnie nie mają cech utworu lub przedmiotu praw pokrewnych w rozumieniu przepisów ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2017 r. poz. 880 ze zm.) lub stanowiących bazę danych w rozumieniu przepisów ustawy z 27.7.2001 r. o ochronie baz danych (Dz.U. z 2001 r. Nr 128, poz. 1402 ze zm.). W praktyce mogą to być np. treści dokumentów, materiały urzędowe czy proste informacje dotyczące funkcjonowania urzędu, czy wydatkowania środków publicznych.

W przypadku ISP, dostępnych w BIP lub CRIP, brak wyraźnej informacji o warunkach ponownego wykorzystywania należy uznać za zgodę podmiotu zobowiązanego na bezwarunkowe korzystanie (art. 11 ust. 4 InfSekPublU). W tym wypadku zainteresowany wykorzystywaniem ISP nie musi składać wniosku do właściwego podmiotu zobowiązanego.

Ważne

Brak informacji o warunkach ponownego wykorzystywania ISP udostępnionych w Biuletynie Informacji Publicznej lub w Centralnym Repozytorium Informacji Publicznej (portal danepubliczne.gov.pl) oznacza możliwość dowolnego wykorzystywania tych informacji bez ograniczeń jakimikolwiek warunkami.

Możliwe warunki

Artykuł 8 ust. 1 dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE stanowi, że organ sektora publicznego może zezwolić na ponowne wykorzystywanie dokumentów bez żadnych warunków lub może określić warunki, w uzasadnionych przypadkach, w ramach licencji. Warunki te nie ograniczają niepotrzebnie możliwości ponownego wykorzystywania i nie są stosowane do ograniczania konkurencji. Motyw 26 dyrektywy 2013/37/UE podaje dwa przykłady tego rodzaju dopuszczalnych warunków: obowiązek podania źródła i wskazania, czy dokument został w jakikolwiek sposób zmieniony. Stanowi również, że wszelkie licencje powinny w każdym przypadku jak najmniej ograniczać ponowne wykorzystywanie, na przykład przez ograniczenie do wskazania źródła.

Polski ustawodawca, transponując dyrektywę 2013/37/UE, nie wprowadził w InfSekPublU podstawy dla stosowania standardowych otwartych licencji typu *Creative Commons* (CC). Nie ustanowił również – wzorem niektórych państw członkowskich UE – licencji krajowej. Powtórzono zaś z pewnymi modyfikacjami rozwiązanie funkcjonujące do 16.6.2016 r. pod rządami dotychczasowych przepisów dotyczących ponownego wykorzystywania informacji publicznych zawartych w Rozdziale 2a DostInfPubU, opierające się na koncepcji warunków ponownego wykorzystywania zawartych w ofercie.

W art. 14 InfSekPublU określono katalog warunków ponownego wykorzystywania, jakie podmiot zobowiązany może ustanowić, udostępniając lub przekazując ISP do ponownego wykorzystywania. Dotyczą one:

1) obowiązku poinformowania o źródle, czasie wytworzenia i pozyskania informacji od podmiotu zobowiązanego;
2) obowiązku poinformowania o przetworzeniu informacji ponownie wykorzystywanej;
3) zakresu odpowiedzialności podmiotu zobowiązanego za udostępniane lub przekazywane informacje.

Warto zauważyć, że w ustawie zrezygnowano z warunku obowiązującego poprzednio na gruncie DostInfPubU, polegającego na obowiązku dalszego udostępniania innym użytkownikom informacji w pierwotnie pozyskanej formie (uchylony art. 23b ust. 1 pkt 2 DostInfPubU).

Pierwszy z warunków ma charakter informacyjny, ponieważ jego spełnienie zapewnia potencjalnym użytkownikom i „dalszym użytkownikom"

[4] Cele CRIP realizuje rządowy portal otwartych danych, czyli danepubliczne.gov.pl. Zob. *A. Gos*, Serwis danepublicze.gov.pl, Informacja w Administracji Publicznej, Nr 3, Warszawa 2017, s. 44.

wiedzę, co do statusu ponownie wykorzystywanych informacji[5]. Realizacja tego wymogu zapewnia możliwość sprawdzenia wiarygodności informacji oraz ich aktualności, a więc chroni końcowego użytkownika produktu, usługi czy jakiejkolwiek innej treści powstałej w wyniku ponownego wykorzystywania.

Spełnienie przez użytkownika drugiego obowiązku pozwala na zapewnienie wiarygodności informacji, którymi podmiot ten się posługuje. Jednocześnie ma na celu ochronę interesu podmiotu zobowiązanego, który udostępnia do ponownego wykorzystywania informację w określonej formie i o określonej treści, więc może oczekiwać, że przypisywane mu będzie wytworzenie takiej właśnie informacji[6].

Zastrzeżenie trzeciego warunku służy ograniczeniu odpowiedzialności podmiotu zobowiązanego. Chodzi o to, aby podmiot ten nie ponosił negatywnych konsekwencji wynikających z ponownego wykorzystywania pochodzących od niego zasobów informacyjnych[7].

Obligatoryjne ustalenie warunków

Zgodnie z art. 13 ust. 2 InfSekPublU określenie przez podmiot zobowiązany warunków ponownego wykorzystywania jest obowiązkowe dla ISP mających cechy utworu lub przedmiotu praw pokrewnych lub stanowiących bazę danych, do których przysługują mu autorskie prawa majątkowe lub prawa pokrewne. W takim przypadku podmiot zobowiązany określa warunek dotyczący obowiązku poinformowania o nazwisku, imieniu lub pseudonimie twórcy lub artysty wykonawcy, jeżeli są znane. Może również określić również inne warunki (art. 13 ust. 3 InfSekPublU), które będą zdeterminowane zakresem praw przysługujących podmiotowi zobowiązanemu.

Warunki fakultatywne dla bibliotek, archiwów i muzeów

Odrębności w zakresie określenia warunków mogą dotyczyć zasobów, które są udostępniane lub przekazywane do ponownego wykorzystywania przez muzea państwowe lub samorządowe, biblioteki publiczne lub naukowe oraz archiwa tworzące państwową sieć archiwalną i innych jednostek organizacyjnych prowadzących działalność archiwalną w zakresie państwowego zasobu archiwalnego. Podmioty te, zgodnie z art. 14 ust. 2 InfSekPublU, mogą ustalić warunki ograniczające wykorzystywanie ISP:

1) w działalności komercyjnej lub na określonych polach eksploatacji, jeżeli dotyczą zbiorów o charakterze martyrologicznym oraz zawierają godło, barwy i hymn Rzeczypospolitej Polskiej, a także herby, reprodukcje orderów, odznaczeń lub odznak honorowych, odznak lub oznak wojskowych bądź innych odznaczeń;
2) do działalności niekomercyjnej, jeżeli są powiązane z obiektami objętymi roszczeniami osób trzecich lub niebędącymi własnością podmiotu zobowiązanego.

Przyjęcie takiego rozwiązania w pierwszym przypadku uzasadnione było ochroną zasobów, które stanowią część narodowego dziedzictwa kulturowego i często są ważnymi dla kraju symbolami[8]. W drugim przypadku, chodzi o zasoby o nieustalonym statusie, objęte roszczeniami prawno-własnościowymi osób trzecich, a także ISP, niebędące własnością podmiotu zobowiązanego, ale znajdujące się np. w czasowym depozycie.

Forma określenia warunków

Warunki ponownego wykorzystywania ISP przekazanej na wniosek (art. 23 ust. 1 pkt 3 InfSekPublU), jak i udostępnionej w systemie teleinformatycznym stanowić będą (art. 12 ust. 1 i 2 InfSekPublU) ofertę. Pojęcie oferty należy rozumieć zgodnie z art. 66 i n. Kodeksu cywilnego. W przypadku przyjęcia przez wnioskodawcę oferty złożonej przez podmiot zobowiązany w odpowiedzi na wniosek albo rozpoczęcia ponownego wykorzystywania opatrzonej warunkami informacji udostępnionej w systemie teleinformatycznym, dochodzi do zawarcia umowy cywilnoprawnej, której stronami są podmiot zobowiązany (oferent) i użytkownik (oblat)[9]. W konsekwencji, w przypadku naruszenia warunków określonych w umowie, zastosowanie znajdą ogólne zasady odpowiedzialności cywilnej[10].

W przypadku ISP udostępnionych w CRIP, warunki określone przez podmiot zobowiązany (dostawcę danych), zgodnie z § 7 ust. 1 pkt 2 rozporządzenia Rady Ministrów z 12.3.2014 r. w sprawie Centralnego Repozytorium Informacji Publicznej (Dz.U. z 2014 r. poz. 361 ze zm.), stanowią element metadanych. Warunki te są w CRIP – odpowiednio dla poszczególnych zasobów danych – wizualizowane (wraz z pozostałymi metadanymi opisującymi dany zasób). W przypadku podjęcia przez dostawcę decyzji o udostępnieniu w CRIP zasobów bez zastrzegania warunków, informacja taka nie jest podawana (brak jest informacji o możliwości wykorzystywania zasobu bez jakichkolwiek warunków w metadanych). Zastosowanie będzie miała wówczas reguła opisana powyżej, oznaczająca domniemaną zgodę na

[5] *M. Sakowska-Baryła*, Warunki ponownego wykorzystywania ISP, [w:] *E. Badura*, *M. Błachucki*, *X. Konarski*, *M. Maciejewski*, *H. Niestrój*, *A. Piskorz-Ryń*, *M. Sakowska-Baryła*, *G. Sibiga*, *K. Ślaska*, Ponowne wykorzystywanie informacji sektora publicznego, Ministerstwo Cyfryzacji 2016, s. 130.
[6] Tamże, s. 132.
[7] Tamże, s. 133.
[8] Zob. *E. Badura*, Ponowne wykorzystywanie w muzeach, [w:] Ponowne wykorzystywanie..., s. 351.
[9] Tamże, s. 252.
[10] Uzasadnienie, s. 13.

bezwarunkowe ponowne wykorzystywanie.

PRZYKŁAD

Na dzień 22.9.2017 r. dla 387 zbiorów danych dostępnych w portalu danepubliczne.gov.pl określono warunki ponownego wykorzystywania. Bez warunków dostępnych jest 347 zbiorów danych.

Natomiast w odniesieniu do informacji udostępnianych w BIP należy wskazać, że zgodnie z wyrażoną w art. 11 zasadą przejrzystości podmiot zobowiązany udostępnia na swojej stronie podmiotowej BIP w menu przedmiotowym w kategorii „Ponowne wykorzystywanie" warunki ponownego wykorzystywania, jeżeli zostały przez niego określone.

PRZYKŁAD

Informacja o warunkach ponownego wykorzystywana dostępna na stronie BIP Ministerstwa Cyfryzacji. Warunki ponownego wykorzystywania informacji sektora publicznego udostępnionych na stronie mc.bip.gov.pl obejmują:

1) obowiązek poinformowania o źródle, czasie wytworzenia i pozyskania informacji od MC;
2) obowiązek poinformowania o przetworzeniu informacji ponownie wykorzystywanej.

Ministerstwo Cyfryzacji może określić również inne warunki, jeśli ponowne wykorzystywanie dotyczy informacji sektora publicznego spełniającej cechy utworu lub przedmiotu praw pokrewnych w rozumieniu przepisów ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych lub stanowiących bazę danych w rozumieniu przepisów ustawy z 27.7.2001 r. o ochronie baz danych, do których przysługują mu autorskie prawa majątkowe lub prawa pokrewne. Wówczas MC w szczególności określi warunek dotyczący obowiązku poinformowania o nazwisku, imieniu lub pseudonimie twórcy lub artysty wykonawcy, jeżeli jest znany.

Ministerstwo Cyfryzacji nie ponosi odpowiedzialności za ponowne wykorzystywanie informacji udostępnionej na stronie: mc.bip.gov.pl

Z kolei podmiot zobowiązany, który udostępnia ISP w celu ponownego wykorzystywania w sposób inny niż w BIP lub CRIP (np. w innym systemie teleinformatycznym) wraz z ich udostępnieniem informuje o braku warunków ponownego wykorzystywania lub opłat za ponowne wykorzystywanie albo określa te warunki lub wysokość opłat za ponowne wykorzystywanie (art. 11 ust. 2 InfSekPublU). W ustawie nie sprecyzowano w jaki sposób ten obowiązek powinien zostać spełniony. Można uznać, że podanie informacji dotyczącej warunków (lub opłat) powinno towarzyszyć udostępnionej ISP i stanowić łatwo zauważalny dla potencjalnego użytkownika komunikat[11].

Jeżeli ISP została udostępniona w sposób inny niż w BIP lub CRIP i nie zostały określone warunki ponownego wykorzystywania lub opłaty albo nie poinformowano o braku takich warunków lub opłat, wówczas zainteresowany potencjalny użytkownik wykorzystywaniem informacji powinien wnieść wniosek o ponowne wykorzystywanie (art. 21 ust. 1 pkt 2 InfSekPublU).

Ważne

Udostępnienie ISP na stronie internetowej urzędu (niebędącej BIP), np. portalu informacyjnym gminy, bez określenia warunków, nie stanowi domniemania zgody na dowolne ponowne wykorzystywanie tak upublicznionych informacji. Ponowne wykorzystywanie będzie możliwe, jeżeli wraz z tak udostępnianą ISP zostaną podane ewentualne warunki ponownego wykorzystywania albo zostanie podana informacja o braku warunków dalszego korzystania z informacji.

Miejsce podania warunków ponownego wykorzystywania			
Lp.	**Tryb udzielenia ISP**	**Miejsce**	**Przepis InfSekPublU**
1.	Przekazanie na wniosek	Oferta	art. 21 ust. 1 pkt 3
2.	Udostępnienie w BIP	Zakładka „Ponowne wykorzystywanie"	art. 11 ust. 1 pkt 1
3.	Udostępnienie w CRIP	Metadane opisujące zasób informacyjny	art. 11 ust. 4 § 7 rozporządzenia Ministra Administracji i Cyfryzacji z 12.3.2014 r. w sprawie Centralnego Repozytorium Informacji Publicznej
4.	Udostępnienie „w inny sposób", np. na portalu informacyjnym	Wraz z daną ISP, np. w formie noty, zastrzeżenia	art. 11 ust. 2

[11] Zob. *M. Maciejewski*, Zasady udostępniania i przekazywania isp w celu ponownego wykorzystywania [w:] Ponowne wykorzystywanie..., s. 123.

Kwestionowanie warunków

Bez względu na tryb udzielenia ISP do ponownego wykorzystywania przepisy ustawy zapewniają użytkownikom możliwość kwestionowania ustalonych warunków.

Wnioskodawca, który otrzymał ofertę, może w terminie 14 dni od dnia jej otrzymania złożyć sprzeciw z powodu naruszenia przepisów ustawy albo poinformować o jej przyjęciu. Brak reakcji wnioskodawcy w tym terminie jest równoznaczny z wycofaniem wniosku (art. 23 ust. 2 InfSekPublU). W przypadku otrzymania sprzeciwu podmiot zobowiązany, w drodze decyzji, rozstrzyga o warunkach ponownego wykorzystywania ISP lub o wysokości opłat (art. 23 ust. 3 InfSekPublU).

Z kolei, w przypadku ISP już udostępnionej (np. w BIP lub CRIP), dla której określono warunki, użytkownik, który chciałby wykorzystywać informację na innych warunkach, może wystąpić z wnioskiem (art. 21 ust. 1 pkt 3 InfSekPublU). Wówczas przedmiotem wniosku jest określenie innych warunków lub zezwolenie na ponowne wykorzystywanie bez spełnienia jakichkolwiek warunków.

Zasady ogólne dotyczące warunków

Należy podkreślić, że w każdym przypadku, bez względu na rodzaj informacji, formę jej udzielenia, czy status podmiotu zobowiązanego, określenie warunków nie może w sposób nieuzasadniony ograniczać możliwości ponownego wykorzystywania (art. 15 InfSekPublU). Z powodu posłużenia się przez ustawodawcę wyrażeniem nieostrym – tj. „w sposób nieuzasadniony" – każdy z przypadków należy będzie rozpatrywać indywidualnie. Wydaje się, że zamysłem ustawodawcy było, aby określone warunki nie utrudniały czy wręcz uniemożliwiały w ogóle ponownego wykorzystywania danej ISP poprzez zbyt restrykcyjne zastrzeżenia. Z jednej strony ustalenie warunków ma chronić interesy podmiotów uprawnionych oraz gwarantować pewność prawną dla użytkowników wykorzystujących dostępne ISP, z drugiej zaś nie może niweczyć celów ustawy, czyli jak najpełniejszego twórczego wykorzystania danych wytworzonych, czy gromadzonych w sektorze publicznnym w innowacyjnych produktach, usługach, czy aplikacjach powstałych na ich podstawie.

Ze wspomnianą powyżej zasadą jawności warunków ponownego wykorzystywania informacji (art. 11 InfSekPublU) koresponduje zasada niedyskryminacji (równego traktowania). Reguła ta stanowi, że udostępnienie lub przekazanie ISP nie powinno odbywać się na warunkach, które wyeliminowałyby lub ograniczały konkurencję. Do tak niekorzystnego zjawiska mogłoby dojść w przypadku oferowania przez podmiot zobowiązany zróżnicowanych warunków w podobnych okolicznościach wykorzystywania informacji. Dlatego też w art. 8 InfSekPublU sformułowano obowiązek stosowania jednolitych warunków ponownego wykorzystywania w porównywalnych sytuacjach. Ponadto w przypadku, gdy ponowne wykorzystywanie jest dokonywane przez użytkowników będących podmiotami wykonującymi zadania publiczne w ramach działalności wykraczającej poza realizację takich zadań, warunki ponownego wykorzystywania lub opłaty za ponowne wykorzystywanie określa się na takich samych zasadach, jak w przypadku innych użytkowników.

Podstawa prawna

- art. 11–15, art. 21–23 ustawy z 25.2.2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2016 r. poz. 352 ze zm.)
- § 7 rozporządzenia Ministra Administracji i Cyfryzacji z 12.3.2014 r. w sprawie Centralnego Repozytorium Informacji Publicznej (t.j. Dz.U. z 2014 r. poz. 361 ze zm.)

Podsumowanie

Warunki ponownego wykorzystywania ISP mogą zostać przez podmiot zobowiązany ustalone zarówno w ramach bezwnioskowego trybu udostępniania informacji za pośrednictwem systemów teleinformatycznych, jak i przekazania informacji na wniosek o ponowne wykorzystywanie. Podmiot zobowiązany może również udzielić ISP do ponownego wykorzystywania bezwarunkowo. Możliwość ta nie obejmuje ISP chronionych prawami własności intelektualnej. Określone warunki ponownego wykorzystywania w każdym przypadku stanowią ofertę. Konsekwencją naruszenia warunków będzie odpowiedzialność cywilnoprawna użytkownika.

Dopuszczalność umorzenia postępowania w przedmiocie odmowy udostępnienia informacji publicznej przez organ odwoławczy

Bartosz Wilk
Prawnik, wiceprezes stowarzyszenia Sieć Obywatelska Watchdog Polska

Analizowane rozstrzygnięcie jest w praktyce stosowane wówczas, gdy organ odwoławczy (np. samorządowe kolegium odwoławcze), rozpatrujący odwołanie od decyzji podmiotu zobowiązanego (np. prezydenta miasta) o odmowie udostępnienia informacji publicznej uznaje, że odmowa udostępnienia informacji w określonym stanie faktycznym jest niezasadna, a zarazem, że decyzja została wydana zgodnie z przepisami postępowania, zaś zakres sprawy jest dostatecznie wyjaśniony.

Konstrukcja uchylenia decyzji podmiotu zobowiązanego do udostępniania informacji publicznej oraz umorzenia postępowania w przedmiocie odmowy udostępnienia informacji jest efektem poszukiwań sposobu zapobieżenia nieefektywnemu postępowaniu, gdy podmiot zobowiązany odmawia udostępnienia informacji, choć wydanie decyzji odmownej jest niezasadne. Znaczenie tego rozstrzygnięcia jest widoczne zwłaszcza wtedy, gdy podmiot zobowiązany konsekwentnie (i niekiedy wielokrotnie) odmawia udostępnienia informacji na podstawie tych samych przesłanek (podstaw ograniczenia prawa do informacji) w danej sprawie oraz pomimo jasnych wskazań organu odwoławczego, co do nieprawidłowości wydawanych rozstrzygnięć.

PRZYKŁAD

Podmiot zobowiązany odmawia udostępnienia imienia i nazwiska osoby, która podpisała umowę cywilnoprawną z gminą. W świetle wyroku SN z 8.11.2012 r. (I CSK 190/12, Legalis) i orzecznictwa NSA (zob. np. wyr. NSA z 4.2.2015 r., I OSK 531/14, Legalis) można uznać za ugruntowany pogląd, że odmowa udostępnienia tych informacji ze względu na posłużenie się przesłanką ochrony prywatności osoby fizycznej nie jest zasadna w omawianej sytuacji. Pomimo tego, podmiot zobowiązany odmawia udostępnienia przedmiotowej informacji. Dysponenta informacji nie przekonało rozstrzygnięcie podmiotu zobowiązanego o uchyleniu decyzji i przekazanie sprawy do ponownego rozpatrzenia, choć w uzasadnieniu decyzji organu odwoławczego w sposób jednoznaczny wskazano, że odmowa udostępnienia informacji publicznej w tej sprawie z powołaniem się na przesłankę ochrony prywatności nie ma podstaw.

Możliwe rozstrzygnięcia organu odwoławczego

W świetle art. 138 ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257; dalej: KPA), organ odwoławczy może wydać następujące rozstrzygnięcia:

1) utrzymać w mocy zaskarżoną decyzję (art. 138 § 1 pkt 1 KPA);
2) uchylić zaskarżoną decyzję w całości albo w części i w tym zakresie orzec co do istoty sprawy (art. 138 § 1 pkt 2 *ab initio* KPA);
3) uchylić zaskarżoną decyzję w całości albo w części i umorzyć postępowanie pierwszej instancji w całości albo w części (art. 138 § 1 pkt 2 *in fine* KPA);
4) umorzyć postępowanie odwoławcze (art. 138 § 1 pkt 3 KPA);
5) uchylić zaskarżoną decyzję w całości i przekazać sprawę do ponownego rozpatrzenia organowi pierwszej instancji, gdy decyzja ta została wydana z naruszeniem przepisów postępowania, a konieczny do wyjaśnienia zakres sprawy ma istotny wpływ na jej rozstrzygnięcie (art. 138 § 2 KPA).

Z punktu widzenia poruszanego w tekście zagadnienia nie ma potrzeby analizowania możliwości utrzymania decyzji w mocy oraz umorzenia postępowania odwoławczego. Z uwagi na specyfikę szeroko rozumianego postępowania w sprawie udostępnienia informacji publicznej nie może zostać też wydana decyzja merytoryczna (co do istoty sprawy), którą wymieniono powyżej w pkt 2. Wynika to z faktu, że postępowanie o udostępnienie informacji publicznej toczy się na podstawie ustawy o dostępie do informacji publicznej, a jego stronami jest wnioskodawca oraz podmiot zobowiązany do udostępnienia informacji publicznej. Natomiast w przypadku, gdy zostaje wydana decyzja o odmowie udostępnienia informacji publicznej oraz zostaje ona zakwestionowana przez wnioskodawcę, toczy się inne postępowanie – postępowanie odwoławcze, regulowane przepisami Kodeksu postępowania administracyjnego, którego stronami jest podmiot odwołujący się oraz organ odwoławczy. Nie dość zatem, że wskazane postępowania toczą się z udziałem odmiennych stron oraz z odmiennych podstaw prawnych, pamiętać należy, że generalnie organ odwoławczy nie jest dysponentem żądanej informacji, tj. nie dysponuje wnioskowaną informacją i nie może jej udostępnić, gdy uzna to za stosowne. Ponadto udostępnienie informacji publicznej nie następuje w formie decyzji (którą, formalnie rzecz biorąc, wydaje organ odwoławczy), ale czynności materialno-technicznej podmiotu zobowiązanego – dysponenta informacji.

ORZECZENIE

W tym względzie trafnie wskazał WSA w Krakowie w wyroku z 22.11.2010 r. (II SAB/Kr 105/10, Legalis), że: „Nie będąc dysponentem informacji publicznej nie będzie mógł [*organ odwoławczy* – przyp. B.W.] np. uchylić zaskarżonej decyzji odmownej i podjąć rozstrzygnięcia merytorycznego, tj. udzielić informacji publicznej".

Z kolei zastosowanie art. 138 § 2 KPA w przypadku nieuzasadnionej odmowy udostępnienia informacji przez podmiot zobowiązany budzi wątpliwości w sytuacji, gdy decyzja nie została wydana z naruszeniem przepisów postępowania oraz sprawa jest wystarczająco wyjaśniona, gdyż te właśnie przyczyny uzasadniają wydanie decyzji tzw. kasatoryjnej.

Powyższe problemy skłoniły organy stosujące prawo oraz zainteresowane uzyskaniem informacji podmioty do rozważania możliwości zastosowania art. 138 § 1 pkt 2 *in fine* KPA, czyli uchylenia zaskarżonej decyzji oraz umorzenia postępowania w przedmiocie odmowy udostępnienia informacji publicznej.

Konsekwencje umorzenia postępowania w przedmiocie odmowy udostępnienia informacji

Nie ulega wątpliwości, że gdy organ odwoławczy uchyla zaskarżoną decyzję i przekazuje sprawę do ponownego rozpatrzenia, to podmiot zobowiązany musi raz jeszcze rozpatrzyć wniosek o udostępnienie informacji publicznej. Bierze wówczas pod uwagę wskazania organu odwoławczego co do tego, jakie okoliczności należy wziąć pod uwagę przy ponownym rozpatrzeniu sprawy (art. 138 § 2 zd. 2 KPA) oraz, po nowelizacji KPA obowiązującej od 1.6.2017 r., także ewentualne wytyczne w zakresie wykładni błędnie zastosowanych przepisów (art. 138 § 2a KPA).

Z kolei konstrukcja uchylenia zaskarżonej decyzji i umorzenia postępowania w przedmiocie odmowy udostępnienia informacji ma na celu wyeliminowanie możliwości wydania określonego rozstrzygnięcia (odmowy udostępnienia informacji publicznej z powodu zaistnienia określonej przesłanki, np. prywatności osoby fizycznej) w tych samych okolicznościach faktycznych i prawnych sprawy. Konstrukcja ta nie ma na celu zwolnienia podmiotu zobowiązanego z jakiegokolwiek działania, natomiast ma ograniczyć wydanie rozstrzygnięcia, które organ odwoławczy uznał za błędne i w danej sprawie niedopuszczalne.

Zakończenie postępowania o udostępnienie informacji publicznej może przybrać różne formy, tj.: udostępnienie żądanej przez podmiot wnioskujący informacji, umorzenie postępowania na podstawie art. 14 ust. 2 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764; dalej: DostInfPubU), jak również od-

mowę udostępnienia informacji publicznej. Ta ostatnia, tj. odmowa udostępnienia informacji publicznej, może nastąpić z uwagi na określone w art. 5 ust. 1 i 2 DostInfPubU przesłanki – ochronę prywatności osób fizycznych, tajemnicę przedsiębiorcy, ochronę informacji niejawnych i innych tajemnic ustawowo chronionych. Decyzja odmowna jest wydawana także w przypadku stwierdzenia przez podmiot zobowiązany, że przedmiotem wniosku jest udostępnienie informacji przetworzonej (w rozumieniu art. 3 ust. 1 pkt 1 *ab initio* DostInfPubU), a w sprawie nie została spełniona przesłanka szczególnej istotności dla interesu publicznego (art. 3 ust. 1 pkt 1 *in fine* DostInfPubU).

Umorzenie postępowania w przedmiocie odmowy udostępnienia informacji publicznej, np. z powodu posłużenia się przez organ przesłanką prywatności osoby fizycznej, nie wyklucza zatem innego sposobu zakończenia postępowania o udostępnienie informacji publicznej, tj. m.in. udostępnienie przedmiotowej informacji, poinformowanie wnioskodawcę pismem, że przedmiotem wniosku nie jest informacja publiczna, czy też wydanie decyzji o umorzeniu postępowania w przedmiocie udostępnienia informacji publicznej.

Orzeczenia sądowe dopuszczające możliwość umorzenia postępowania w sprawie odmowy udostępnienia informacji publicznej przez organ odwoławczy

Na kanwie analizowanego zagadnienia sądy administracyjne wydawały rozstrzygnięcia w dwojakiego rodzaju sprawach. Po pierwsze, wyroki zapadały ze skarg na bezczynność wnoszonych w sytuacji, gdy podmiot zobowiązany nie realizował wniosku o udostępnienie informacji publicznej po tym, gdy organ odwoławczy rozstrzygnął o uchyleniu decyzji odmownej i umorzeniu postępowania w przedmiocie odmowy udostępnienia informacji. Wynikało to przede wszystkim z uznania przez podmioty zobowiązane, że umorzenie postępowania kończy postępowanie zainicjowane wnioskiem o udostępnienie informacji publicznej, zatem wniosku tego nie trzeba ponownie rozpatrywać.

ORZECZENIE

Jednym z pierwszych wyroków, który zapadł w tym temacie, jest wyrok NSA z 30.3.2011 r. (I OSK 2116/10, Legalis), w którym wskazano, że „Skoro więc Samorządowe Kolegium Odwoławcze (…) uznało, że w niniejszej sprawie brak było podstaw do wydania przez Burmistrza (…) decyzji o odmowie udostępnienia informacji publicznej w zakresie objętej wnioskiem skarżącego, to postępowanie w przedmiocie wydania takiej decyzji stało się bezprzedmiotowe", a w konsekwencji nie dopatrzył się naruszenia art. 138 § 1 pkt 2 ***in fine*** KPA. Sprawa została zainicjowana skargą na decyzję organu odwoławczego, na mocy której m.in. umorzono postępowanie w przedmiocie odmowy udostępnienia informacji.

ORZECZENIE

W wyroku NSA z 21.7.2010 r. (I OSK 557/10, Legalis) wskazano z kolei, że „(…) W ocenie Naczelnego Sadu Administracyjnego Sąd pierwszej instancji prawidłowo uznał, iż wydanie przez Samorządowe Kolegium Odwoławcze (…) decyzji nie powodowało umorzenia postępowania w sprawie udzielenia informacji publicznej lecz nakładało na Burmistrza (…) obowiązek rozpoznania wniosku (…) w spornej części na zasadach i w trybie określonym w ustawie o dostępie do informacji publicznej". W tej sprawie skarżący zarzucał podmiotowi zobowiązanemu bezczynność wskutek nierozpoznania wniosku po decyzji organu odwoławczego o uchyleniu decyzji podmiotu zobowiązanego i umorzeniu postępowania w przedmiocie odmowy udostępnienia informacji.

ORZECZENIE

W podobnych okolicznościach zapadł wyrok WSA we Wrocławiu z 7.7.2014 r. (IV SAB/Wr 79/14, Legalis), w którym sąd stwierdził, że „Wniosek winien organ rozpoznać w terminach określonych w powyższej ustawie dla udostępnienia informacji publicznej lub wydania decyzji, liczonych od dnia doręczenia Burmistrzowi (…) decyzji Samorządowego Kolegium Odwoławczego (…), przy czym przy zachowaniu identycznych okoliczności prawnych i faktycznych nie może odmówić wnioskodawcy udostępnienia informacji publicznej powołując taką samą podstawę prawną jak w uchylonej decyzji".

ORZECZENIE

Wskutek kwestionowania bezczynność podmiotu zobowiązanego po wydaniu analizowanego w tekście rozstrzygnięcia, zapadł także wyrok WSA w Krakowie w wyroku z 22.11.2010 r. (II SAB/Kr 105/10, Legalis). W orzeczeniu tym podkreślono, że „Organ drugiej instancji w istocie bada kwestię zasadności odmowy udzielenia informacji publicznej i w sytuacji, gdy podziela stanowisko organu pierwszej instancji, to utrzymuje w mocy decyzję tego organu, a w sytuacji, gdy nie widzi podstaw do odmowy udzielenia informacji publicznej uchyla decyzję organu pierwszej instancji, a będąc związany treścią art. 138 KPA nie może poprzestać wyłącznie na uchyleniu decyzji (KPA nie przewiduje możliwości jedynie uchylenia decyzji pierwszej instancji), stąd umarza postępowanie zakończone decyzją odmowną traktując je jako bezprzedmiotowe. Umorzenie postępowania nie oznacza w tym stanie rzeczy zakończenia postępowania w przedmiocie udostępnienia informacji publicznej, lecz wręcz przeciwnie eliminując decyzję odmowną otwiera ponownie drogę do zakończenia postępowania w przedmiocie udzielenia informacji publicznej".

ORZECZENIE

Warto zwrócić także uwagę na wyrok WSA w Krakowie z 5.2.2015 r. (II SA/Kr 1687/14, Legalis). Zapadł on ze skargi prokuratora rejonowego na decyzję organu odwoławczego, w której uchylono decyzję podmiotu zobowiązanego i umorzono postępowanie w przedmiocie odmowy udostępnienia in-

formacji publicznej. Krakowski sąd w istocie podzielił stanowisko NSA wyrażone w przytoczonym wyroku NSA z 30.3.2011 r. (I OSK 2116/10, Legalis).

Orzeczenia stwierdzające niedopuszczalność umorzenia postępowania w sprawie odmowy udostępnienia informacji publicznej przez organ odwoławczy

W wyroku NSA z 13.5.2015 r. (I OSK 1250/14, niepubl.), po długim i zawiłym postępowaniu, sąd uznał, że „(...) Brak jest bowiem jakichkolwiek racjonalnych podstaw do dzielenia postępowania, wywołanego wnioskiem o udostępnienie informacji publicznej, na część, do której odnosi się decyzja organu odwoławczego rozpatrującego odwołanie od decyzji odmawiającej udostępnienia takiej informacji oraz na część, do której ta decyzja się nie odnosi. Nie ma przy tym jakichkolwiek przeszkód by w takim wypadku – w razie uwzględnienia odwołania – organ odwoławczy zastosował regulację przepisu art. 138 § 2 KPA, co powodowało będzie konieczność ponownego rozpoznania wniosku, w tym także stwarzało będzie możliwość zakończenia postępowania w drodze czynności materialno-technicznej udostępnienia żądanej informacji".

ORZECZENIE

Stanowisko to podzielono w wyroku NSA z 30.11.2016 r. (I OSK 1263/16, Legalis), w którym wskazano, że: „(...) w sytuacji gdy organ odwoławczy oceni, iż decyzja o odmowie udzielenia informacji jest błędna, winien zastosować regulację art. 138 § 2 KPA. Organ pierwszej instancji jest wówczas w dalszym ciągu zobowiązany do załatwienia wniosku i związany przepisami ustawy o dostępie do informacji publicznej. Przyjmuje się, że jest też związany oceną prawną organu drugiej instancji co do niezgodności z prawem decyzji wcześniej wydanej na podstawie art. 16 DostInfPubU. Obliguje to podmiot zobowiązany do udzielenia informacji do takiego załatwienia sprawy, aby ponowna decyzja nie spotkała się nie tylko z uchyleniem, lecz także z działaniami podjętymi w trybie nadzorczym lub też prawnokarnym".

Za niedopuszczalnością umorzenia postępowania w przedmiocie odmowy udostępnienia informacji opowiedział się także WSA w Krakowie w szeregu nieprawomocnych wyroków[1]. Wszystkie te wyroki zapadły ze skarg wnioskodawców na decyzje wydane przez samorządowe kolegium odwoławcze, które uchyliło decyzje podmiotu zobowiązanego oraz umorzyło postępowania w przedmiocie odmowy. Choć decyzje były formalnie korzystne dla wnioskodawców, postanowili oni poddać je sądowej kontroli w związku z wątpliwościami w praktyce działania podmiotu zobowiązanego, co do konieczności wykonania wniosku po umorzeniu postępowania w przedmiocie odmowy udostępnienia informacji. Skargi kasacyjne zostały w tych sprawach wniesione przez organ odwoławczy – samorządowe kolegium odwoławcze.

Wobec powyższego, orzecznictwo sądowe, opowiadające się za niedopuszczalnością analizowanej konstrukcji prawnej, opiera się na tym, że po uchyleniu nieprawidłowej decyzji organu I instancji sprawa nie staje się bezprzedmiotowa w świetle art. 105 § 1 KPA, więc nie znajduje podstaw umorzenie postępowania na podstawie art. 138 § 1 pkt 2 *in fine* KPA (*per exemplum* nieprawomocny wyrok WSA w Krakowie z 7.2.2017 r., II SA/Kr 1460/16).

Ponadto wskazuje się, że brak jest jakichkolwiek racjonalnych podstaw do dzielenia postępowania wywołanego wnioskiem o udostępnienie informacji publicznej na część, do której odnosi się decyzja organu odwoławczego rozpatrującego odwołanie od decyzji odmawiającej udostępnienia takiej informacji, oraz na część, do której ta decyzja się nie odnosi. To zaś ma sprawiać, że umorzenie postępowania wywoływałoby skutek co do całego postępowania zainicjowanego złożeniem wnioskiem o udostępnienie informacji publicznej. W końcu dodaje się, że możliwość umorzenia postępowania w świetle art. 138 § 1 pkt 2 *in fine* KPA jest wyjątkiem od zasady obowiązku rozstrzygnięcia sprawy co do *meritum* oraz, że uchylenie zaskarżonej decyzji obliguje podmiot zobowiązany do takiego rozstrzygnięcia, aby decyzja nie tylko nie została uchylona, ale także żeby podmiot ten nie spotkał się z konsekwencjami postępowania nadzorczego lub prawnokarnego.

W orzecznictwie istnieje rozbieżność co do dopuszczalności orzekania przez organ odwoławczy o uchyleniu zaskarżonej decyzji i umorzeniu postępowania w przedmiocie odmowy udostępnienia informacji publicznej. Wcześniejsze orzecznictwo WSA w Krakowie, WSA we Wrocławiu i NSA dopuszcza taką możliwość, natomiast odmienne stanowisko zajął NSA w kilku nowszych rozstrzygnięciach. Na rozpatrzenie przez NSA oczekuje co najmniej kilkanaście spraw, związanych z wniesieniem skarg kasacyjnych od wyroków WSA w Krakowie.

Stowarzyszenie Sieć Obywatelska Watchdog Polska zwróciła się do Rzecznika Praw Obywatelskich[2] o wystąpienie z wnioskiem do NSA o podjęcie uchwały mającej na celu wyjaśnienie przepisów prawnych, których stosowanie wywołało rozbieżności

[1] Orzeczenia z 2.2.2017 r. (II SA/Kr 1461/16, Legalis); z 13.2.2017 r. (II SA/Kr 1462/16. Legalis); z 9.2.2017 r. (II SA/Kr 1503/16, Legalis); z 7.2.2017 r. (II SA/Kr 1459/16, Legalis); z 7.2.2017 r. (II SA/Kr 1460/16, Legalis); z 13.2.2017 r. (II SA/Kr 1506/16, Legalis); z 6.2.2017 r. (II SA/Kr 1463/16, Legalis); z 7.2.2017 r. (II SA/Kr 1464/16, Legalis); z 7.2.2017 r. (II SA/Kr 1504/16, Legalis); z 2.2.2017 r. (II SA/Kr 1457/16, Legalis); z 13.2.2017 r. (II SA/Kr 1458/16, Legalis); z 9.2.2017 r. (II SA/Kr 1505/16, Legalis).

[2] Zob. http://siecobywatelska.pl/wp-content/uploads/2016/12/RPO_wnioski-o-podj%C4%99cie-uchwa-%C5%82-1.pdf, plik do pobrania w tekście: https://siecobywatelska.pl/spotkanie-u-rpo-o-jawnosci/.

w orzecznictwie sądów administracyjnych. Wskazano w piśmie, że uznanie dopuszczalności analizowanego w niniejszym tekście rozstrzygnięcia ma istotne znaczenie dla podmiotów i osób czyniących użytek z konstytucyjnego prawa do informacji publicznej.

Poruszone zagadnienie nie zostało dotąd rozstrzygnięte przez powiększony skład NSA. Zarówno to ewentualne rozstrzygnięcie, jak i kolejne wyroki wydane przez NSA będą krokami w kierunku wyeliminowania rozbieżności w zakresie dopuszczalności umorzenia przez organ odwoławczy postępowania w przedmiocie odmowy udostępnienia informacji publicznej.

Podstawa prawna

- art. 138 ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257)
- art. 5 ust. 1 i 2, art. 14 ust. 2 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764)

Podsumowanie

W praktyce, jeżeli organ odwoławczy umorzył postępowanie w sprawie odmowy udostępnienia informacji, można rekomendować dysponentom informacji dalsze procedowanie wniosku o udostępnienie informacji publicznej, wyłączając przy tym możliwość ponownej odmowy udostępnienia informacji i prowadzenie postępowania w kierunku m.in. udostępnienia informacji publicznej. Przytoczone w tekście przykłady wyroków dowodzą, że dalsze postępowanie może być skutecznie prowadzone. Zarazem takie rozwiązanie umożliwi merytoryczne rozpatrzenie sprawy (a nawet jej zakończenie) i nie będzie wiązało się z zatrzymaniem na wstępnym, formalnym etapie. Natomiast z punktu widzenia organu odwoławczego istotne znaczenie ma art. 138 § 2a KPA, dodany na mocy nowelizacji obowiązującej od 1.6.2017 r. Zgodnie z tym przepisem jeżeli organ pierwszej instancji dokonał w zaskarżonej decyzji błędnej wykładni przepisów prawa, które mogą znaleźć zastosowanie w sprawie, w decyzji uchylającej zaskarżoną decyzję w całości i przekazującej sprawę do ponownego rozpatrzenia, organ odwoławczy określa także wytyczne w zakresie wykładni tych przepisów. Przed nowelizacją, zgodnie z wciąż obowiązującym art. 138 § 2 zd. 2 KPA, organ odwoławczy winien wskazać tylko jakie okoliczności należy wziąć pod uwagę przy ponownym rozpatrzeniu sprawy. W przypadku wątpliwości, co do możliwości wydania decyzji umarzającej postępowanie w przedmiocie odmowy udostępnienia informacji publicznej, warto dać dysponentowi informacji wytyczne, co do wykładni problematycznych przepisów, żeby przybliżyć postępowanie do merytorycznego zakończenia.

Zakres jawności sprawozdań składanych przez fundację

„Czy sprawozdanie fundacji składane właściwemu ministrowi można w odpowiedzi na wniosek składany w trybie ustawy o dostępie do informacji publicznej, udostępnić każdemu kto wystąpi z takim wnioskiem do właściwego ministra?"

Opis stanu prawno-faktycznego

Zgodnie z treścią art. 12 ustawy z 6.4.1984 r. o fundacjach (t.j. Dz.U. z 2016 r. poz. 40 ze zm.; dalej: FundU), każda fundacja składa corocznie właściwemu ministrowi sprawozdanie ze swojej działalności. Sprawozdanie to jest składane w sposób i w zakresie określonym w drodze rozporządzenia z 8.5.2001 r. w sprawie ramowego zakresu sprawozdania z działalności fundacji (Dz.U. z 2001 r. Nr 50, poz. 529; dalej: SprFundR). Jednocześnie do stosownie treści art. 12 ust. 3 FundU, sprawozdanie to jest przez fundację udostępniane do publicznej wiadomości. Obowiązku tego nie stosuje się do fundacji posiadających status organizacji pożytku publicznego, które zamieściły na stronie internetowej urzędu obsługującego ministra właściwego do spraw zabezpieczenia społecznego, sprawozdanie merytoryczne z działalności oraz sprawozdanie finansowe zgodnie z przepisami ustawy z 24.4.2003 r. o działalności pożytku publicznego i o wolontariacie (t.j. Dz.U. z 2014 r. poz. 1118 ze zm.).

ODPOWIEDŹ

Nie ulega wątpliwości, że właściwy minister jest podmiotem obowiązanym do udzielenia informacji publicznej i wniosek jest właściwie skierowany. Sama fundacja składająca sprawozdanie, byłaby podmiotem obowiązanym tylko pod warunkiem, że wykonywałaby zadania władzy publicznej, o czym mowa jest w art. 61 ust. 2 Konstytucji RP. Ustawa z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764; dalej: DostInfPubU), w tym zakresie zawiera przepis art. 4 ust. 1 pkt 5), zgodnie z którym obowiązane do udostępniania informacji publicznej są podmioty reprezentujące inne osoby lub jednostki organizacyjne, które wykonują zadania publiczne.

Sprawozdania fundacji – informacją publiczną

Na samym początku należy ustalić, czy sprawozdania fundacji mogą zostać uznane za informację publiczną. Moim zdaniem, sprawozdania te jako takie nie mogą być uznane za informację publiczną, lecz w jakiejś mierze treści zawarte w tych sprawozdaniach mogą odnosić się do sfery spraw publicznych, tym samym mogą spełniać ustawową definicję informacji publicznej zawartą w art. 1 ust. 1 DostInfPubU, zgodnie z którą informacją publiczną jest każda informacja o sprawach publicznych. Każda fundacja w zakresie, w jakim realizuje zadania publiczne, z całą pewnością staje się podmiotem zobowiązanym do stosowania DostInfPubU, ale tylko w zakresie w jakim odnosi się to do wykonywania zadań publicznych. Zgodnie z § 2 pkt 8 SprFundR sprawozdanie powinno zawierać dane o działalności zleconej fundacji przez podmioty państwowe i samorządowe (usługi, państwowe zadania zlecone i zamówienia publiczne) oraz o wyniku finansowym tej działalności. Należy uznać, że sprawozdanie każdej fundacji może zawierać w swojej treści informacje publiczne, ale tylko w zakresie, w jakim ta konkretna fundacja realizowała zadania zlecone przez podmioty państwowe i samorządowe. Zatem sprawozdania jako takie nie są informacją publiczną, lecz mogą zawierać w swojej treści informacje publiczne, które mogą być przedmiotem wniosku o udostępnienie informacji publicznej składanego w trybie DostInfPubU. I jako takie powinny być udostępnione każdemu.

ORZECZENIE

Bardzo ciekawe w tym obszarze rozważania poczynił NSA w wyr. z 21.4.2017 r. (I OSK 1953/15, Legalis), w którym czytamy m.in.: „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".

Nie ma znaczenia, że posiadane przez ministra sprawozdania fundacji jest traktowane jako tzw. dokument prywatny. Dokumenty tego typu same w sobie nie stanowią informacji publicznej, lecz mogą ją zawierać. Jak słusznie stwierdzały to wielokrotnie sądy administracyjne[1]. „Każdy dokument urzędowy (a nie każde pi-

[1] Por. wyr. NSA 19.8.2009 r., I OSK 683/09, Legalis; wyr. NSA z 13.6.2014 r., I OSK 3070/13, Legalis; wyr. NSA z 18.2.2015 r., I OSK 752/14, Legalis.

smo) jest sam w sobie informacją publiczną. Pismo niebędące dokumentem urzędowym niewątpliwie może być nośnikiem informacji publicznej. Wtedy jednak udostępnieniu podlega ta informacja publiczna, która zawarta jest w jego treści, a nie samo pismo (tj. jego „treść i postać"). Informacja bowiem udzielana na wniosek, a niebędąca dokumentem urzędowym, nie jest tożsama z bezpośrednim zetknięciem się z elementem rzeczywistości, lecz z opisem tej rzeczywistości" (post. WSA w Krakowie z 8.7.2010 r., II SAB/Kr 46/10, Legalis).

Jaki jest zakres jawności sprawozdania fundacji

Zwracam uwagę, że uznanie danego obszaru informacyjnego za informację publiczną nie stawia znaku równości z jawnością. W szczególnych sytuacjach może zdarzyć się, że sprawozdanie fundacji dotyczące wykonywanych zadań zleconych, będzie zawierało w swojej treści takiego typu informacje, które np. będą odnosiły się do osób trzecich i w takim zakresie nie powinny być udostępniane. W takiej sytuacji minister realizujący wniosek o udostępnienie złożonego sprawozdania, powinien rozważyć, czy ta część sprawozdania zawierająca dane chronione ze względu na prawo do prywatności, nie powinna zostać poddana stosownej anonimizacji.

Osobiście uważam, że **właściwy minister przyjmujący sprawozdania fundacji, ma obowiązek udostępnić te informacje ze sprawozdania fundacji, których charakter świadczy o tym, że dana fundacja stała się podmiotem obowiązanym do stosowania DostInfPubU**. Może mieć to miejsce tylko w zakresie w jakim fundacja wykonuje zadania publiczne. Co do zaś kwestii technicznej owego udostępnienia przez właściwego ministra, może ono nastąpić poprzez przekazanie informacji wraz z nośnikiem – można zawsze dokonać stosowanej anonimizacji lub poprzez przekazanie samej tylko informacji bez nośnika. Jeżeli bowiem dana fundacja w sprawozdaniu nie wykazała żadnej działalności zleconej przez podmioty państwowe i samorządowe (usługi, państwowe zadania zlecone i zamówienia publiczne), to tym samym ta jej działalność, aczkolwiek objęta obowiązkiem sprawozdawczości, nie dotyczy sprawy publicznej. Tym samym nie stanowi informacji publicznej. O takim podejściu do sprawy świadczy fakt, że sądy wyraźnie wskazują, iż tzw. dokumenty prywatne (a z takimi mamy tu do czynienia), nie są same w sobie informacją publiczną, ale mogą ją zawierać. Tym samym dokumenty prywatne poprzez fakt ich wysyłania ministrom właściwym w trybie sprawozdawczym, nie stają się dokumentami urzędowymi.

Ważne

Reasumując, sprawozdania fundacji składane do właściwego ministra z całą pewnością nie stanowią informacji publicznej jako takie, lecz mogą zawierać w swojej treści informacje publiczne i te elementy powinny być poddane ocenie możliwego ich ujawnienia.

Czy obowiązek upublicznienia sprawozdań czyni je jawną informacją publiczną

Obowiązek upublicznienia przez samą fundację treści sprawozdania, jaki wynika z treści art. 12 ust. 3 FundU, nie ma żadnego wpływu na status sprawozdania z punktu widzenia prawa do informacji. Przepis art. 12 ust. 3 FundU jest typowym *lex imperfecta*, gdyż nie wskazuje żadnej sankcji z tym związanej, w razie gdyby sama fundacja nie realizowała obowiązku upublicznienia. Kto bowiem miałby i w jakim trybie wymóc na fundacji realizację obowiązku upublicznienia sprawozdania? Jedyny możliwy mechanizm to próba złożenia skargi na bezczynność do WSA na faktyczne działania polegające na nieupublicznieniu sprawozdania. Czy jednak tego typu działania mieszczą się w zakresie dopuszczalnej kognicji sądów administracyjnych? Zgodnie z art. 3 § 2 pkt 9 ustawy – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2017 r. poz. 1369 ze zm.), sądy administracyjne sprawują kontrolę działalności administracji publicznej, która obejmuje orzekanie w sprawach skarg na m.in.: bezczynność w ramach postępowania administracyjnego określonego w KPA. Działanie fundacji, a może raczej jego brak, które wynika z treści obowiązku wynikającego z art. 12 ust. 3 FundU nie jest postępowaniem administracyjnym, ani też postępowaniem, do którego mają zastosowanie przepisy KPA, zatem wydaje się, że ewentualna skarga na bezczynność fundacji polegającą na nieupublicznieniu sprawozdania składanego właściwemu ministrowi, nie może być przedmiotem skargi na bezczynność, a tym samym skarga taka powinna zostać odrzucona jako niedopuszczalna.

Podsumowując, **każdy minister jest zobowiązany do rozważenia zakresu ujawnienia tych informacji ze sprawozdania fundacji, które odnoszą się do realizacji przez fundację zadań publicznych**.

dr Piotr Sitniewski
Prezes fundacji JAWNOSC.PL
www.jawnosc.pl

Podstawa prawna

- art. 12 ustawy z 6.4.1984 r. o fundacjach (t.j. Dz.U. z 2016 r. poz. 40 ze zm.)
- art. 4 ust. 1 pkt 5 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764)

Sprzeciw od oferty zawierającej warunki ponownego wykorzystywania informacji sektora publicznego

Zasadą jest, że informacje sektora publicznego udostępnia się lub przekazuje w celu ich ponownego wykorzystywania bezwarunkowo. Podmiot zobowiązany może jednak, poprzez przedstawienie oferty, określić warunki ponownego wykorzystywania. Od oferty przysługuje wnioskodawcy prawo sprzeciwu. Poniżej przedstawiono wzór sprzeciwu wraz z praktycznymi objaśnieniami.

Barbara Pietrzak
Radca prawny, pracownik samorządowy

Po wpłynięciu do podmiotu zobowiązanego wniosku o ponowne wykorzystywanie informacji sektora publicznego, podmiot ten, o ile posiada przedmiotowe informacje, może podjąć jedno z następujących działań:

1) przekazać informację sektora publicznego w celu ponownego wykorzystywania bez określania warunków ponownego wykorzystywania;
2) poinformować o braku warunków ponownego wykorzystywania w przypadku posiadania informacji sektora publicznego przez wnioskodawcę;
3) złożyć ofertę zawierającą warunki ponownego wykorzystywania lub informację o wysokości opłat za ponowne wykorzystywanie;
4) odmówić, w drodze decyzji, wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego.

Jeżeli podmiot zobowiązany zdecyduje się określić warunki ponownego wykorzystywania lub ustalić opłatę za ponowne wykorzystywanie, powinien w tym celu złożyć wnioskodawcy ofertę. Wnioskodawca może ofertę przyjąć w terminie 14 dni od dnia jej otrzymania lub też złożyć od niej sprzeciw.

Ważne

Podstawą złożenia sprzeciwu powinno być naruszenie przepisów ustawy o ponownym wykorzystywaniu informacji sektora publicznego. Naruszenie to należy w sprzeciwie wskazać.

Brak zawiadomienia o przyjęciu oferty w terminie 14 dni od dnia jej otrzymania jest równoznaczny z wycofaniem wniosku.

Zgodnie z art. 23 ust. 3 ustawy z 25.2.2016 r. o ponownym wykorzystywaniu informacji sektora publicznej

(Dz.U. z 2016 r. poz. 352 ze zm.; dalej: InfSekPublU), w przypadku otrzymania sprzeciwu podmiot zobowiązany, w drodze decyzji, rozstrzyga o warunkach ponownego wykorzystywania lub o wysokości opłat za ponowne wykorzystywanie. Brzmienie przywołanego przepisu wskazuje na konieczność wydania decyzji niezależnie od tego, czy podmiot zobowiązany uzna, że sprzeciw jest zasadny bądź niezasadny. Podmiot zobowiązany może zatem wydać decyzję określającą warunki i opłaty tożsame z tymi zawartymi w ofercie lub też odmienne. Wydaje się, że decyzję należy wydać również w przypadku, gdy podmiot zobowiązany uzna, iż przekazanie informacji powinno być bezwarunkowe.

Wniosek dotyczący umożliwienia, przez okres nie dłuższy niż 12 miesięcy, ponownego wykorzystywania

Odmiennie ma się sytuacja w przypadku wniosku dotyczącego umożliwienia, przez okres nie dłuższy niż 12 miesięcy, ponownego wykorzystywania, w sposób stały i bezpośredni w czasie rzeczywistym, informacji sektora publicznego gromadzonych i przechowywanych w systemie teleinformatycznym podmiotu zobowiązanego. W takim przypadku podmiot zobowiązany może:

1) złożyć ofertę zawierającą warunki ponownego wykorzystywania lub informację o wysokości opłat za ponowne wykorzystywanie;
2) poinformować wnioskodawcę o braku możliwości ponownego wykorzystywania w sposób wskazany we wniosku;
3) odmówić, w drodze decyzji, wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego.

Od oferty złożonej w odpowiedzi na taki wniosek nie przysługuje sprzeciw. Wnioskodawca może jedynie w terminie 14 dni od dnia otrzymania wniosku przyjąć ofertę, zawiadamiając o tym podmiot zobowiązany. Brak zawiadomienia o przyjęciu oferty w terminie 14 dni od dnia jej otrzymania jest równoznaczny z wycofaniem wniosku.

Wzór sprzeciwu od oferty zawierającej warunki ponownego wykorzystywania informacji sektora publicznego

Prezydent Miasta .....

(adres)

SPRZECIW

Działając w imieniu Fundacji XYZ, pełnomocnictwo w załączeniu[1], na podstawie art. 23 ust. 2 ustawy z 25.2.2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2016 r. poz. 352, dalej „ustawa") składam sprzeciw od oferty z dnia 11 kwietnia 2017 r. znak: ABC.1.12.2017 zawierającej warunki ponownego wykorzystywania informacji sektora publicznego.

Wyżej wymienionej ofercie zarzucam naruszenie przepisów ustawy tj. art. 8 ust. 1 poprzez nierówne traktowanie Fundacji XYZ w stosunku do innych podmiotów uprawnionych do ponownego wykorzystywania.

UZASADNIENIE

Fundacja XYZ, w dniu 30.9.2017 r. zwróciła się do Prezydenta Miasta ..... z wnioskiem o ponowne wykorzystanie informacji sektora publicznego – lokalizacji przystanków autobusowych oraz tramwajowych znajdujących się na terenie Miasta, wraz z podaniem dokładnych współrzędnych geograficznych ich położenia.

W odpowiedzi na wniosek Prezydent Miasta … złożył Fundacji XYZ ofertę zawierającą warunki ponownego wykorzystywania informacji sektora publicznego. W ofercie wskazano, że przy ponownym wykorzystywaniu informacji sektora publicznego konieczne jest informowanie, iż informacje te zostały uzyskane od Miasta ..... oraz że Miasto nie ponosi odpowiedzialności za udostępniane lub przekazywane informacje[2], [3].

Jednocześnie, Prezydent Miasta ..... w odpowiedzi na wniosek o ponowne wykorzystywanie informacji sektora publicznego, złożony przez Spółkę EFG S.A. w styczniu 2017 r. dotyczący również zlokalizowania przystanków na terenie Miasta oraz wskazania tras miejskich autobusów, przekazał Spółce informację sektora publicznego w celu ponownego wykorzystywania, bez określania warunków ponownego wykorzystywania.

W tym miejscu wskazuję, że zgodnie z art. 8 ust. 1 ustawy, podmiot zobowiązany w porównywalnych sytuacjach udostępnia lub przekazuje informacje sektora publicznego w celu ponownego wykorzystywania na takich samych zasadach. W ocenie Fundacji wniosek złożony przez Spółkę i wniosek Fundacji są wnioskami na tyle zbliżonymi, co do zakresu informacji oraz sposobu i formy ich udostępnienia, że zachodzi porównywalność obu sytuacji. Oznacza to, że podmiot zobowiązany powinien potraktować wniosek Fundacji i wniosek Spółki w ten sam sposób, tj. udostępnić informacje sektora publicznego bezwarunkowo lub określić takie same warunki w ofertach. Skoro zatem Spółce przekazano informację bezwarunkowo, to również tak samo informacje powinny zostać przekazane Fundacji.

Z powyższych względów niniejszy sprzeciw jest uzasadniony.

.....

(podpis)

Objaśnienia

[1] Pełnomocnictwo

Sprzeciw powinien złożyć sam wnioskodawca lub osoba uprawniona do działania w jego imieniu. Upoważnienie do działania może wynikać z dokumentu pełnomocnictwa lub np. ze statutu, odpisu aktualnego z Krajowego Rejestru Sądowego – w przypadku osób prawnych.

[2] Obligatoryjność i fakultatywność określania warunków ponownego wykorzystywania

Obligatoryjne jest określenie przez podmiot zobowiązany warunków ponownego wykorzystywania informacji sektora publicznego, mających cechy utworu lub przedmiotu praw pokrewnych w rozumieniu przepisów ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych lub stanowiących bazę danych w rozumieniu przepisów ustawy z 27.7.2001 r. o ochronie baz danych, o ile autorskie prawa majątkowe lub prawa pokrewne przysługują podmiotowi zobowiązanemu. W pozostałych przypadkach podmiot zobowiązany może, ale nie musi określać warunków ponownego wykorzystywania – jest to jego uprawnienie, nie obowiązek.

[3] Katalog warunków ponownego wykorzystywania

W art. 14 ust. 1 InfSekPublU wskazano katalog możliwych do określenia przez podmiot zobowiązany warunków ponownego wykorzystywania.

Należą do nich:

1) obowiązek poinformowania o źródle, czasie wytworzenia i pozyskania informacji od podmiotu zobowiązanego;
2) obowiązek poinformowania o przetworzeniu informacji ponownie wykorzystywanej;
3) zakres odpowiedzialności podmiotu zobowiązanego za udostępniane lub przekazywane informacje.

W przypadku informacji sektora publicznego, mających cechy utworu lub przedmiotu praw pokrewnych w rozumieniu przepisów ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych lub stanowiących bazę danych w rozumieniu przepisów ustawy z 27.7.2001 r. o ochronie baz danych, warunkiem ponownego wykorzystywania jest również obowiązek poinformowania o nazwisku, imieniu lub pseudonimie twórcy lub artysty wykonawcy, jeżeli jest znany. W przypadku muzeów państwowych, muzeów samorządowych, bibliotek publicznych, bibliotek naukowych i archiwów wskazany wyżej katalog podlega rozszerzeniu o warunki wskazane w art. 14 ust. 2 InfSekPublU.

Podstawa prawna

- art. 23 ust. 3 ustawy z 25.2.2016 r. o ponownym wykorzystywaniu informacji sektora publicznej (Dz.U. z 2016 r. poz. 352 ze zm.)

Postępowanie w sytuacji braku uzyskania informacji publicznej – schemat postępowania

Kamila Kędzierska
Radca prawny, ekspert z zakresu dostępu do informacji publicznej

Wniosek o dostęp do informacji publicznej składany na podstawie przepisów ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764; dalej: DostInfPubU) ma na celu udostępnienie wnioskowanych informacji. W niektórych jednak przypadkach nie dochodzi do udostępnienia wnioskodawcy żądanych przez niego informacji. Na poniższym schemacie przedstawione zostało dalsze postępowanie w takich właśnie sytuacjach.

W pierwszej kolejności należy prześledzić postępowanie w sytuacji wydania przez adresata wniosku o dostęp do informacji publicznej decyzji odmawiającej udostępnienia wnioskowanych informacji. Jak wskazano na schemacie, podstawą wydania takiej decyzji może być:

1. Ochrona prywatności osób fizycznych (art. 5 ust. 2 DostInfPubU).
2. Ochrona tajemnicy przedsiębiorcy (art. 5 ust. 2 DostInfPubU).
3. Ochrona innych tajemnic ustawowo chronionych (art. 5 ust. 1 DostInfPubU).
4. Brak szczególnie istotnego interesu publicznego w udostępnieniu wnioskodawcy informacji przetworzonej (art. 3 ust. 1 pkt 1 DostInfPubU).

Wydanie decyzji odmownych

W przypadku wydania decyzji odmownych, zgodnie z art. 16 ust. 2 DostInfPubU, postępowanie odwoławcze prowadzone jest zgodnie z przepisami art. 127–140 ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257), z zastrzeżeniami wskazanymi w DostInfPubU. Postępowanie odwoławcze w omawianej sytuacji polegać może bądź na złożeniu odwołania od decyzji do organu wyższego stopnia (art. 127 § 2 KPA), bądź na złożeniu do organu I instancji wniosku o ponowne rozpatrzenie sprawy (art. 127 § 3 KPA).

Co powinno zawierać odwołanie

Odwołanie powinno zawierać co najmniej wskazanie osoby, od której pochodzi, jej adres i żądanie (art. 63 § 2 KPA), nie wymaga jednak szczegółowego uzasadnienia. Wystarczy, jeżeli z odwołania wynika, że strona nie jest zadowolona z wydanej decyzji (art. 128 KPA). W związku z powyższym należy zwrócić szczególną uwagę na wszelką korespondencję kierowaną do organu I instancji po wydaniu przez ten organ decyzji odmawiającej udostępnienia informacji. Może bowiem zdarzyć się tak, że wnioskodawca skieruje

do organu pismo zatytułowane „skarga" lub nie zawierające oznaczenia rodzaju, które jednak w istocie stanowić będzie odwołanie od wydanej decyzji. Rolą organu, który otrzymał tego typu korespondencję jest ocenić, czy nie stanowi ona w istocie odwołania od wydanej decyzji administracyjnej.

Złożenie skargi do sądu administracyjnego

Kolejnym etapem, w przypadku utrzymania w mocy decyzji organu I instancji, jest złożenie skargi do sądu administracyjnego. Z uwagi na fakt, że stroną takiego postępowania jest organ II instancji, najczęściej organ wydający decyzję nie jest świadomy, iż toczy się postępowanie sądowoadministracyjne dotyczące także wydanej przez niego decyzji odmawiającej udostępnienia informacji.

Ważne

Inaczej prezentuje się ścieżka postępowania w przypadku nieudostępnienia wnioskowanej informacji, bądź to w wyniku bezczynności, bądź też z uwagi na dokonaną przez adresata wniosku ocenę wskazującą, że wnioskowana informacja nie stanowi informacji publicznej i jako taka nie podlega udostępnieniu.

O bezczynności adresata wniosku mówimy w sytuacji, gdy nie ustosunkował się on do otrzymanego wniosku w terminie ustawowym – bez zbędnej zwłoki, nie później jednak niż 14 dni od dnia otrzymania wniosku (art. 13 ust. 1 DostInfPubU) lub też w terminie przedłużonym, zgodnie z art. 13 ust. 2 DostInfPubU.

ORZECZENIE

Jak wskazał WSA w Poznaniu w wyroku z 5.4.2017 r. (IV SAB/Po 15/17, Legalis), bezczynność polega zasadniczo na nieudostępnieniu informacji i na niewydaniu decyzji o odmowie jej udzielenia lub decyzji o umorzeniu postępowania, jak też niepoinformowaniu, iż organ nie dysponuje żądną informacją lub że żądana informacja nie ma charakteru informacji publicznej. Stan bezczynności ustępuje w sytuacji, gdy organ udostępni żądaną informację w zakresie i w formie wnioskowanej przez podmiot zainteresowany jej uzyskaniem.

ORZECZENIE

W tym zakresie niezwykle istotny jest pogląd zaprezentowany przez NSA w wyroku z 14.4.2017 r. (I OSK 2221/16, Legalis), zgodnie z którym okoliczność zwrócenia się do strony o wykazanie spełnienia przesłanki istnienia szczególnego interesu publicznego, nie zwalnia organu od dochowania terminów, z jakimi ustawa o dostępie do informacji publicznej wiąże obowiązek udzielenia odpowiedzi na złożony wniosek.

ORZECZENIE

Należy także zwrócić uwagę na stanowisko NSA z 27.1.2017 r. (I OSK 2626/16, Legalis), w którym sąd wskazał, że przedstawienie informacji innej niż ta, na którą oczekuje wnioskodawca, informacji niepełnej lub też informacji wymijającej, czy wręcz nieadekwatnej do treści wniosku, świadczy o bezczynności podmiotu zobowiązanego do udostępnienia informacji publicznej, do którego skierowano wniosek o jej udostępnienie, co niewątpliwie narusza regulację zawartą w art. 13 ust. 1 DostInfPubU.

W sytuacji pozostawania adresata wniosku w bezczynności, wnioskodawca uprawniony jest do złożenia skargi do sądu administracyjnego. Zgodnie z utrwaloną linią orzeczniczą (por. wyr. WSA w Rzeszowie z 25.8.2016 r., II SAB/Rz 56/16, Legalis; post. NSA z 22.7.2014 r., I OZ 522/14, Legalis), skarga na bezczynność w zakresie udzielenia informacji publicznej jest dopuszczalna bez konieczności uprzedniego wyczerpania środków zaskarżenia na drodze administracyjnej. Przed jej wniesieniem nie jest również konieczne wezwanie właściwego organu do usunięcia naruszenia prawa w trybie art. 52 § 3 lub 4 ustawy z 30.8.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2016 r. poz. 718 ze zm.), gdyż tryb przewidziany w tych przepisach odnosi się do aktów i czynności, a nie bezczynności. W związku z powyższym niezasadne jest wymaganie przez adresata wniosku od wnioskodawcy dokonywania jakichkolwiek czynności poprzedzających złożenie skargi do sądu administracyjnego.

W momencie otrzymania skargi adresat wniosku zobowiązany jest do jej procedowania, zgodnie z regułami określonymi w przepisach Prawa o postępowaniu przed sądami administracyjnymi z zastrzeżeniami wynikającymi z DostInfPubU. Po otrzymaniu skargi organ powinien przekazać ją sądowi wraz z aktami sprawy i odpowiedzią na skargę w terminie 15 dni od dnia jej wniesienia (art. 21 pkt 1 DostInfPubU). Niezależnie od tego obowiązku, organ może rozpatrzyć sprawę i wydać akt (np. decyzję odmawiającą udostępnienia informacji) lub podjąć czynność materialno-techniczną (udostępnić wnioskowaną informację). Podjęcie działań przez organ administracji może nastąpić również po przesłaniu skargi wraz z odpowiedzią do sądu, a przed dniem rozstrzygnięcia sprawy przez sąd administracyjny. W takim wypadku okoliczność, że sprawa została załatwiona, będzie wzięta pod uwagę przy orzekaniu w sprawie przez sąd, który albo oddali skargę na bezczynność, albo też umorzy postępowanie (por. wyr. NSA z 15.5.2015 r., I OSK 1329/14, Legalis).

Podobna droga postępowania występuje w sytuacji, gdy adresat wniosku poinformował, że wnioskowana informacja nie stanowi informacji publicznej, wbrew stanowisku wnioskodawcy lub też gdy poinformował, że nie dysponuje wnioskowaną informacją.

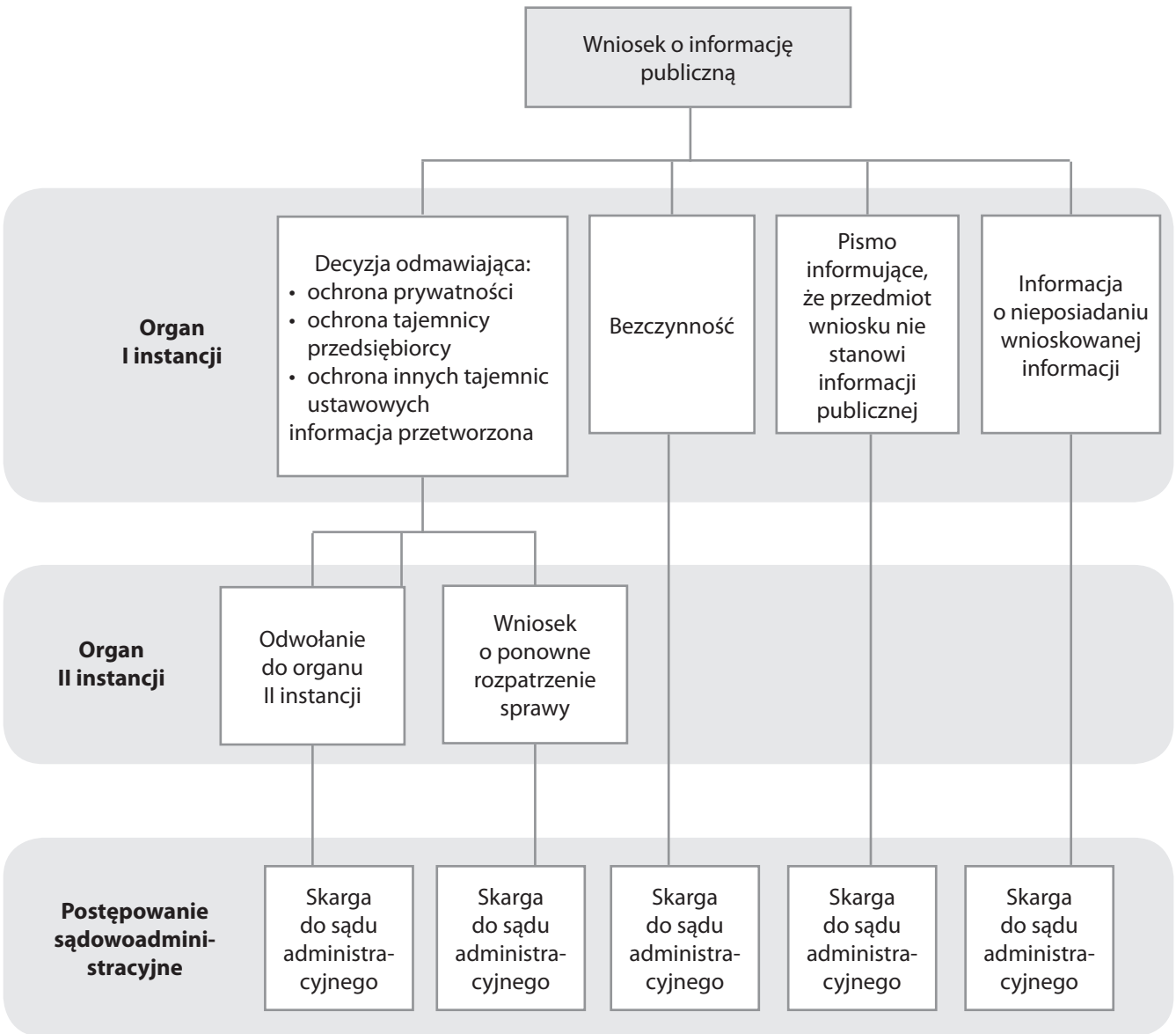
ORZECZENIE

Jak wskazał WSA w Białymstoku w wyroku z 10.11.2015 r. (II SAB/Bk 62/15, Legalis) niezależnie od tego, czy w ocenie podmiotu zobowiązanego do udostępnienia informacji publicznej, wnioskowane dane nie stanowią informacji publicznej lub że podmiot nie jest zobowiązany do jej udzielenia, albo że nie dysponuje daną informacją, bądź że w sprawie zastosowanie ma odmienny tryb dostępu do informacji, podmiot ten zobowiązany jest do poinformowania wnioskodawcy o zajętym stanowisku, choćby w formie zwykłego pisma. Nie do zaakceptowania jest zaś sytuacja, gdy podmiot taki, po otrzymaniu wniosku o udostępnienie informacji publicznej, nie reaguje na niego w żaden sposób uzewnętrzniony wnioskodawcy. Dopiero bowiem reakcja organu uwalnia go od zarzutu bezczynności.

Podstawa prawna

- art. 3 ust. 1 pkt 1, art. 5 ust. 1 i 2, art. 16 ust. 2, art. 21 pkt 1 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 poz. 1764)
- art. 127–140 ustawy z 14.6.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257)
- art. 52 § 3 lub 4 ustawy z 30.8.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2016 r. poz. 718 ze zm.)

Schemat postępowania w sytuacji braku uzyskania informacji publicznej



Dostęp do oświadczeń majątkowych osób, których oświadczenia majątkowe są jawne i podlegają opublikowaniu w BIP

Komentowany wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z 29.9.2016 r., (II SAB/Wr 115/16, Legalis) dotyczy problematyki związanej z dostępem do oświadczeń majątkowych osób, których oświadczenia majątkowe są jawne i podlegają opublikowaniu w BIP, ale które wskutek różnych okoliczności nie zostały tam zamieszczone.

dr hab. Przemysław Szustakiewicz
Profesor Uczelni Łazarskiego

Przedmiotowa sprawa została wszczęta wnioskiem osoby zainteresowanej o udostępnienie informacji publicznej w postaci kopii oświadczeń majątkowych za 2015 r. następujących osób: burmistrza, zastępcy burmistrza, sekretarza, skarbnika gminny, wszystkich radnych gminnych, oraz dyrektorów i kierowników jednostek budżetowych jednej z gmin położonych w Województwie Dolnośląskim.

Burmistrz odpowiedział wnioskodawcy, że skany oświadczeń majątkowych za 2015 r. zostały opublikowane na gminnej stronie BIP, natomiast oświadczenia Burmistrza oraz Przewodniczącej zostaną udostępnione po weryfikacji i odesłaniu przez Wojewodę.

Wnioskodawca niezadowolony z udzielonej mu odpowiedzi wniósł do WSA we Wrocławiu skargę na bezczynność Burmistrza, domagając się zobowiązania Burmistrza do załatwienia wniosku z 11.5.2016 r. W uzasadnieniu wskazał on, że do dnia złożenia skargi nie zostały mu udostępnione wszystkie z żądanych oświadczeń majątkowych, a na stronie BIP brak jest oświadczeń Burmistrza i Przewodniczącej Rady.

Podmiot zobowiązany w odpowiedzi na skargę wskazał, że nie pozostaje w bezczynności, ponieważ oświadczenia o stanie majątkowym zarówno Burmistrza, jak P0rzewodniczący Rady Gminy zostaną udostępnione w BIP po weryfikacji i odesłaniu przez Wojewodę, gdyż jak wynika z art. 24h ust. 3 pkt 2 ustawy z 8.3.1990 r. o samorządzie gminnym (t.j. Dz.U. z 2017 r. poz. 1875; dalej: SamGminU), oświadczenia majątkowe wójtów (burmistrzów, prezydentów) oraz przewodniczących rad gmin składane są przez nich do właściwych wojewodów. Dopiero więc po otrzymaniu od Wojewody stosownej

Teza

Fakt nieopublikowania w BIP oświadczenia majątkowego funkcjonariusza samorządu gminnego, o którym mowa w art. 24h ust. 1 SamGminU nie oznacza, że nie ma ono waloru jawności, albowiem staje się ono jawne z chwilą jego złożenia. W związku z tym może być ono udostępnione na wniosek informacyjnie zainteresowanego w trybie art. 10 DostInfPubU.

kopii złożonych oświadczeń majątkowych możliwe staje się udostępnienie tych informacji publicznych, w tym poprzez udostępnienie ich w BIP. Omawiane oświadczenia majątkowe zostały doręczone przez Wojewodę organowi i niezwłocznie, tak jak nakazuje art. 24i ust. 3 SamGminU zostały udostępnione w BIP.

Sąd oddalił skargę, ponieważ uznał, że informacja została udostępniona w BIP, ale jednocześnie nie podzielił stanowiska podmiotu zobowiązanego, wedle którego dopóki oświadczenia majątkowe znajdują się u Wojewody w zasadzie nie podlegają ujawnieniu. Sąd zauważył bowiem, że z treści art. 24i ust. 2 SamGminU wynika, że organ wykonawczy i przewodniczący rady gminy przekazują wójtowi kopie oświadczeń majątkowych, które im złożono. Z ustawy o samorządzie gminnym nie można natomiast wywieść, w jakim terminie wojewoda zobowiązany jest do odesłania kopii złożonych mu oświadczeń. Dopóki jednak organ ten nie przekaże wójtowi kopii złożonych mu oświadczeń, nie mogą być one opublikowane w BIP, pomimo że *de facto* wójt i przewodniczący rady pozostają w ich posiadaniu. Natomiast fakt nieopublikowania w BIP oświadczenia majątkowego funkcjonariusza samorządu gminnego, o którym mowa w art. 24h ust.1 SamGminU, nie oznacza, że nie ma ono waloru jawności, ponieważ staje się ono jawne z chwilą jego złożenia. W związku z tym może być ono udostępnione na wniosek zainteresowanego.

Stanowisko WSA

Stanowisko WSA we Wrocławiu jest niewątpliwie trafne. Nawiązuje ono bowiem do konstytucyjnej (art. 61 ust. 1 ustawy z 2.4.1997 r. – Konstytucja Rzeczypospolitej Polskiej, Dz.U. Nr 78, poz. 483 ze zm. i sprost.) zasady jawności wedle której sprawy publiczne są jawne. Niewątpliwie, co wynika wprost z art. 24i SamGminU, zasada ta dotyczy jawności oświadczeń majątkowych wysokich funkcjonariuszy podstawowej jednostki samorządu terytorialnego, którą jest gmina. Należy wskazać, że obowiązek składania oświadczeń majątkowych przez wymienionych w art. 24h ust. 1 SamGminU funkcjonariuszy publicznych posiada szczególne ostrze antykorupcyjne, ponieważ pozwala społeczeństwu kontrolować, czy w przypadku osób gospodarujących mieniem publicznym nie dochodzi do niespodziewanego, niemającego podstaw w ich dochodach „przyrostu" majątku. Utrudnia to również ukrycie takiego majątku. Stąd obowiązek publikacji oświadczeń majątkowych w BIP prowadzonym przez daną jednostkę samorządu terytorialnego. Nadto należy pamiętać, że organ wykonawczy gminy odpowiada za publikację w BIP oświadczeń majątkowych składanych przez wszystkich funkcjonariuszy samorządu gminnego. Dotyczy to także jego własnego oświadczenia oraz oświadczenia przewodniczącego rady a także wszystkich radnych. Jednak warunkiem publikacji oświadczenia organu wykonawczego gminy (wójt, burmistrz, prezydent) oraz przewodniczącego rady jest przekazanie ich kopii wójtowi przez wojewodę. W SamGminU brak ustawowo zakreślonego terminu, w jakim oświadczenia należy zamieścić w BIP. Wydaje się jednak oczywiste, że oświadczenia powinny być publikowane niezwłocznie po ich złożeniu. Z art. 24i ust. 2 SamGminU wynika, że wojewoda i przewodniczący rady gminy przekazują wójtowi (burmistrzowi, prezydentowi) kopie oświadczeń majątkowych, które im złożono. Z ustawy o samorządzie gminnym nie wynika natomiast, w jakim terminie wojewoda zobowiązany jest do odesłania kopii złożonych mu oświadczeń. Dopóki jednak wojewoda nie przekaże organowi wykonawczemu gminy kopii złożonych mu oświadczeń, nie mogą być one opublikowane w BIP, pomimo że faktycznie zarówno organ wykonawczy, jak i przewodniczący rady pozostają w ich posiadaniu.

Brak zakazu udostępniania oświadczeń majątkowych

W omawianej sprawie burmistrz nieprawidłowo przyjął, że istnieje swego rodzaju zakaz udostępniania oświadczeń majątkowych, które nie zostały zweryfikowane przez wojewodę i zwrócone właściwemu organowi gminy do publikacji w BIP. Tymczasem SamGminU nie wprowadza takiego zakazu.

Ważne

Przypomnieć też należy, że orzecznictwo sądów administracyjnych od lat stoi na stanowisku, że nie można zakazu udostępnienia informacji wywodzić z interpretacji przepisów. Zakaz taki musi być jasno sprecyzowany, aby można było skutecznie odmówić udostępnienia informacji (por. wyr. WSA w Gdańsku z 20.1.2005 r., II SAB/Gd 66/04, Legalis; wyr. NSA z 21.9.2012 r., I OSK 1393/12,

Legalis), a same przepisy wyłączające stosowanie ustawy o dostępie do informacji publicznej powinny być wykładane ściśle.

Zasadą bowiem jest jawność życia publicznego. Oznacza to również pewną zmianę myślenia podmiotu zobowiązanego, który powinien robić wszystko, aby ujawniać posiadane informacje. Dlatego też ujawnienie tak ważnych informacji jakimi są oświadczenia majątkowe osób pełniących najważniejsze funkcje publiczne w podstawowej jednostce samorządu terytorialnego, jaką jest gmina nie może być uzależnione od wojewody, który nieskrępowany żadnymi terminami mógłby na wiele miesięcy, a nawet lat, uniemożliwić ujawnienia oświadczenia majątkowego wójta (burmistrza, prezydenta) oraz przewodniczącego rady. Taka sytuacja rodziłaby, co oczywiste, pole do nadużyć.

Podstawa prawna

- art. 24h ust. 3 pkt 2, 24i ust. 13 ustawy z 8.3.1990 r. o samorządzie gminnym (t.j. Dz.U. z 2017 r. poz. 1875)
- art. 10 ustawy z 6.9.2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764)

Podsumowanie

Jak słusznie podniesiono w komentowanym orzeczeniu, już z chwilą złożenia oświadczenia majątkowe są jawne, a procedura weryfikacji oświadczenia majątkowych organu wykonawczego gminy i przewodniczącego rady przez wojewodę dotyczy jedynie kwestii technicznej, tj. momentu, od którego można takie oświadczenie opublikować w BIP, nie ma ona natomiast żadnego znaczenia, gdy chodzi o kwestie jawności oświadczenia majątkowego, które może być udostępnione w trybie wnioskowym.

Nowelizacja ustawy o ochronie informacji niejawnych

„Czy ustawa z 5.8.2010 r. o ochronie informacji niejawnych była nowelizowana?"

ODPOWIEDŹ

Ustawa z 5.8.2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2016 r. poz. 1167 ze zm.; dalej: OchrInfU) została przygotowana w sposób profesjonalny, projekt poddano szerokiej konsultacji, opiniowaniu, obowiązuje od 2.1.2011 r., jest sprawdzona w praktyce. Jednak niektóre z jej przepisów wymagają pewnych zmian, ale takich propozycji rząd nie zgłasza. Dokonano natomiast kilku zmian, mających charakter redakcyjny, wynikający z nowelizacji innych ustaw.

Zmiany art. 3 OchrInfU

Artykuł 3 OchrInfU, znowelizowany przez art. 13 ustawy z 7.4.2017 r. o zmianie ustawy – Kodeks postępowania administracyjnego oraz niektórych innych ustaw (Dz.U. z 2017 r. poz. 935), otrzymuje brzmienie. „Do postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego, w zakresie nie uregulowanym w ustawie, mają zastosowanie przepisy art. 6, art. 7, art. 8, art. 12, art. 14–16, art. 24 § 1 pkt 1–6 i § 2–4, art. 26 § 1, art. 28, art. 29, art. 30 § 1–3, art. 35 § 1, art. 39, art. 41–47, art. 50, art.55, art. 57–60, art. 61 § 3 i 4, art. 63 § 4, art. 64, art. 65, art. 72, art. 75 § 1, art. 77 § 1, art. 97 § 1 pkt 4 i § 2, art. 98, art.101, art. 103, art. 104, art. 105 § 2, art. 107, art. 109 § 1, art. 112, art. 113 § 1, art. 125 § 1, art. 156–158 oraz art. 217 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego…" .

Jest to zmiana redakcyjna, występujące wcześniej na początku wyliczanki wyrazy „art. 6–8", (czyli art. 6, art. 7, art. 8) zastąpiono wyrazami „art. 6, art. 7, art. 8". Nie jest to więc zmiana merytoryczna. Warto nadmienić, że ustawa zmieniająca dodała w KPA między art. 7 i 8 dwa dodatkowe art. 7a i 7b. Dlatego też pozostawienie w art. 3 OchrInfU dotychczasowego zwrotu („art. 6–8"), spowodowałoby objęcie jego zakresem także tych dodatkowych przepisów: „art. 6, art. 7, art. 7b, art. 8".

Brak takiego uzasadnienia.

Zmiany w KPA, mające wpływ na OchrInfU

Spośród przepisów ustawy z 14.6.1960 r. Kodeks postępowania administracyjnego (t.j. Dz.U. z 2017 r. poz. 1257) mających zastosowanie w postępowaniach prowadzonych na podstawie OchrInfU dokonano zmiany w następujących przepisach:

- art. 16 – dodano § 3 w brzmieniu: „§ 3. Decyzje ostateczne, których nie można zaskarżyć do sądu, są prawomocne", usunięto więc lukę w przepisach KPA;
- art. 64 § 2 – termin siedmiu dni na usunięcie braków formalnych w podaniu zastąpiono „wyznaczonym terminem, nie krótszym niż siedem dni";
- art. 107 § 1 – dokonano kilku zmian, dotychczasową redakcję (dwa zdania) zastąpiono punktami, w zdaniu wstępnym („decyzja powinna zawierać") pominięto wyraz „powinna", w obecnym pkt 8, dotyczącym podpisu, wyrazy „osoby upoważnionej" zastąpiono wyrazami „pracownika organu upoważnionego", rozbudowano treść pkt 7 i 9, dotyczących pouczeń.

Art. 5 ust. 7 OchrInfU

Art. 5 ust. 7 OchrInfU, znowelizowany przez art. 23 ustawy z 28.11.2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz.U. z 2015 r. poz. 21), która weszła w życie 8.4.2015 r., przez dodanie zwrotu: „osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie z 28.11.2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka".

Art. 7 ust. 2 OchrInfU

Art. 7 ust. 2 OchrInfU, znowelizowany przez art. 8 ustawy z 29.4.2016 r. o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 749), która weszła w życie 16.6.2016 r., poprzez zastąpienie zwrotu „chyba, że dostęp do określonych dokumentów został zastrzeżony w trybie art. 39 ustawy wymienionej w pkt 1" zwrotem „chyba, że nadano im klauzulę tajności w wyniku przeglądu, o którym mowa w art. 19 ustawy z 29.4.2016 r. o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 749), lub przeglądu, o którym mowa w art. 6 ust. 4".

Art. 34 ust. 10 pkt 15 OchrInfU

Art. 34 ust. 10 pkt 15 OchrInfU, znowelizowany przez art. 22 ustawy z 10.7.2015 r. o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 1224), która weszła w życie 1.1.2016 r., poprzez dodanie asesora sądowego, wobec którego nie przeprowadza się postępowania sprawdzającego.

Prof. Stanisław Hoc

▶ Podstawa prawna

- art. 3, art. 5 ust. 7, art. 16, art. 34 ust. 10 pkt 15, art. 64 § 2, art. 107 § 1 ustawy z 5.8.2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2016 r. poz. 1167 ze zm.)

Żądanie udostępnienia danych dziennikarza a tajemnica dziennikarska

„W lokalnej gazecie opublikowano nieprawdziwy i obraźliwy artykuł na temat funkcjonowania jednego z wydziałów naszego urzędu. Podjęliśmy decyzję o dochodzeniu roszczeń za naruszenie dóbr osobistych na drodze sądowej. Redakcja gazety odmawia podania danych autora artykułu powołując się na tajemnicę dziennikarską. Czy słusznie i gdzie można się odwołać od jej stanowiska?"

ODPOWIEDŹ

Ocena, czy udostępnienie danych autora artykułu prasowego na potrzeby procesu sądowego narusza tajemnicę dziennikarską będzie zależała od okoliczności faktycznych sprawy. Jednakże odmowa ujawnienia wnioskowanych danych może być przedmiotem kontroli Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Jeśli organ uzna, że działania redakcji naruszyły prawo, to działając w oparciu o art. 18 ust. 1 pkt 2 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. 2016 r. poz. 922; dalej: OchrDanychU) nakaże redakcji udostępnienie żądanych danych osobowych.

Solidarna odpowiedzialność podmiotów prasowych

Podmiotowi, którego dobra osobiste zostały naruszone nierzetelnym artykułem prasowym przysługuje możliwość pociągnięcia do odpowiedzialności cywilnej autora artykułu, redaktora, jak również innych osób, które spowodowały opublikowanie materiału prasowego, np. wydawcy (art. 38 ustawy z 26.1.1984 r. Prawo Prasowe – Dz.U. Nr 5 poz. 24 ze zm.; dalej: PrPras).

W celu skutecznego dochodzenia swoich praw na drodze sądowej pokrzywdzony powinien dysponować danymi pozwalającymi na precyzyjne oznaczenie strony pozwanej. Zgodnie z wymogami określonymi w art. 187 § 1 w zw. z art. 126 § 1 i 2 ustawy z 17.11.1964 r. Kodeks postępowania cywilnego (t.j. Dz.U. z 2016 r. poz. 1822 ze zm.) w pozwie należy bowiem wskazać imiona i nazwiska lub nazwy stron oraz miejsca ich zamieszkania lub siedziby oraz adresy.

Przesłanka dopuszczalności przetwarzania danych

Żądanie udostępnienia danych osobowych autora nierzetelnego artykułu pokrzywdzony urząd może uzasadnić przesłanką dopuszczalności przetwarzania danych z art. 23 ust. 1 pkt 5 OchrDanychU.

Decyzję, czy w danym konkretnym przypadku dane w oparciu o ww. przesłankę mogą być udostępnione przeprowadza redakcja jako dysponent (administrator) tych danych. Odwołanie się od stanowiska redakcji jest możliwe poprzez zwrócenie się do GIODO o przeprowadzenie kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Jeśli GIODO uzna, że działania redakcji były sprzeczne z prawem, to nakaże jej udostępnienie żądanych danych osobowych (art. 18 ust. 1 pkt 2 OchrDanychU).

Tajemnica dziennikarska

Działania redakcji mogą być uznane za naruszające art. 23 ust. 1 pkt 5 OchrDanychU, gdy ta powołała się na przeszkody w udostępnieniu danych pomimo, że faktycznie nie miały one miejsca. Tajemnica dziennikarska jest jedną z przesłanek uzasadniających odmowę udostępnienia danych autora artykułu prasowego. Zgodnie z art. 15 ust. 2 PrPras dziennikarz, a także inne osoby zatrudnione w redakcjach mają obowiązek zachowania w tajemnicy danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych. Powinny zacho-

wać w tajemnicy także wszelkie inne informacje jeśli ich ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.

Ustalenie, czy udostępnienie danych zgodnie z wnioskiem urzędu stanowi naruszenie tajemnicy dziennikarskiej zależeć będzie od okoliczności konkretnego przypadku. Jeśli artykuł prasowy był opublikowany anonimowo lub opatrzony był pseudonimem, to redakcja słusznie odmawia podania danych osobowych jego autora. W myśl bowiem art. 15 ust. 1 PrPras autorowi materiału prasowego przysługuje prawo zachowania w tajemnicy swego nazwiska.

ORZECZENIE

Jak wskazuje się w doktrynie, tajemnica nazwiska autora wchodzi w zakres tajemnicy dziennikarskiej określonej w art. 15 ust. 2 PrPras. W takich okolicznościach urząd może dochodzić roszczeń z tytułu naruszenia dóbr osobistych jedynie od redaktora naczelnego i wydawcy (por. wyrok WSA w Warszawie z dnia 13.02.2009 r., II SA/Wa 1570/08, Legalis).

Jeśli natomiast dane osobowe autora artykułu prasowego zostały opublikowane, a urząd wnioskuje o podanie adresu miejsca zamieszkania dziennikarza, to powoływanie się przez redakcję na tajemnicę dziennikarską jest nieuzasadnione.

ORZECZENIE

Tajemnica dziennikarska przewidziana w art. 15 ust. 2 PrPras chroni osobę, która przekazuje dziennikarzowi informacje, a nie samego dziennikarza, którego obciąża realizacja obowiązku zachowania w tajemnicy jej danych (por. wyrok NSA z 22.01.2015 r., I OSK 1161/13, Legalis).

Przeszkody w udostępnieniu danych nie stanowi także art. 3a ust. 2 OchrDanychU, zgodnie z którym przepisów tej ustawy nie stosuje się do prasowej działalności dziennikarskiej.

ORZECZENIE

Zgodnie bowiem z wypracowanym w orzecznictwie sądów administracyjnych stanowiskiem, wyłączenie zawarte w tym przepisie dotyczy jedynie „prasowej działalności dziennikarskiej", a nie dziennikarzy w ogólności, rozumianych jako grupa zawodowa (por. wyrok NSA z 28.6.2011 r. I OSK 1217/10, Legalis).

Przeciwny pogląd prowadziłby do sytuacji, w której dziennikarze publikowaliby nierzetelne artykuły, bez obawy pociągnięcia ich do odpowiedzialności cywilnej.

Agnieszka Kręcisz-Sarna

▶ Podstawa prawna

- art. 18 ust. 1 pkt 2, art. 23 ust. 1 pkt 5 ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. 2016 r. poz. 922)
- art. 15 ust. 1 i 2, art. 38 ustawy z 26.1.1984 r. Prawo Prasowe (Dz.U. Nr 5 poz. 24. ze zm.)
- 126 § 1 i 2, art. 187 § 1 ustawy z 17.11.1964 r. Kodeks postępowania cywilnego (t.j. Dz.U. z 2016 r. poz. 1822 ze zm.)

Postępowanie z niejawną przesyłką oznaczoną „do rąk własnych" – schematy postępowania

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

Postępowanie z przesyłką niejawną oznaczoną „do rąk własnych" wymaga szczególnego traktowania. Nieuprawnione otwarcie takiej przesyłki może narazić osobę naruszającą obowiązujące przepisy na przykre konsekwencje prawne. Mówi o tym art. 267 § 1 Kodeksu karnego: „Kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną, otwierając zamknięte pismo, (…) podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Biorąc powyższe pod uwagę, przy otrzymaniu przesyłki niejawnej należy stosować się ściśle do postanowień zawartych w rozporządzeniu Rady Ministrów z 7.12.2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2011 r. Nr 276, poz. 1631; dalej: OrgKancR).

Schematy, opublikowane w artykule, wraz z opisem przedstawiają usystematyzowany sposób postępowania z przesyłką oznaczoną napisem „do rąk własnych", jak również zasady jej ewidencjonowania oraz postępowanie z taką przesyłką przy zwrocie jej przez adresata do kancelarii.

Schemat nr 1. Przyjęcie i udostępnienie przesyłki „Do rąk własnych"

Przesyłki niejawne przekazywane są w dwóch nieprzeźroczystych kopertach (zewnętrznej i wewnętrznej) odpowiednio oznaczonych.

Oznaczenia na kopercie zewnętrznej

Oznaczenia na kopercie zewnętrznej nie wskazują charakteru tej przesyłki. Informacje zawarte na tym opakowaniu dotyczą wyłącznie nazwy jednostki organizacyjnej adresata, adresu siedziby adresata, nazwy jednostki organizacyjnej nadawcy oraz numeru wykazu i pozycji w wykazie przesyłek nadanych.

Dlatego w każdym przypadku personel kancelarii uprawniony jest do otwarcia koperty zewnętrznej.

Oznaczenia na kopercie wewnętrznej

Zupełnie inne informacje przedstawione są na kopercie wewnętrznej. Zamieszczone są tutaj klauzule tajności i ewentualne dodatkowe oznaczenia, określenie adresata, imię, nazwisko i podpis osoby pakującej oraz numer, pod którym dokument został zarejestrowany. Przez dodatkowe oznaczenia

rozumie się na przykład napisy: „Pilne", „Do rąk własnych".

W przypadku adnotacji na kopercie wewnętrznej o treści „**do rąk własnych**" nie wolno pod żadnym pozorem otwierać tej koperty.

Ważne

Zdarzają się przypadki, wynikające z błędów personelu kancelarii nadawcy, że na kopercie wewnętrznej nie ma oznaczenia „do rąk własnych", natomiast na dokumencie wewnątrz koperty zawarto takie oznaczenie. W takim przypadku należy bezwzględnie dołączyć do dokumentu kopertę wewnętrzną (jako dowód uprawnionego otwarcia przesyłki) i w takiej formie przekazać/udostępnić przesyłkę adresatowi.

Przesyłka oznaczona adnotacją „do rąk własnych", przed przekazaniem jej adresatowi, podlega zaewidencjonowaniu na niżej wymienionych zasadach:

1. W dzienniku ewidencyjnym wpisuje się:
- symbol oznaczenia klauzuli tajności,
- numer kolejny zapisu,
- datę rejestracji dokumentu (datę wpływu przesyłki),
- nazwę nadawcy,
- numer dokumentu otrzymanego.

Ogólnie mówiąc w dzienniku ewidencyjnym wypełnia się tylko te pola, które można określić na podstawie zapisów z kopert zewnętrznej i wewnętrznej przesyłki.

Ponadto, w rubryce „Informacje uzupełniające/Uwagi" odnotowuje się, że przesyłka była oznaczona „do rąk własnych".

2. Kopertę wewnętrzną (bez jej otwierania) opatruje się:
- numerem, pod którym zarejestrowano przesyłkę,
- datą wpływu.

Po spełnieniu powyższych wymagań w zakresie ewidencyjnym, przesyłkę można przekazać wyłącznie adresatowi wskazanemu na kopercie wewnętrznej, a w razie jego nieobecności – osobie przez niego pisemnie upoważnionej do odbioru.

Ważne

Upoważnienie do odbioru korespondencji oznaczonej „do rąk własnych" musi mieć formę pisemną. Jest jednostronną czynnością prawną i można je w każdej chwili cofnąć. Upoważnienie powinno określać jego zakres – uprawnienie odbioru przesyłek oznaczonych „do rąk własnych" adresowanych do osoby udzielającej pełnomocnictwa, dane osoby upoważnionej, okres obowiązywania, a także wskazanie podmiotu udzielającego takiego pełnomocnictwa.

W sektorze publicznym, na przykład w organach administracji rządowej, organach jednostek samorządu terytorialnego, sądach, organach kontroli państwowej itp. przedmiotowe upoważnienie może być wydane również w formie decyzji, zarządzenia bądź jasno sprecyzowane w regulaminie organizacyjnym.

Przesyłkę przekazuje się za pokwitowaniem w dzienniku ewidencyjnym. Pokwitowanie polega na wpisaniu w odpowiedniej rubryce dziennika niżej wymienionych informacji:
- data pobrania przesyłki oznaczonej „do rąk własnych",
- imię i nazwisko osoby pobierającej,
- podpis osoby pobierającej.

Należy jednocześnie poinstruować osobę pobierającą przesyłkę, że w tym przypadku to do jego obowiązków należy:
- sprawdzenie, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
- ustalenie, czy liczba stron lub innych jednostek miary materiałów oraz liczba załączników jest zgodna z liczbą oznaczoną na poszczególnych materiałach.

Schemat nr 2. Zwrot do kancelarii przesyłki „Do rąk własnych"

Z chwilą zwrotu do kancelarii przesyłki, kierownik kancelarii lub inny upoważniony pracownik uzupełnia pozostałe dane dotyczące przesyłki w dzienniku ewidencyjnym:

1) w pierwszej kolejności:
   a) potwierdzenie zwrotu dokumentu (data i podpis personelu kancelarii);
2) następnie:
   a) data otrzymanego dokumentu (data nadana przez nadawcę);
   b) nazwa dokumentu lub czego dotyczy;
   c) liczba stron dokumentu lub innych jednostek miary;
   d) liczba załączników;
   e) liczba stron wszystkich załączników lub innych jednostek miary;
   f) informacje uzupełniające/uwagi – np. „pismo przewodnie JAWNE".

Należy zaznaczyć, że adresat przesyłki może zwrócić ją do kancelarii w stanie zamkniętym, w formie zabezpieczonego przez siebie pakietu lub w stanie otwartym.

Postępowanie personelu kancelarii w obu przypadkach jest odmienne.

Zwrot przesyłki do kancelarii w stanie zamkniętym

W przypadku, gdy adresat podjął decyzję o przechowywaniu w kancelarii przesyłki oznaczonej „do rąk własnych" w stanie zamkniętym, kierownik kancelarii lub inny upoważniony pracownik dokonuje czynności uzupełniających w Dzienniku Ewidencyjnym przy

udziale adresata. Adresat przesyłki zobligowany jest do podania wszystkich powyżej wymienionych informacji.

Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi". Przesyłkę taką można wpiąć do teczki przedmiotowej w formie zabezpieczonego pakietu, zgodnie z decyzją adresata.

Należy przy tym zaznaczyć, że odpowiedzialność za zawartość zabezpieczonego pakietu ponosi adresat przesyłki. Personel kancelarii pod żadnym pozorem, np. kontroli okresowej, nie ma prawa ingerencji w zabezpieczony pakiet.

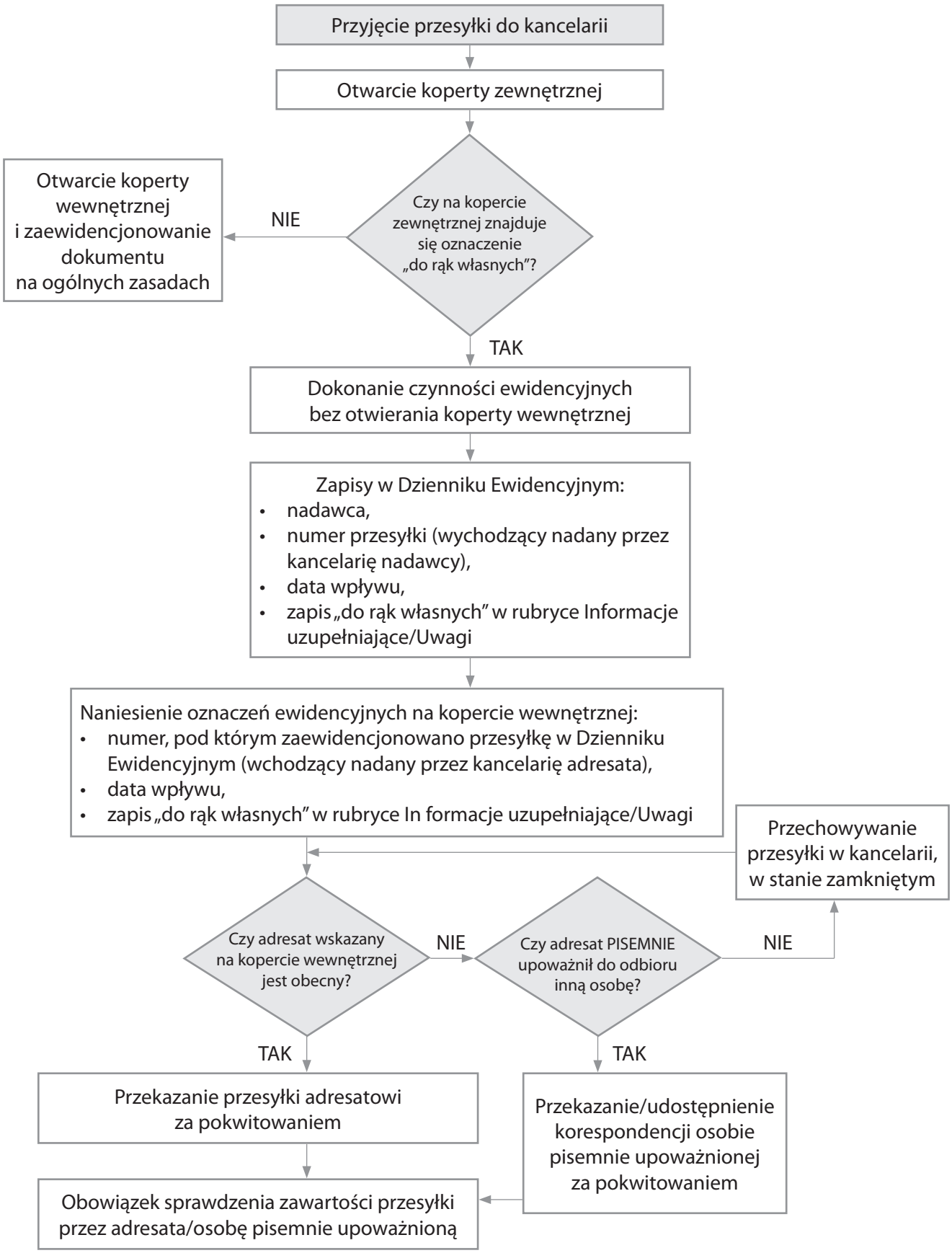
Zwrot przesyłki do kancelarii w stanie otwartym

W przypadku zwrotu przesyłki do kancelarii w stanie otwartym, kierownik kancelarii lub inny upoważniony pracownik dokonuje czynności uzupełniających w Dzienniku Ewidencyjnym samodzielnie bez współudziału adresata. Dodatkowo nanosi oznaczenia ewidencyjne bezpośrednio na dokumencie przy zachowaniu oznaczeń i zapisów pierwotnie naniesionych na opakowaniu:

1) numer, pod którym zarejestrowano przesyłkę,
2) data wpływu.

Przesyłka zdana w stanie otwartym taktowana jest już na ogólnych zasadach obowiązujących w kancelarii.

Schemat nr 1. Przyjęcie i udostępnienie przesyłki „Do rąk własnych"



Schemat nr 2. Zwrot do kancelarii przesyłki „Do rąk własnych"