Dariusz Wociór

Rozdział III. Dane osobowe szczególnej kategorii

W OchrOsFizR wprowadzono nowe pojęcie „dane osobowe szczególnej kategorii", które zastąpi 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.

Dane biometryczne

Nowością jest włączenie danych biometrycznych do danych wrażliwych. Biometria jest dziedziną nauki zajmującą się pomiarami istot żywych w celu określenia ich indywidualnych cech. Biometria bada 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.

Warunki przetwarzania szczególnych kategorii danych osobowych

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 pracownikiem 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 jako-

ści 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.

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

Prawa osoby, której dane dotyczą, a obowiązki administratora danych

W OchrOsFizR uszczegółowiono również regulacje dotyczące przejrzystości oraz trybu korzystania z praw osoby, której dane dotyczą. Jest to kolejne wyjście naprzeciw osobie, której dane dotyczą. Nowe przepisy podkreślają, iż udzielane informacje mają być zakomunikowane osobie, której dane dotyczą, w jak najprostszej formie. Natomiast już w samej preambule wskazano, iż zastosowane w OchrOsFizR instytucje mają na celu zapewnienie zwiększenia przejrzystości i przestrzegania jego postanowień.

W OchrOsFizR wskazano, że przedsiębiorca będący administratorem danych podejmuje odpowiednie środki, aby w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, dotyczących przetwarzania danych oraz prowadzić z nim wszelką komunikację w sprawie przetwarzania danych osobowych. Informacji udziela się na piśmie lub innymi sposobami, a w stosownym przypadku – elektronicznie. Jeżeli osoba, której dane dotyczą, składa wniosek w formie elektronicznej, informacje można zasadniczo przekazywać w formie elektronicznej, chyba że osoba, której dane dotyczą, zażąda innej formy. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile potwierdzi się tożsamość osoby, której dane dotyczą. Nowe przepisy wskazują, iż zadaniem administratora jest ułatwianie osobie, której dane dotyczą, korzystania z praw przysługujących jej na mocy OchrOsFizR, mają być one stosowane w sposób jak najbardziej zrozumiały dla osoby fizycznej.

Informacje podawane w przypadku zbierania danych

Nowe przepisy modyfikują obowiązek informacyjny ciążący na administratorze danych.

Administrator bez zbędnej zwłoki – najpóźniej w terminie jednego miesiąca od otrzymania wniosku – udziela osobie, której dane dotyczą, informacji o działaniach dotyczących przetwarzania jej danych. W razie potrzeby termin ten można przedłużyć o kolejne dwa

miesiące z uwagi na skomplikowany charakter wniosku oraz liczbę wniosków. Nowością jest możliwość przedłużenia terminu. Jeżeli zastosowanie ma termin przedłużony, w terminie jednego miesiąca od otrzymania wniosku informuje się osobę, której dane dotyczą, o przyczynach opóźnienia. Jeżeli administrator nie podejmuje działań względem wniosku osoby, której dane dotyczą, to bez zbędnej zwłoki – najpóźniej w terminie jednego miesiąca od otrzymania wniosku – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego.

Informacje te oraz wszelka komunikacja są wolne od opłat. Jeżeli wnioski osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, zwłaszcza ze względu na swój ustawiczny charakter, administrator może odmówić podjęcia działań względem wniosku. W takim przypadku obowiązek wykazania, że wniosek ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby składającej wniosek, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Jeżeli dane osobowe o osobie, której dane dotyczą, są zbierane bezpośrednio od osoby, której dane dotyczą, administrator podczas pozyskiwania danych osobowych podaje osobie, której dane dotyczą, w szczególności następujące informacje:

1) swoją tożsamość i dane kontaktowe oraz tożsamość i dane kontaktowe swojego przedstawiciela, jeżeli istnieje,
2) dane kontaktowe inspektora ochrony danych, jeżeli istnieje,
3) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania,
4) prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f (jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem),
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
6) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych – gdy ma to zastosowanie.

Administrator podczas pozyskiwania danych osobowych podaje osobie, której dane dotyczą, inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania i uwzględnia przy tym konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych.

Jeżeli administrator planuje przetwarzać dane w celu innym niż cel, w którym dane zostały zebrane, informuje on przed takim dalszym przetwarzaniem osobę, której dane do-

tyczą, o tym innym celu oraz dostarcza mu wszelkich innych stosownych informacji. Takim innym celem będzie prowadzenie marketingu.

Obowiązek informacyjny podczas zbierania danych, w stosunku do obecnie obowiązujących przepisów, zostanie poszerzony o następujące dane:
1) informacja o inspektorze ochrony danych,
2) termin usunięcia danych lub jakie są zasady ustalania tych terminów,
3) o profilowaniu.

Omawiana zmiana będzie bez wątpienia kosztowna dla przedsiębiorców, bo wymagać będzie wymiany wszelkich formularzy, zarówno papierowych, jak i elektronicznych.

Osoba, której dane dotyczą, będzie miała prawo w sposób wolny od opłat, w racjonalnych odstępach czasu, uzyskiwać od administratora potwierdzenie, czy przetwarzane są dane osobowe go dotyczące, a jeżeli takie dane są przetwarzane, dostęp do nich i następujące informacje:
1) cele przetwarzania,
2) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
3) w miarę możliwości – planowany okres przechowywania danych osobowych,
4) informacje o prawie do tego, by zwrócić się do administratora o poprawienie, usunięcie, lub ograniczenie przetwarzania danych osobowych dotyczących osoby, której dane dotyczą, lub by wnieść sprzeciw wobec przetwarzania takich danych osobowych,
5) informacje o prawie wniesienia skargi do organu nadzorczego,
6) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
7) informacje w przypadku decyzji opartych na automatycznym przetwarzaniu, w tym na profilowaniu, o trybie jego działania oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania.

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich gwarancjach.

Prawo dostępu przysługujące osobie, której dane dotyczą

Na wniosek i bez nadmiernych opłat – zgodnie z OchrOsFizR – administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Prawo do uzyskania tej kopii nie ma zastosowania, jeżeli nie można jej dostarczyć bez ujawnienia danych osobowych innych osób, których dane dotyczą, lub poufnych danych administratora. Ponadto prawo to nie ma zastosowania, jeżeli ujawnienie danych osobowych naruszyłoby prawa własności intelektualnej związane z przetwarzaniem tych danych. Są to nowe obowiązki, które mogą być bardzo uciążliwe dla przedsiębiorców.

Już na etapie gromadzenia danych przedsiębiorca powinien zastosować system, który umożliwi w przyszłości wygenerowanie kopii danych osobowych dotyczących konkretnej osoby. W późniejszym etapie może się bowiem okazać, iż bez zastosowania specjalnych procedur lub systemu przedsiębiorca może mieć problem z wygenerowaniem przedmiotowej kopii.

Prawo do poprawienia danych

Prawo do poprawiania danych zostało wprowadzone do OchrOsFizR praktycznie w niezmienionej formie. Osoba, której dane dotyczą, ma prawo spowodować, by administrator bez zbędnej zwłoki poprawił dane osobowe jej dotyczące, jeżeli są one nieścisłe. Z uwzględnieniem celów, w których przetworzono dane, osoba, której dane dotyczą, ma prawo spowodować, by niekompletne dane osobowe zostały uzupełnione, w tym poprzez przedstawienie dodatkowego oświadczenia.

Prawo do bycia zapomnianym

Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe – zwłaszcza dane osobowe zebrane, gdy osoba, której dane dotyczą, była dzieckiem – a osoba, której dane dotyczą, ma prawo spowodować, by administrator – bez zbędnej zwłoki – usunął dane osobowe go dotyczące, jeżeli zachodzi jedna z następujących okoliczności:

1) dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetworzone,
2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej do przetwarzania danych,
3) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania danych osobowych i nie istnieją żadne nadrzędne uzasadnione podstawy do przetwarzania,
4) dane zostały przetworzone niezgodnie z prawem,
5) dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator,
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w OchrOsFizR.

Jeżeli administrator upublicznił dane osobowe, a ma obowiązek te dane usunąć, to – biorąc pod uwagę dostępną technologię i koszt realizacji – przedsiębierze racjonalne kroki, w tym środki techniczne, by poinformować administratorów przetwarzających te dane, że osoba, której dane dotyczą, wystąpiła o to, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych.

Choć prawo do bycia zapomnianym pozwala na ochronę danych obywateli, to może być trudne lub niemożliwe do wyegzekwowania w realizacji. Usunięcie danych osobowych upublicznionych może być technicznie skomplikowane i kosztowne.

Prawo do usunięcia danych zostaje wyłączone w zakresie, w jakim przetwarzanie danych osobowych jest niezbędne:

1) do skorzystania z prawa wolności wypowiedzi i informacji,
2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania danych osobowych na mocy prawa UE lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej mu powierzonej,
3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
4) do celów archiwalnych w interesie publicznym lub do celów naukowych, statystycznych i historycznych,
5) do ustalenia, realizacji lub obrony roszczeń prawnych.

Nie wiadomo, jak w praktyce będzie wyglądała realizacja tych praw – będziemy czekać na pierwsze decyzje, wytyczne i interpretacje w tym zakresie. Na pewno przepis będzie problematyczny dla podmiotów świadczących usługi społeczeństwa informacyjnego, takie jak np. Facebook, Google itp.

Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, ma prawo spowodować, by administrator ograniczył przetwarzanie danych osobowych, jeżeli:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń prawnych,
3) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli przetwarzanie danych osobowych zostało ograniczone, dane takie można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, realizacji lub obrony roszczeń prawnych lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub ze względu na ważne przesłanki interesu publicznego. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

Obowiązek powiadomienia o sprostowaniu danych, ich usunięciu lub ograniczeniu przetwarzania

W OchrOsFizR nałożono na administratora obowiązek komunikowania poprawienia, usunięcia lub ograniczenia przetwarzania danych, których dokonał, każdemu odbiorcy, któremu ujawniono dane, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Zwroty te są niedookreślone, stąd nie wiadomo, jak będą stosowane w praktyce, co zostanie uznane za wymagające niewspółmiernie dużego wysiłku, a co w opinii organu nadzorczego nim nie będzie.

Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym i maszynowo czytelnym formacie dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane innemu administratorowi bez przeszkód ze strony administratora, któremu danych tych dostarczono, jeżeli:

1) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy,
2) przetwarzanie odbywa się w sposób zautomatyzowany.

Ogólnie przenosić można te dane, które przetwarzane są w pełni automatycznie i wyłącznie na podstawie zgody osoby, której dane dotyczą. Nie do końca jest jasne, co należy rozumieć przez w pełni automatyczne przetwarzanie. Zmiana ta jest niekorzystna dla przedsiębiorców, będą oni musieli zmodyfikować systemy, aby potrafiły wygenerować dane do przeniesienia.

Prawo do sprzeciwu

Treść prawa do sprzeciwu znana jest obecnym przepisom ochrony danych osobowych, prawo to ma poszerzyć się o sprzeciw wobec profilowania.

Zgodnie z OchrOsFizR osoba, której dane dotyczą, ma więc prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych, podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub do ustalenia, realizacji lub obrony roszczeń.

Prawo do sprzeciwu a dane osobowe przetwarzane do celów marketingu, historycznych, statystycznych lub naukowych

Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych do tych celów, w tym profilowania. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, należy wyraźnie poinformować ją o tym prawie. Informacja ta powinna być zakomunikowana wyraźnie – w sposób odrębny od innych informacji. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać w tym celu. Jeżeli dane osobowe są przetwarzane do celów historycznych, statystycznych lub naukowych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej indywidualną sytuacją – wobec przetwarzania danych osobowych jej dotyczących, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Nowe obowiązki administratora

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki i jest w stanie wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z OchrOsFizR.

Administratorzy wdrażają środki techniczne i organizacyjne odpowiednie do wykonywanej czynności przetwarzania i do jej celów, np. minimalizację i pseudonimizację danych, w taki sposób by przetwarzanie było zgodne z wymogami.

Administrator wdraża odpowiednie środki, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne w stosunku do każdego konkretnego celu przetwarzania. Dotyczy to ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Jeżeli celem przetwarzania nie jest podanie informacji do wiadomości publicznej, mechanizmy te mają gwarantować, że domyślnie dane osobowe nie będą udostępniane nieokreślonej liczbie osób bez ludzkiej interwencji.

Wywiązywanie się z tych obowiązków można wykazać między innymi poprzez zatwierdzony mechanizm certyfikacji. W OchrOsFizR nie ma jednak wskazania konkretnie, jak należy rozumieć „odpowiednie środki techniczne i organizacyjne". Brak jest uregulowań co do środków bezpieczeństwa, jakie należy przedsięwziąć w zależności od rodzaju i sposobu przetwarzanych danych osobowych, w tym – jak powinny być zabezpieczone systemy informatyczne.

Strategie ochrony danych *privacy by design* i *privacy by default*

W preambule do OchrOsFizR czytamy, że „administrator danych powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych".

Pierwsza z wyżej wymienionych koncepcji zakłada, iż już podczas projektowania systemu ochrony danych osobowych należy wdrażać takie środki, by od samego początku chronić przetwarzane dane oraz prywatność osób, których dane dotyczą.

Druga koncepcja traktuje prywatność jako ustawienie domyślne – ustawienia domyślne danego systemu powinny przewidywać możliwie najdalej posunięte zabezpieczenia danych osobowych. Ustawienia aplikacji czy serwisów społecznościowych domyślnie powinny udostępniać minimalną ilość informacji o użytkowniku. Poszerzenie zakresu udostępnianych danych może nastąpić jedynie na podstawie zmiany ustawień dokonanych przez samego użytkownika. Wcześniej takie zagadnienia nie były uregulowane w polskim prawie.

Kodeksy postępowania i mechanizmy certyfikacji

Jest to kolejna nowość w sferze ochrony danych osobowych. Posiadanie zatwierdzonych kodeksów postępowania bądź certyfikatów, o których mowa w OchrOsFizR, ma ułatwiać przedsiębiorcom m.in. wdrożenie zasad ochrony danych osobowych. Mechanizm ten również może oddziaływać na klientów, którzy będą bardziej preferować certyfikowane podmioty – jako bardziej godne zaufania.

Wywiązywanie się z obowiązków administratora można wykazać między innymi przez stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonego mechanizmu certyfikacji.

Mając na uwadze dostępną technologię i koszt wdrażania oraz uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i powagę zagrożenia dla praw i wolności osób fizycznych – administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, np. pseudonimizację danych osobowych, aby zapewnić poziom bezpieczeństwa odpowiadający temu zagrożeniu.

Przy ocenie poziomu bezpieczeństwa uwzględnia się przede wszystkim zagrożenia, które niesie przetwarzanie danych, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przenoszonych, przechowywanych lub w inny sposób przetwarzanych.

Administrator oraz podmiot przetwarzający podejmują działania, by zagwarantować, że każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, będzie je przetwarzać wyłącznie na polecenie

administratora, chyba że wymaga tego od niej prawo UE lub prawo państwa członkowskiego.

Kodeksy postępowania a przedsiębiorcy

Zgodnie z OchrOsFizR państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych (EROD) oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu OchrOsFizR – z uwzględnieniem szczególnych cech różnych sektorów przetwarzających dane oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Stowarzyszenia i inne organy reprezentujące administratorów lub podmioty przetwarzające różnych kategorii mogą przygotowywać, zmieniać lub poszerzać kodeksy postępowania, aby doprecyzować zastosowanie przepisów OchrOsFizR, np. co do:

1) rzetelnego i przejrzystego przetwarzania danych,
2) prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach,
3) zbierania danych,
4) pseudonimizacji danych osobowych,
5) informowania opinii publicznej i osób, których dane dotyczą,
6) wykonywania przez osoby, których dane dotyczą przysługujących im praw,
7) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody rodzica i opiekuna,
8) środków i procedur, o których mowa w art. 24 i 25 OchrOsFizR, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32 OchrOsFizR,
9) zgłaszania organowi nadzorczemu naruszenia ochrony danych osobowych oraz zawiadamiania o nim osób, których dane dotyczą,
10) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych,
11) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79 OchrOsFizR.

Kodeks postępowania przewiduje mechanizmy pozwalające prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu przez administratorów lub podmioty przetwarzające, którzy podjęli się jego stosowania, bez uszczerbku dla zadań i uprawnień organu nadzorczego, którym w Polsce jest GIODO.

Stowarzyszenia i inne organy reprezentujące administratorów lub podmioty przetwarzające różnych kategorii przygotują kodeks postępowania lub zmienią, lub poszerzą kodeks już obowiązujący, a następnie przedłożą jego projekt organowi nadzorczemu. Organ nadzorczy wyda opinię o zgodności projektu, zmienionego kodeksu lub poszerzonego kodeksu z OchrOsFizR i zatwierdzi taki projekt, zmieniony kodeks lub poszerzony kodeks, jeżeli uzna, że stanowią one wystarczające gwarancje.

Jeżeli opinia ta potwierdza, że kodeks postępowania, zmieniony kodeks postępowania lub poszerzony kodeks postępowania są zgodne z OchrOsFizR i jeżeli kodeks ten zostanie zatwierdzony i nie dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, organ nadzorczy zarejestruje ten kodeks i opublikuje szczegółowe informacje o nim. Jeżeli projekt kodeksu postępowania dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, właściwy organ nadzorczy – przed zatwierdzeniem – przedkłada go EROD-owi, który wydaje opinię o zgodności projektu, zmienionego kodeksu lub poszerzonego kodeksu z OchrOsFizR i wskazuje, czy kodeks postępowania zawiera odpowiednie gwarancje.

Jeżeli opinia ta potwierdza, że kodeks postępowania, zmieniony kodeks postępowania lub poszerzony kodeks postępowania są zgodne z OchrOsFizR, stanowią odpowiednie gwarancje – EROD przedkłada tę opinię Komisji.

Komisja może przyjmować akty wykonawcze w celu stwierdzenia, że zatwierdzone kodeksy postępowania oraz zmiany lub poszerzenia już obowiązujących zatwierdzonych kodeksów jej przedłożone mają ogólną moc obowiązującą w UE. Komisja zapewnia odpowiednie propagowanie zatwierdzonych kodeksów, których ogólną moc obowiązującą stwierdziła. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie zatwierdzone kodeksy podstępowania i zmiany do nich i udostępnia je opinii publicznej za pomocą odpowiednich środków, np. za pomocą europejskiego portalu e-Sprawiedliwość (http://e-justice.europa.eu).

Monitorowanie zatwierdzonych kodeksów postępowania

Bez uszczerbku dla zadań i uprawnień GIODO monitorowaniem przestrzegania kodeksu postępowania może się zajmować podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez właściwy organ nadzorczy. Podmiot ten może zostać akredytowany w tym celu, jeżeli:

1) w sposób satysfakcjonujący wykazał GIODO swoją niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu,
2) dysponuje procedurami pozwalającymi mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo weryfikować jego funkcjonowanie,
3) dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwalają zapewnić przejrzystość tych procedur i struktur wobec osób, których dane dotyczą, i opinii publicznej,
4) w sposób satysfakcjonujący wykaże właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.

Generalny Inspektor Ochrony Danych Osobowych przedkłada proponowane kryteria akredytacji podmiotu EROD-owi. Podmiot może podjąć odpowiednie działania w przy-

padku naruszenia kodeksu przez administratora lub podmiot przetwarzający, w tym zawiesić lub wykluczyć administratora lub podmiot przetwarzający spośród stosujących kodeks. O działaniach tych i powodach ich podjęcia informuje on GIODO, który cofa akredytację podmiotu, jeżeli nie spełnia on lub przestał spełniać warunki akredytacji lub jeżeli działania przez niego podejmowane nie są zgodne z OchrOsFizR.

Certyfikacja

Zgodnie z OchrOsFizR państwa członkowskie, EROD oraz Komisja zachęcają – w szczególności na szczeblu UE – do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych osobowych oraz pieczęci i oznaczeń mających świadczyć o zgodności z OchrOsFizR operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Mechanizmy certyfikacji oraz pieczęcie i oznaczenia w dziedzinie ochrony danych, zatwierdzone i przestrzegane przez administratorów lub podmioty przetwarzające, którzy podlegają OchrOsFizR, mogą być ustanowione także do wykazania odpowiednich gwarancji przez administratorów lub podmioty przetwarzające, którzy nie podlegają OchrOsFizR, w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązanie – za pomocą instrumentów umownych lub w inny sposób – do stosowania tych odpowiednich gwarancji, w tym w odniesieniu do praw osób, których dane dotyczą.

Certyfikacja nie ogranicza spoczywającego na administratorze lub podmiocie przetwarzającym obowiązku przestrzegania OchrOsFizR i pozostaje bez uszczerbku dla zadań i uprawnień GIODO.

Administrator lub podmiot przetwarzający poddający swoje przetwarzanie mechanizmowi certyfikacji udzielają podmiotowi certyfikującemu – lub w stosownym przypadku właściwemu organowi nadzorczemu – wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania, które są niezbędne do przeprowadzenia procedury certyfikacji. Udziela się jej administratorowi lub podmiotowi przetwarzającemu maksymalnie na okres trzech lat. Certyfikację można przedłużyć na tych samych warunkach, o ile nadal spełnione są stosowne wymogi. Organy certyfikujące mogą cofnąć certyfikację, jeżeli jej wymogi nie są spełnione lub przestały być spełniane. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie mechanizmy certyfikacji i pieczęcie w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków, np. europejskiego portalu e-Sprawiedliwość (http://e-justice.europa.eu).

Zadania podmiotu certyfikującego

Podmiot certyfikujący dysponujący odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych dokonuje certyfikacji i jej przedłużenia. Czyni to bez uszczerbku dla

zadań i uprawnień GIODO. Każde państwo członkowskie określa, czy te podmioty certyfikujące są akredytowane przez:
1) właściwy organ nadzorczy, którym w Polsce jest GIODO,
2) krajową jednostkę akredytującą.

Podmiot certyfikujący może zostać akredytowany w tym celu wyłącznie wtedy, gdy:
1) w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie podlegającej certyfikacji,
2) podjął się respektowania kryteriów certyfikacji zatwierdzonych przez GIODO lub przez EROD,
3) dysponuje procedurami wydawania, okresowego weryfikowania i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych,
4) dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający oraz które zapewniają przejrzystość tych procedur i struktur wobec osób, których dane dotyczą, i opinii publicznej,
5) w sposób satysfakcjonujący wykaże właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.

Podmiot certyfikujący ma obowiązek przed udzieleniem lub cofnięciem certyfikacji dokonać właściwej oceny, bez uszczerbku dla spoczywającego na administratorze lub podmiocie przetwarzającym obowiązku przestrzegania OchrOsFizR. Akredytacji udziela się maksymalnie na okres pięciu lat, można ją przedłużyć na tych samych warunkach, o ile podmiot spełnia wymogi. Podmiot certyfikujący przedstawia GIODO powody udzielenia lub cofnięcia żądanej certyfikacji.

Organ nadzorczy w łatwo dostępny sposób podaje wymogi certyfikacji do wiadomości publicznej oraz przekazuje je EROD-owi, który gromadzi w rejestrze wszystkie mechanizmy certyfikacji i pieczęcie w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków, np. za pomocą europejskiego portalu e-Sprawiedliwość.

GIODO lub krajowa jednostka akredytująca cofają akredytację udzieloną przez siebie podmiotowi certyfikującemu, jeżeli podmiot ten nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania przez niego podejmowane nie są zgodne z OchrOsFizR.

Komisja jest uprawniona do przyjmowania aktów w celu doprecyzowania kryteriów i wymogów, które należy uwzględnić w przypadku mechanizmów certyfikacji w dziedzinie ochrony danych. Kryteria i wymogi opiniuje EROD, a następnie przekazuje je Komisji.

Komisja może ustanowić techniczne standardy mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposoby propagowania i uznawania mechanizmów certyfikacji oraz pieczęci i oznaczeń w dziedzinie ochrony danych.