Piotr Kowalik, Dariusz Wociór

Rozdział I. Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego

1. Wstęp

Każda informacja dotycząca osoby fizycznej ujawnia pewne cechy lub właściwości tej osoby. Ma ona zatem jakąś wartość, nierzadko możliwą do oszacowania. W związku z tym pozyskanie takiej informacji przez dowolny podmiot może być dla niego korzystne, a w pewnych sytuacjach korzystne także dla osoby, której ta informacja dotyczy. Z drugiej jednak strony zgromadzenie i późniejsze korzystanie z informacji o osobie fizycznej może być przez nią negatywnie odbierane, a czasem wręcz ingerować w jej prywatność. Z uwagi na powyższe obrót informacjami o osobach fizycznych został uregulowany i poddany kontroli władzy publicznej, przy jednoczesnym przyznaniu tym osobom wielu uprawnień informacyjnych i kontrolnych.

Prawna ochrona informacji o osobach fizycznych trwale wrosła w porządek prawny naszego kraju. Stanowi ona część ochrony praw i wolności obywatelskich, których ustanowienie i przestrzeganie jest jednym z podstawowych filarów funkcjonowania demokratycznego państwa prawa.

2. Ustawa o ochronie danych osobowych a rozporządzenie unijne

W polskim ustawodawstwie ochrona informacji o osobach fizycznych znajduje umocowanie w samej Konst, której art. 47 i 51 wprowadzają prawo do ochrony życia prywat-

nego oraz prawo obywateli do kontrolowania gromadzenia informacji na ich temat. Zasady obrotu tymi informacjami (danymi osobowymi) oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych, określone zostały przez przepisy OchrDanychU. Ustawa ta stanowi implementację do naszego porządku prawnego dyrektywy 95/46/WE.

W dniu 14.4.2016 r. Parlament Europejski zakończył pracę nad jednolitą i powszechnie obowiązującą europejską kodyfikacją z zakresu ochrony danych osobowych przyjmując OchrOsFizR oraz OchrOsFizD. Oba akty prawne zostały sporządzone 27.4.2016 r. i opublikowane 4.5.2016 r. w Dzienniku Urzędowym UE L 119. Skutkiem reformy będzie obowiązywanie OchrOsFizR we wszystkich państwach członkowskich. Rozporządzenie to będzie stosowane po upływie dwóch lat od jego opublikowania w Dz.Urz. UE (bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego), tj. od 25.5.2018 r. Natomiast OchrOsFizD weszło w życie pierwszego dnia po opublikowaniu w Dz.Urz. UE, czyli 5.5.2016 r. W zakresie wdrożenia OchrOsFizD będzie wymagane jednak przyjęcie ustawy na szczeblu krajowym, która będzie regulowała te zagadnienia, gdyż nie ma takich regulacji w naszym kraju.

Ważne

W OchrOsFizD ustanowiono przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Przyjęte OchrOsFizR zastąpi dotychczas obowiązującą dyrektywę 95/46/WE. Rozporządzenie to akt, który obowiązuje bezpośrednio w krajach członkowskich, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Co więcej, w polskim porządku prawnym OchrOsFizR będzie miało pierwszeństwo w stosowaniu wobec ustawodawstwa krajowego (por. art. 91 ust. 3 Konst). Nastąpi pełna harmonizacja prawa materialnego dotyczącego ochrony danych i ich przepływu w ramach UE.

W OchrOsFizR określono, m.in.:

1) nową rolę inspektora ochrony danych, obecnie zwanego ABI,
2) ułatwienia dla grup kapitałowych – przez wprowadzenie konstrukcji „współadministratorów",
3) wysokie kary pieniężne za nieprzestrzeganie przepisów OchrOsFizR,
4) zasady profilowania,
5) obowiązek prowadzenia przez inspektora ochrony danych osobowych rejestru czynności przetwarzania,
6) obowiązek uwzględnienia ochrony danych w fazie projektowania oraz wprowadzenia mechanizmów domyślnej ochrony danych,
7) szerokie uprawnienia dla osób, których dane dotyczą (m.in. prawo do bycia zapomnianym, przetwarzanie danych dzieci poniżej 16. roku życia tylko za zgodą prawnego opiekuna, przejrzyste udzielanie informacji osobie, której dane dotyczą, itd.),

8) większe obowiązki administratora danych osobowych (m.in. rozszerzenie obowiązku informacyjnego, obowiązek zgłaszania naruszeń ochrony danych osobowych, obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych).

Zagadnienia te przedstawimy w dalszych częściach publikacji. Trudno jednak formułować zarówno kategoryczne osądy co do tych regulacji, jak i dawać stanowcze wskazówki interpretacyjne. Decydujące znaczenie będzie miało orzecznictwo sądów oraz praktyka organu ochrony danych osobowych utrwalona po wejściu w życie OchrOsFizR. Trudno przewidzieć, jak do nowej regulacji podejdzie polski ustawodawca, w szczególności, czy zdecyduje się on na zmianę obecnie obowiązujących krajowych przepisów z tego zakresu.

W związku z powyższym w dalszych rozważaniach siłą rzeczy **skupimy się na krajowych przepisach o ochronie danych osobowych, które w trakcie okresu przejściowego (do momentu ropoczęcia obowiązania OchrOsFizR) muszą być bezwzględnie stosowane przez wszystkie strony procesu przetwarzania danych osobowych. Porównamy również przepisy OchrDanychU z OchrOsFizR**.

3. Dane osobowe

3.1. Zagadnienia ogólne

Rozważania dotyczące ochrony danych osobowych w jednostkach sektora publicznego należy rozpocząć od odpowiedzi na pytanie, co to są dane osobowe i dlaczego ustawodawca uznał za zasadne wprowadzenie regulacji odnoszących się do korzystania z nich.

W świetle art. 6 ust. 1 OchrDanychU za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zgodnie z art. 6 ust. 2 OchrDanychU za osobę możliwą do zidentyfikowania uznaje się osobę, której tożsamość jest możliwa do ustalenia bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny (NIP, PESEL) albo jeden czynnik lub kilka specyficznych czynników określających jej cechy:

1) fizyczne,
2) fizjologiczne,
3) umysłowe,
4) ekonomiczne,
5) kulturowe,
6) społeczne.

Informacji o danej osobie nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

W świetle definicji ustawowej za dane osobowe uznaje się zatem zarówno takie informacje, które pozwalają bezpośrednio na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, są jednakże przy pewnym nakładzie kosztów, czasu lub działań wystarczające do jej ustalenia. Definicja ta, mimo że dość spójna, może w praktyce rodzić pewne problemy interpretacyjne. Rozstrzygnięcie,

jakiego rodzaju informacje stanowią dane osobowe w konkretnej sytuacji, zależeć może od kontekstu, w jakim one występują.

Ogólne pojęcie danych osobowych nie zostało co do zasady zmienione przez OchrOsFizR.

3.2. Dane osobowe zwykłe i szczególnie chronione (wrażliwe, sensytywne)

Ustawa o ochronie danych osobowych rozróżnia dwie kategorie danych osobowych:

1) **zwykłe** – są to wszystkie dane niebędące danymi szczególnie chronionymi (wrażliwymi, sensytywnymi), takie np. jak: imię, nazwisko, adres zamieszkania, wzrost, waga, dochody czy też sytuacja majątkowa,
2) **szczególnie chronione (wrażliwe, sensytywne)** – są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym).

Katalog danych wymienionych w powyższym punkcie został określony w art. 27 ust. 1 OchrDanychU. Obrót tymi danymi co do zasady jest zabroniony i tylko w wypadkach określonych w art. 27 ust. 2 OchrDanychU możliwe jest ich przetwarzanie.

W OchrOsFizR nieco odmiennie zdefiniowano pojęcie danych szczególnie chronionych.

3.3. Dane osobowe szczególnej kategorii w ogólnym rozporządzeniu unijnym

Wprowadzono nowe pojęcie „dane osobowe szczególnej kategorii", które zastąpi używane w praktyce pojęcie „danych wrażliwych" – zwanych sensytywnymi. Zaliczamy do nich:

1) dane osobowe ujawniające pochodzenie rasowe lub etniczne,
2) poglądy polityczne,
3) przekonania religijne lub światopoglądowe,
4) przynależność do związków zawodowych,
5) dane genetyczne, dane biometryczne (w celu jednoznacznego zidentyfikowania osoby) lub dotyczące zdrowia lub seksualności i orientacji seksualnej.

W OchrOsFizR nie wprowadzono w ramach pojęcia danych osobowych szczególnej kategorii informacji dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie warunków zgodności przetwarzania danych osobowych z prawem wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem UE lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności

osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

W OchrOsFizR zdefiniowano „dane genetyczne" (dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej) oraz wprowadzono pojęcie „dane dotyczące zdrowia" (dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia).

3.4. Dane osobowe pogrupowane według rodzaju informacji

Dane osobowe możemy grupować według różnych kryteriów m.in. rodzaju informacji, jakich dotyczą. Wówczas będziemy mogli wyróżnić:

1) numery identyfikacyjne: PESEL, NIP, REGON, numer paszportu i dowodu osobistego,
2) cechy fizyczne: wygląd zewnętrzny, siatkówka oka, linie papilarne,
3) cechy fizjologiczne: grupa krwi, kod genetyczny,
4) cechy ekonomiczne: status majątkowy, zaległości finansowe,
5) cechy umysłowe, kulturowe lub społeczne: poglądy, wyznanie, pochodzenie lub przynależność związkowa.

Katalog danych osobowych jest nieograniczony. Jeżeli informacja dotyczy zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jest to już dana osobowa. Nie ma nigdzie zamkniętego katalogu danych osobowych. Opisując konkretną osobę, zamieszkałą pod określonym adresem, wymieniamy jej dane osobowe. Podobnie jeżeli nie wymieniamy imienia i nazwiska określonej osoby, ale opisujemy i identyfikujemy ją określonym przymiotem znanym pewnej grupie osób, np. wieloletni Wójt gminy x, to również wskazujemy jej dane osobowe.

4. Ogólne zasady ochrony danych osobowych

4.1. Przetwarzanie danych osobowych

Podstawowym założeniem OchrDanychU jest przyznanie każdej osobie, której dane dotyczą, prawa do ochrony dotyczących jej danych osobowych. Jest to zatem próba administracyjnego uregulowania obrotu informacjami o osobach fizycznych, przy założeniu przyznania tym osobom pewnych praw i ograniczeniu administratorów danych w swobodzie działań na danych osobowych.

Przetwarzanie danych osobowych, czyli wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych, a zwłaszcza tych, które wykonuje się w systemach informatycznych (art. 7 pkt 2 OchrDanychU), może mieć w świetle OchrDanychU

miejsce tylko ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich. Przetwarzanie danych osobowych może odbywać się jedynie w ściśle określonych przypadkach, w zakresie i trybie określonym w OchrDanychU (art. 23 i 27 OchrDanychU).

Ustawa o ochronie danych osobowych określa także zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są przetwarzane w zbiorach danych lub mogą być w nich przetwarzane. Tym samym cały zasób informacji o osobach fizycznych znajdujący się w jednostce podlega regulacjom ustawowym, bez względu na formę ich przechowywania, a tylko niejako pomocniczo OchrDanychU stanowi, że stosuje się ją do przetwarzania danych osobowych:

1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

4.2. Zbieg ustawy o ochronie danych osobowych z innymi przepisami

Informacje stanowiące dane osobowe mogą być chronione także na podstawie innych ustaw, regulujących kwestie obrotu jakimiś informacjami. Gdy ustawy te przewidują dalej idącą ich ochronę, niż wynika to z OchrDanychU, to stosuje się przepisy tych aktów prawnych. Wydaje się, że dobrym przykładem takiej szczególnej ustawy może być OchrInfU.

Podobnie jeśli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej, OchrDanychU nie jest stosowana. Pierwszeństwo ma taka umowa międzynarodowa i jej zapisy decydują, czy dany podmiot poddany jest reżimowi polskiej OchrDanychU, czy też nie.

5. Podmioty zobowiązane do stosowania ustawy o ochronie danych osobowych

Ustawę o ochronie danych osobowych – zgodnie z jej art. 3 ust. 1 i 2 OchrDanychU – stosuje się do:

1) organów państwowych,
2) organów samorządu terytorialnego,
3) państwowych i komunalnych jednostek organizacyjnych,
4) podmiotów niepublicznych realizujących zadania publiczne,
5) osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi (jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych), które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie

trzecim – jeśli przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Ważne

Ustawa o ochronie danych osobowych ma bardzo szeroki zakres podmiotowy i reguluje przetwarzanie danych osobowych zarówno w sektorze publicznym, jak i prywatnym.

5.1. Podmioty publiczne

Pierwszą grupą podmiotów zobowiązanych do stosowania OchrDanychU, którą możemy wyodrębnić na podstawie OchrDanychU, są szeroko rozumiane podmioty publiczne. Zaliczymy do nich organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne.

5.1.1. Organy państwowe

Organy państwowe to wyodrębnione prawnie pojedyncze osoby bądź zespoły ludzi upoważnione do wykonywania określonych czynności władczych w imieniu państwa. Wszystkie urzędy państwowe pełnią funkcję pomocniczą względem tych organów państwowych, a razem tworzą wyodrębnioną strukturę organizacyjną – aparat państwowy.

W zależności od przyjętego kryterium wyróżnia się następujące organy państwowe:
1) jednoosobowe (np. prezydent, minister) i kolegialne (wieloosobowe – np. Rada Ministrów) – **kryterium ilościowe**;
2) centralne, obejmujące swoim zasięgiem cały kraj (np. prezydent, parlament, ministrowie), i terenowe, tzn. działające na części obszaru państwa (np. wojewoda, kurator oświaty) – **kryterium terytorialne**;
3) wyłonione w wyborach (np. Sejm, Senat) i pochodzące z nominacji (np. wojewoda, prokurator) – **kryterium sposobu powoływania**.

Najważniejszym jednak podziałem organów państwa jest ich klasyfikacja funkcjonalna. Z tego względu organy państwa, stosownie do zasady trójpodziału władzy, dzieli się na:
1) prawodawcze (władza ustawodawcza) – upoważnione do tworzenia prawa; taką funkcję pełni głównie parlament (Sejm i Senat);
2) wykonawcze (władza wykonawcza) – mają charakter wykonawczo-zarządzający, realizują zadania wyznaczone w obowiązujących ustawach – administracja publiczna; w skali ogólnokrajowej taką funkcję pełni rada ministrów;
3) sądownicze (władza sądownicza) – zadaniem ich jest rozstrzyganie sporów prawnych na podstawie obowiązujących norm prawnych; funkcję tę pełnią sądy i trybunały.

5.1.2. Organy samorządu terytorialnego

Do organów samorządu terytorialnego (gmin, powiatów, województw) zaliczamy:
1) wójta, burmistrza (prezydenta miasta),
2) zarząd powiatu i zarząd województwa,
3) organy stanowiące tych jednostek: rady gmin, powiatu, sejmiki województwa.

W praktyce urzędów i starostw budzi wątpliwość, kto jest administratorem danych osobowych: urząd (starostwo) czy wójt (zarząd). Pamiętajmy, że administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych. Urzędy i starostwa obsługują organy zarówno stanowiące, jak i wykonawcze, a wójt, starosta i marszałek realizuje swoje zadania przez urząd lub starostwo, dlatego to właśnie osoby pełniące te funkcje powinny zostać uznane za administratora danych osobowych w jednostkach samorządu terytorialnego.

5.1.3. Państwowe i komunalne jednostki organizacyjne

Kolejną kategorią podmiotów zobligowanych do stosowania OchrDanychU są państwowe i komunalne jednostki organizacyjne. Należy tu wymienić wszelkie niewyposażone w odrębną osobowość prawną jednostki tworzone przez organy władzy państwowej czy też samorząd terytorialny. Dobrym przykładem będą tu zwłaszcza jednostki budżetowe, o których mowa w art. 11 FinPubU.

Ustawa o ochronie danych osobowych ma zatem bardzo szerokie zastosowanie do podmiotów publicznych. Musi być ona stosowana np. w Kancelarii Prezydenta RP, Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezesa Rady Ministrów, ministerstwach, sądach, prokuraturze, jednostkach policji, urzędach skarbowych, publicznych podmiotach leczniczych (dawniej zakłady opieki zdrowotnej), ZUS, gminach, powiatach, województwach itd.

5.2. Podmioty prywatne

Drugą grupą podmiotów zobligowanych do stosowania OchrDanychU są podmioty prywatne niewyposażone we władztwo publiczne.

Podmioty prywatne – zgodnie z art. 3 ust. 2 pkt 2 OchrDanychU – to:

1) podmioty niepubliczne realizujące zadania publiczne (np. prywatne podmioty lecznicze, prywatne szkoły i przedszkola),
2) osoby fizyczne i osoby prawne (np. spółki z o.o., spółki akcyjne, stowarzyszenia, fundacje, spółdzielnie) oraz jednostki organizacyjne niebędące osobami prawnymi (np. niemające osobowości prawnej spółki prawa handlowego, wspólnoty mieszkaniowe).

Podmioty wymienione w pkt 2 objęte są OchrDanychU, jeżeli przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych.

Ustawa o ochronie danych osobowych obejmuje swoim zakresem wymienione podmioty, jeśli mają siedzibę albo miejsce zamieszkania na terytorium Rzeczpospolitej Polskiej albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej (art. 3 ust. 2 pkt 2 OchrDanychU). Państwa trzecie to – zgodnie z OchrDanychU – państwa nienależące do Europejskiego Obszaru Gospodarczego.

Jak widać, wśród wymienionych podmiotów prywatnych pokaźną grupę stanowią przedsiębiorcy, którzy – co nie może budzić żadnych wątpliwości – są zobligowani do stosowania OchrDanychU.

6. Administrator danych

Każdy z wymienionych wyżej podmiotów – czy to publicznych, czy też prywatnych – jeśli bierze udział w procesie przetwarzania danych i decyduje o celach i środkach przetwarzania danych w ramach swoich zadań, staje się w świetle art. 7 pkt 4 OchrDanychU administratorem przetwarzanych w ten sposób danych osobowych. Jest to o tyle istotne, że OchrDanychU jest tak skonstruowana, że właśnie na administratora danych nakłada wiele obowiązków związanych z pozyskiwaniem i dalszym wykorzystywaniem danych osobowych. Ustawa o ochronie danych osobowych wymusza tym samym na wszystkich podmiotach biorących udział w procesie przetwarzania danych pewną refleksję i rozstrzygnięcie, kto jest gospodarzem tego procesu, przetwarzając dane realizuje swoje zadania i wykorzystuje do tego swoje środki. Podmiot ten stanie się administratorem takich danych i będzie brał za nie prawną odpowiedzialność.

Błąd pracownika, który doprowadził do udostępnienia danych osobom do tego nieupoważnionym, należy co do zasady traktować jako zaniedbanie obowiązków przez administratora danych osobowych. Chyba że ten wykaże, iż proces przetwarzania danych jest u niego prawidłowo uregulowany, sprawowany jest nadzór nad tym procesem itp. Fakt, że zaniedbania dopuścił się określony pracownik, nie zwalnia automatycznie administratora z odpowiedzialności za niewłaściwą ochronę przetwarzanych danych osobowych w jednostce.

Kwestią wtórną jest odpowiedzialność tego pracownika wobec administratora lub podmiotu działającego w jego imieniu. Może ona kształtować się w różny sposób, zależnie od regulacji wewnętrznych oraz relacji podmiot – pracownik i administrator – pracownik.

7. Obowiązki administratora danych

Na administratorze danych osobowych ciąży wiele obowiązków. Do najważniejszych z nich należą:

1) przetwarzanie danych zgodnie z prawem (na podstawie przesłanek legalizujących proces przetwarzania danych wymienionych w art. 23 ust. 1 i art. 27 ust. 2 OchrDanychU) i z poszanowaniem zasad ochrony danych osobowych,
2) obowiązek informacyjny – czyli przekazania osobom, których dane dotyczą, pewnych informacji zarówno o samym administratorze, jak i procesie przetwarzania danych wymienionych w art. 24 i 25 OchrDanychU,
3) związany z nim obowiązek respektowania praw osób, których dane dotyczą – prawa te szczegółowo opisane są w rozdziale 4 OchrDanychU,
4) obowiązek zgłoszenia zbioru danych do rejestracji GIODO, z zachowaniem zwolnień określonych w art. 43 OchrDanychU,
5) obowiązek zabezpieczenia danych – określony w art. 36–39a OchrDanychU i wydanych na jej podstawie przepisów wykonawczych.

W dalszych rozważaniach omówimy te obowiązki.

8. Wyłączenia stosowania ustawy o ochronie danych osobowych

Ustawy o ochronie danych osobowych nie stosuje się do:

1) osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych (terminarze spotkań, zbiory wizytówek, prywatne zapiski itp.);
2) podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych;
3) do prasowej działalności dziennikarskiej w rozumieniu PrPras oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą; w tym jednak wypadku zastosowanie znajdą przepisy dotyczące kontrolnych uprawnień GIODO (art. 14–19 OchrDanychU) – czyli ogólnopolskiego organu ochrony danych oraz przepisy dotyczące zabezpieczenia danych.

Niezależnie od tego ustawodawca w pewnych sytuacjach ogranicza możliwość stosowania OchrDanychU albo pewnych jej części. Będziemy odnosić się do takich przypadków w dalszych rozdziałach naszego opracowania. Jako przykład można wskazać zbiory danych sporządzone doraźnie. Ustawę o ochronie danych osobowych stosuje się jedynie w zakresie zabezpieczenia danych osobowych w stosunku do takich zbiorów danych osobowych (prowadzonych wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych), które po ich wykorzystaniu są niezwłocznie usuwane albo poddane anonimizacji.

9. Kodyfikacje europejskie

9.1. Zakres podmiotowy i przedmiotowy ogólnego rozporządzenia unijnego

Z uwagi na to, że zapisy OchrOsFizR będą stosowane dopiero od 25.5.2018 r. wyodrębniliśmy oddzielny rozdział, w którym omówiono ogólne zasady, jakie OchrOsFizR wprowadza w zakresie danych osobowych i ich przetwarzania.

W OchrOsFizR wprowadzono przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy dotyczące swobodnego przepływu danych osobowych. Regulacje wynikające z OchrOsFizR dotyczą także danych osobowych osób fizycznych prowadzących działalność gospodarczą oraz przetwarzania danych przez przedsiębiorców. Zapisy zawarte w OchrOsFizR mają zastosowanie do podmiotów publicznych z wyłączeniem przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

Zapisy zawarte w OchrOsFizR mają bardzo szeroki terytorialny zakres obowiązywania, wykraczający de facto poza obszar UE. W OchrOsFizR wskazano m.in., że przetwarzanie danych osobowych w kontekście działalności prowadzonej przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w UE powinno odbywać się zgodnie z OchrOsFizR, niezależnie od tego, czy samo przetwarzanie ma miejsce w UE. Co więcej – przetwarzanie danych osobowych osób, których dane dotyczą, znajdujących się w UE, przez administratora lub podmiot przetwarzający, który nie posiada jednostki organizacyjnej w UE, powinno podlegać OchrOsFizR, jeżeli czynności przetwarzania wiążą się z oferowaniem takim osobom towarów lub usług, niezależnie od tego, czy pociąga to za sobą płatność.

Powyższe wymusza na podmiotach spoza UE obowiązek stosowania przepisów OchrOsFizR.

Ważne

Państwa członkowskie będą mogły zachować lub wprowadzić bardziej szczegółowe regulacje, aby dostosować stosowanie przepisów OchrOsFizR do przetwarzania danych osobowych.

Ogólne rozporządzenie unijne ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Oznacza to, że reguluje ono przetwarzanie danych zarówno w systemie informatycznym, jak i poza nim. Nie ma ono zastosowania do przetwarzania danych osobowych:

1) w ramach działalności nieobjętej zakresem prawa UE,
2) przez instytucje, organy i jednostki organizacyjne UE,
3) przez państwa członkowskie w ramach wykonywania działań zewnętrznych UE i dotyczących wspólnej polityki zagranicznej i bezpieczeństwa,
4) przez osobę fizyczną w ramach działalności osobistej lub domowej.

9.2. Pojęcie osoby, której dane dotyczą w ogólnym rozporządzeniu unijnym

W OchrOsFizR w dalszym ciągu funkcjonuje pojęcie „osoby, której dane dotyczą" (mimo że na wcześniejszym etapie prac legislacyjnych planowano zastąpić je pojęciem „podmiotu danych"). Według OchrOsFizR osobą, której dane dotyczą, jest zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynni-

ków określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Treściowo pojęcie to jest analogiczne do pojęcia zastosowanego przez obecne przepisy. **Do katalogu informacji, na podstawie których można zidentyfikować daną osobę, OchrOsFizR dodało jedynie dane o lokalizacji oraz identyfikator internetowy.**

9.3. Warunki przetwarzania szczególnych kategorii danych osobowych w ogólnym rozporządzeniu unijnym

W OchrOsFizR wprowadzono następujące przesłanki przetwarzania danych szczególnej kategorii:

1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych, w jednym lub kilku konkretnych celach, chyba że prawo UE lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu;
2) przetwarzanie jest niezbędne do wypełnienia obowiązków i skorzystania ze szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem UE lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego, przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody;
4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane nie są ujawniane na zewnątrz bez zgody osób, których dane dotyczą;
5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa UE lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa UE lub prawa państwa członkowskiego, lub zgodnie z umową z pra-

cownikiem służby zdrowia i z zastrzeżeniem warunków i gwarancji, określonych w OchrOsFizR;

9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa UE lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
10) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym lub do celów badań naukowych lub historycznych, lub statystycznych i podlega warunkom i gwarancjom ustanowionym w prawie UE lub prawie państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Ważne

Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy odnośnie do danych genetycznych, biometrycznych lub danych dotyczących zdrowia.

9.4. Dane biometryczne w ogólnym rozporządzeniu unijnym

Nowością jest wyraźne włączenie danych biometrycznych do danych wrażliwych. Biometria jest dziedziną nauki zajmującą się pomiarami istot żywych w celu określenia ich indywidualnych cech. Biometrią będzie wszystko, co pozwala na identyfikowanie indywidualnych cech, wśród których są m.in. owal twarzy, rozkład punktów charakterystycznych (oczy, usta) lub temperatur na twarzy. Jest wykorzystywana głównie przy weryfikacji tożsamości, autoryzacji dostępu do systemów informatycznych czy ogólnej identyfikacji. Nowe przepisy znacznie utrudnią wdrażanie systemów opartych na biometrii.

9.5. Współadministratorzy w kodyfikacji europejskiej

Obecne polskie przepisy w zakresie ochrony danych osobowych nie definiują konstrukcji współadministratorów danych. Na chwilę obecną podmioty te mają te same prawa i obowiązki, co de facto oznacza, że każdy z nich jest osobnym administratorem danych. Nowe przepisy pozwolą współadministratorom podzielić się prawami i obowiązkami (o czym osoba, której dane dotyczą, będzie musiała zostać poinformowana). Nadto grupa podmiotów publicznych będzie mogła wyznaczyć jednego inspektora ochrony danych, „o ile można będzie łatwo nawiązać z nim kontakt z każdej siedziby".

W OchOsFizR wskazano, że jeżeli dwaj administratorzy lub większa ich liczba wspólnie ustalają cele i sposoby przetwarzania danych osobowych, to są oni współadministratorami. W drodze wspólnych uzgodnień w przejrzysty sposób określają oni podział zadań w zakresie wypełniania obowiązków wynikających z OchrOsFizR, w szczególności odnośnie korzystania przez osobę, której dane dotyczą, z przysługujących jej praw oraz po-

dział obowiązków w zakresie podawania informacji. W uzgodnieniach należy wskazać, który ze współadministratorów pełni funkcję pojedynczego punktu kontaktowego wobec osób, których dane dotyczą, chcących skorzystać ze swoich praw. Osoba, której dane dotyczą, może korzystać z przysługujących jej praw wynikających z OchrOsFizR wobec każdego z administratorów i przeciwko każdemu z nich. Nie ma to zastosowania, jeżeli osoba, której dane dotyczą, została w przejrzysty i jednoznaczny sposób poinformowana, który ze współadministratorów ponosi odpowiedzialność, chyba że takie uzgodnienie – inne niż określone prawem UE lub prawem państwa członkowskiego – jest niesprawiedliwe względem jej praw. W uzgodnieniach należycie odzwierciedla się faktyczną rolę każdego ze współadministratorów i jego relacje z osobami, których dane dotyczą, a zasadnicza treść uzgodnień jest udostępniana osobie, której dane dotyczą.

Ważne

Nowa instytucja współadministratorów będzie miała zastosowanie do podmiotów publicznych, które wspólnie ustalają cele i sposoby przetwarzania. Instytucja ta będzie ułatwieniem z uwagi na podział obowiązków w zakresie ochrony danych osobowych.

9.6. Przedstawiciele administratorów niemających siedziby w UE w kodyfikacji europejskiej

Administrator na piśmie wyznacza swojego przedstawiciela w UE, jeżeli nie ma miejsca zamieszkania lub siedziby w UE oraz jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom, których dane dotyczą – niezależnie od tego, czy wymaga się od tych osób, których dane dotyczą, płatności lub monitorowania ich zachowania, o ile do zachowania tego dochodzi w UE. Obowiązek ten nie ma zastosowania w przypadku przetwarzania, które ma charakter sporadyczny i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele niosło zagrożenie dla praw i wolności osób fizycznych lub przetwarzania organu lub podmiotu publicznego.

Przedstawiciel ma siedzibę w jednym z państw członkowskich będących miejscem zamieszkania osób, których dane dotyczą, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane. Przedstawiciel zostaje upoważniony przez administratora, by do celów zapewnienia przestrzegania OchrOsFizR mogły się do niego zwracać – oprócz lub zamiast do administratora – w szczególności organy nadzorcze i osoby, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem danych osobowych. Wyznaczenie przedstawiciela przez administratora pozostaje bez uszczerbku dla postępowań sądowych, które mogą zostać wszczęte przeciwko administratorowi.

Podstawa prawna:

- art. 8 § 1 KC,
- art. 47, 51, 91 ust. 3 Konst,
- art. 11 FinPubU,
- art. 3 ust. 1 i 2, art. 6, 7, 14–19, 23, 25, 27, 36–39a, 43 OchrDanychU,
- OchrOsFizR,
- OchrOsFizD.