RODO

co się zmieniło w ochronie danych dla sektora publicznego

experto24.pl

Spis treści

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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) z 27 kwietnia 2016 r. (Dz.Urz.UE.L nr 119, str. 1; dalej: RODO) jest stosowane od 25 maja 2018 r.

WAŻNE

RODO znajduje bezpośrednie zastosowanie we wszystkich państwach członkowskich Unii Europejskiej i ma pierwszeństwo wobec ustawodawstwa krajowego.

W polskim porządku prawnym wprowadzane przez RODO zasady ochrony danych osobowych doprecyzowuje nowa ustawa o ochronie danych osobowych z 10 maja 2018 r., która obowiązuje już od 25 maja 2018 r.

Nowe przepisy przewidują m.in. wysokie kary pieniężne za nieprzestrzeganie przepisów RODO, większe obowiązki administratora danych osobowych, szerokie uprawnienia dla osób, których dane dotyczą, a także nową rolę inspektora ochrony danych (następca dotychczasowego administratora bezpieczeństwa informacji – ABI). Wszystkie te zagadnienia znajdują pełne zastosowanie do instytucji administracji publicznej, wszystkie one na co dzień administrują i przetwarzają bowiem rozmaite dane osobowe.

W tym i kolejnych artykułach (które zostaną opublikowane w kolejnych wydaniach) na temat zmian w ochronie danych osobowych w administracji publicznej omawiamy kluczowe zmiany, jakie wprowadza RODO, a także ich skutki dla sektora publicznego. Podpowiadamy też, jak dostosować się do nowych przepisów. Należy jednak podkreślić, że nie we wszystkich obszarach regulowanych przez RODO można na ten moment sformułować jednoznaczne wskazówki interpretacyjne dla podmiotów administracji publicznej. Decydujące znaczenie będzie tu miało orzecznictwo sądów oraz praktyka organu ochrony danych osobowych utrwalona po wejściu w życie nowych przepisów.

Pamiętaj o przejrzystym języku

Ważna preambuła

Tekst RODO jest napisany bardzo przystępnym językiem. W preambule, stanowiącej wstęp do rozporządzenia, zostały wyjaśnione ogólne założenia i powody zmiany przepisów, a także przedstawiona częściowa ich interpretacja. Preambuła RODO składa się z 173 motywów i stanowi swego rodzaju „wprowadzenie" do tego aktu prawnego. Jej znajomość pozwala zrozumieć sens i cel stosowania wielu wymagań, dlatego też nie powinno czytać się rozporządzenia, nie zapoznawszy się wcześniej z tekstem preambuły. Po preambule znajduje się właściwa treść RODO podzielona na 11 rozdziałów.

Przekazywanie informacji

Również same zapisy RODO wymagają od administratora danych, aby osobom, których dane przetwarza, przedstawiał informacje (zapytanie o zgodę, informowanie o prawach, zawiadomienie o naruszeniu bezpieczeństwa informacji) „jasnym i prostym" językiem.

WAŻNE

Administrator danych ma obowiązek przekazywać informacje osobom, których dane przetwarza, jasnym i prostym językiem.

Pracownicy administracji publicznej, którzy do tej pory używali bardzo formalnego, a niekiedy nawet prawniczego języka, będą musieli zastanowić się, jak przekazywać informacje. Dotyczy to w szczególności urzędów, w których stosowany język jest bardzo „formalny".

Właściwa interpretacja

Mimo że zarówno samo rozporządzenie, jak i jego polskie tłumaczenie zostało napisane przystępnym językiem, dokładna interpretacja jego zapisów i umiejętność ich zastosowania w praktyce wciąż mogą nastręczać pewnych problemów. Wynika to z tego, że są to nowe przepisy i nie ma jeszcze doświadczenia w ich stosowaniu.

Co więcej, w najbliższym czasie pojawi się dużo zmian w przepisach krajowych. Z uwagi na to warto rozważyć zatrudnienie przez jednostkę specjalisty (najlepiej z wykształceniem prawniczym i doświadczeniem w zakresie ochrony danych osobowych), który pomoże administratorowi danych właściwie zinterpretować przepisy i określić kierunki działania.

Jakie kompetencje ma nowy organ nadzorczy

Nowa nazwa

Nowa ustawa o ochronie danych osobowych z 10 maja 2018 r. sprawiła, że dotychczasowy – Generalny Inspektor Ochrony Danych Osobowych (GIODO) – zyskał nową nazwę – Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

WAŻNE

Dotychczasowy Generalny Inspektor Ochrony Danych Osobowych (GIODO) zmienił nazwę na Prezesa Urzędu Ochrony Danych Osobowych (Prezes UODO).

Zmiana ta wynika z tego, że RODO w miejsce dotychczasowego ABI wprowadza inspektora ochrony danych i mogło to prowadzić do niejasności, jaka jest relacja między „zwykłym" inspektorem a inspektorem „generalnym". Ponadto zaproponowano, aby dawnych inspektorów GIODO nazwać „kontrolującymi", aby nie mylono ich z inspektorami ochrony danych, o których mowa w RODO.

Odpowiednie zasoby dla organów nadzorczych

RODO przewiduje, że krajowe organy nadzorcze, których odpowiednikiem w Polsce jest obecnie Prezes UODO muszą być wyposażone w odpowiednie zasoby techniczne, kadrowe i finansowe. Nie ma zatem wątpliwości, że Urząd Ochrony Danych Osobowych musi być znacząco rozbudowany w porównaniu do Biura GIODO. Prezes UODO ma być organem, z którego decyzjami przedsiębiorcy i administracja publiczna będą musieli się liczyć. Zyskał „powagę" i nazwę podobną do UOKiK.

Uprawnienia Urzędu Ochrony Danych Osobowych nie różnią się znacząco od dotychczasowych, choć pojawiły się pewne nowe obowiązki, które nie występowały w dotychczasowych przepisach, np. Prezes Urzędu Ochrony Danych Osobowych ma udzielać zaleceń dotyczących szczególnych operacji przetwarzania (art. 57 ust. 1 RODO). Nowe przepisy dotyczące organów nadzorczych mówią o m.in. prowadzeniu rejestru naruszeń, obowiązku wzajemnej pomocy i współpracy z innymi organami nadzorczymi.

Motyw 127 RODO stanowi, że każde państwo członkowskie musi zapewnić organowi nadzorującemu ochronę danych osobowych warunki i możliwości operowania odpowiednimi zasobami ludzkimi.

WAŻNE

Każdy organ nadzorczy zostanie wyposażony w zasoby finansowe i kadrowe, pomieszczenia i infrastrukturę, niezbędne do skutecznego wykonywania zadań, w tym zadań związanych z wzajemną pomocą i współpracą z innymi organami nadzorczymi z całej Unii Europejskiej.

Ponadto każdy organ nadzorczy powinien dysponować odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu krajowego lub państwowego. Takie szczególne wymogi dotyczące warunków pracy UODO przewiduje też art. 52 ust. 4, 5 i 6 RODO.

Skarga do UODO

Ogólne rozporządzenie o ochronie danych przewiduje, że skargę do Prezesa UODO można złożyć bezpłatnie, a odbiorcą takiej skargi może zostać dowolny organ nadzorczy w UE.

WAŻNE

Za złożenie skargi do UODO nie trzeba płacić.

Jeśli skarga zostanie złożona do innego organu nadzorczego w UE, Prezes UODO będzie, upraszczając, brał udział w sprawie jako tzw. organ nadzorczy, którego sprawa dotyczy. Będzie też można skarżyć się bezpośrednio do sądu, z pominięciem organu nadzorczego (art. 79 RODO). Dotychczas ograniczone zasoby kadrowe GIODO sprawiały, że skargi rozpatrywane były bardzo wolno – to z pewnością się zmieni.

Z kolei art. 70 nowej ustawy o ochronie danych osobowych umożliwia Prezesowi UODO tymczasowe zobowiązanie administratora do ograniczenia przetwarzania danych osobowych jeszcze w toku postępowania. Będzie to możliwe, jeśli zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych i dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki.

Kolejnym ważnym zagadnieniem jest „uprawnienie organizacji społecznej do wystąpienia z żądaniem wszczęcia postępowania bądź udziału w postępowaniu, nie tylko w przypadku gdy przemawia za tym interes społeczny, o czym stanowi art. 31 § 1 Kodeksu postępowania administracyjnego, ale również gdy przemawia za tym interes osoby, której prawa zostały naruszone".

W praktyce może to skutkować powstaniem wielu organizacji, które będą wyszukiwać potknięcia w przetwarzaniu danych przez instytucje publiczne i wykorzystywać ten fakt przeciwko nim. Do podobnych sytuacji dochodziło wejściu w życie ustawy o świadczeniu usług drogą elektroniczną.

Zgodnie z RODO organ nadzorczy ma wykonywać zadania na rzecz osób, których dane dotyczą (a jeżeli istnieje – również na rzecz inspektora ochrony danych), w sposób wolny od opłat. Opłaty za wniesienie skargi przewidziane są tylko w sytuacji, gdy wnioski skarżącego są ewidentnie nieuzasadnione lub nadmierne.

WAŻNE

To na organie nadzorczym będzie spoczywać ciężar udowodnienia, że wnioski skarżącego są ewidentnie nieuzasadnione lub nadmierne i w związku z tym powinny podlegać opłacie.

Bardzo istotne jest, aby przygotowując instytucję publiczną do nowych przepisów, przeanalizować dotychczasowy sposób reagowania na skargi klientów, szczególnie na te związane z przetwarzaniem danych osobowych. Wiadome jest, że większość kontroli następuje w efekcie postępowania skargowego, można zatem przypuszczać, że po wejściu w życie nowych przepisów liczba i prawdopodobieństwo kontroli znacząco wzrosną.

Dobrym rozwiązaniem dla instytucji publicznej będzie prowadzenie rejestru wszelkich skarg na przetwarzanie danych osobowych, aby móc poznać skalę potencjalnego problemu, szczególnie że w procesie obsługi takich skarg powinien brać udział inspektor ochrony danych. Przepisy nowej ustawy o ochronie danych osobowych przewidują, że w toku kontroli Prezesa UODO kontrolujący może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji, a organy kontroli państwowej lub Policja wykonują czynności na polecenie kontrolującego.

WAŻNE

Prezes Urzędu Ochrony Danych Osobowych będzie uprawniony do przeprowadzania kontroli bez uprzedniego zawiadomienia o tym kontrolowanego.

Jakie nowe zadania będzie miał procesor

Dalsze przetwarzanie

RODO wprowadza wiele istotnych obowiązków i ograniczeń dla procesora, czyli podmiotu przetwarzającego dane w imieniu instytucji publicznej. Przede wszystkim powierzanie dalszego przetwarzania danych osobowych będzie wymagać zgody administratora.

WAŻNE

Niedopuszczalne jest powierzanie dalszego przetwarzania danych osobowych bez zgody administratora.

Podmiot przetwarzający nie może zatem korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody instytucja powinna informować administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

Dotychczas (do 25 maja 2018 r.) umowa z podmiotem przetwarzającym dane osobowe w imieniu administratora (procesorem) również musiała być zawarta na piśmie (art. 31 ust. 1 ustawy o ochronie danych osobowych). Rozporządzenie uzupełnia tę zasadę – powierzenie przetwarzania danych może też zostać uregulowane innym instrumentem prawnym.

W myśl art. 33 ust. 2 RODO jeżeli podmiot przetwarzający dane w imieniu instytucji publicznej stwierdzi naruszenie ochrony danych osobowych, ma obowiązek zgłosić to administratorowi, nie musi natomiast zgłaszać naruszenia do Prezesa UODO.

Rejestr czynności przetwarzania

Obowiązkiem podmiotu przetwarzającego jest prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu instytucji publicznej (administratora). Procesor ma również obowiązek udostępnić taki rejestr na żądanie Prezesa UODO, a także wyznaczyć inspektora ochrony danych, jeśli zaistnieje przynajmniej jeden z czynników, o których stanowi art. 37 ust. 1 RODO.

WAŻNE

Podmiot przetwarzający powierzone dane osobowe ma obowiązek prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

Odpowiedzialność procesora

RODO wprowadza zasadę bezpośredniej odpowiedzialności procesora za nałożone na niego obowiązki z zakresu ochrony danych osobowych. Procesor musi m.in. wdrażać stosowne środki techniczne i organizacyjne, prowadzić rejestr czynności przetwarzania, w konkretnych okolicznościach wyznaczyć inspektora ochrony danych, spełnić te same wymagania przekazywania danych do państw trzecich jak administrator czy powiadamiać administratora o naruszeniach ochrony danych. Prezes UODO może egzekwować stosowanie RODO bezpośrednio w stosunku do przetwarzającego.

WAŻNE

Działający w imieniu instytucji publicznej procesor bezpośrednio odpowiada za nałożone na niego obowiązki z zakresu ochrony danych osobowych.

RODO wyraźnie podkreśla, że jeżeli podmiot przetwarzający naruszy zasady rozporządzenia przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania (co nie wyklucza stosowania przepisów art. 82, 83 i 84 dotyczących sankcji, kar, odszkodowań i odpowiedzialności). Oznacza to przykładowo, że jeśli dana instytucja publiczna powierzy dane, które zgromadziła, innej instytucji, a ta zmieni pierwotny cel przetwarzania i inaczej wykorzysta te dane, to ta druga instytucja stanie się dodatkowym administratorem danych. Taki stan obowiązywał już wcześniej, ale nie jako bezpośredni zapis prawny, a efekt interpretacji przepisów. To kolejny przykład na to, że przystępny język, w jakim napisano rozporządzenie, ułatwia wyjaśnienie i uregulowanie niejasnych i wymagających wcześniej interpretacji kwestii.

Dostosowując się do nowych przepisów, instytucje publiczne powinny przeprowadzić inwentaryzację wszystkich przypadków powierzenia przetwarzania danych, zapewnić, że są w formie umowy na piśmie (możliwa jest też forma elektroniczna) oraz ocenić, w jakim stopniu regulują kwestie

zdefiniowane przez RODO. Jeśli okaże się, że umowy nie zawierają wszystkich wymaganych elementów, powinny zostać zmienione (aneksowane).

WAŻNE

Administratorzy powinni na bieżąco oceniać zgodność współpracujących podmiotów z obecnymi i przyszłymi przepisami.

Kim ma być inspektor ochrony danych

IOD zamiast ABI

RODO zastępuje administratora bezpieczeństwa informacji (dalej ABI) inspektorem ochrony danych (dalej IOD). Zastąpienie ABI przez IOD nie polega tylko na nowym „tytule". Istotnym zmianom ulegną bowiem wymagania, jakie ma spełniać IOD oraz sytuacje, w których konieczne będzie jego wyznaczenie.

WAŻNE

Wszystkie instytucje publiczne (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości) – jednostki sektora finansów publicznych, instytuty badawcze i Narodowy Bank Polski – będą miały obowiązek wyznaczenia inspektora ochrony danych.

Z wytycznych dotyczących inspektorów ochrony danych (opracowanych przez Grupę Roboczą Art. 29) dowiadujemy się m.in., że:

- jeśli z przepisów nie wynika, że trzeba wyznaczyć IOD, to warto udokumentować taką decyzję,
- można dobrowolnie wyznaczyć IOD, nawet jeśli takiego obowiązku nie ma,
- IOD powinien brać udział w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji,
- zaleca się inspektorowi „ustalanie priorytetów w swojej pracy i koncentrowanie się na aspektach pociągających za sobą większe ryzyko".

Wymogi wobec IOD

Inspektor ochrony danych może mieć również obowiązki niezwiązane z ochroną danych osobowych. Wytyczne Grupy Roboczej art. 29 podkreślają, że „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów". Oznacza to, że inspektor nie może zajmować w instytucji stanowiska, które pociąga za sobą określanie sposobów i celów przetwarzania danych. Za powodujące konflikt interesów uważane będą m.in. stanowiska

kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT). Oznacza to, że większość dyrektorów, którzy mają coś wspólnego z przetwarzaniem danych, nie może być inspektorami ochrony danych.

WAŻNE

Funkcji IOD nie będą mogły pełnić osoby zajmujące stanowiska kierownicze, które mają coś wspólnego z przetwarzaniem danych.

Instytucja publiczna lub podmiot przetwarzający dane w jej imieniu będą mieli obowiązek publikować dane kontaktowe inspektora ochrony danych i zawiadomić o nich organ nadzorczy. To akurat nie jest żadną nowością, gdyż dotychczas również należało zgłosić ABI do rejestracji w GIODO. Informacje o sposobie kontaktu z IOD też trzeba będzie podawać podczas zbierania danych osobowych.

Zgodnie z RODO osoby, których dane są przetwarzane w instytucji, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych oraz z korzystaniem z przysługujących im praw.

WAŻNE

Osoby, których dane są przetwarzane w instytucji, będą mogły kontaktować się bezpośrednio z inspektorem ochrony danych.

W RODO nie wskazano, jakie dane kontaktowe inspektora trzeba będzie podać. Nowa ustawa o ochronie danych osobowych w art. 10 ust. 1 określa, że w zawiadomieniu o wyznaczeniu inspektora ochrony danych do organu nadzorczego trzeba będzie podać jego imię, nazwisko, oraz adres poczty elektronicznej lub numer telefonu. IOD będzie też musiał dysponować odpowiednimi środkami technicznymi umożliwiającymi łatwy i szybki kontakt z zainteresowanymi.

Inspektor może być pracownikiem danej instytucji publicznej lub wykonywać zadania na podstawie umowy o świadczenie usług. Jednak w każdym przypadku należy zapewnić mu zasoby niezbędne do podtrzymania jego wiedzy fachowej.

WAŻNE

Instytucja publiczna będzie musiała uwzględnić plany rozwoju inspektorów ochrony danych i znaleźć na nie środki finansowe.

Funkcja IOD może być też pełniona przez podmiot zewnętrzny. RODO zezwala na taki outsourcing i prawdopodobnie będzie to najlepsze rozwiązanie szczególnie dla tych podmiotów, które nigdy wcześniej nie powoływały administratora bezpieczeństwa informacji. Stanowisko takie przedstawione jest także w wytycznych Grupy Roboczej Art. 29, w których podkreśla się, że „usługowy” inspektor

ochrony danych pozwala wykorzystać siłę tkwiącą w zespole, jaki razem z nim świadczy usługi, co w efekcie pozwala mu lepiej wykonywać swoje zadania.

WAŻNE

Funkcję inspektora ochrony danych można outsource'ować.

Nowa ustawa o ochronie danych osobowych zakłada, że ABI, którzy pełnili tę funkcję 24 maja 2018 r., od 25 maja 2018 r. stali się inspektorami ochrony danych i będą nimi do 1 września 2018 r. Do tego czasu, administrator ma czas na podjęcie decyzji, czy konkretna osoba wciąż będzie pełniła tę funkcję (i dokonanie stosowanego zawiadomienia do Prezesa UODO). Jeśli do tego czasu administrator nie zawiadomi o wyznaczeniu danej osoby na IOD, 1 września 2018 r. z mocy prawa dotychczasowi ABI przestaną pełnić funkcję inspektorów ochrony danych.

Jakie mogą być konsekwencje naruszenia przepisów

Wysokie kary finansowe

Za niestosowanie lub naruszenie zasad przewidzianych w RODO instytucje będą karane bardzo wysokimi grzywnami, które w przypadku urzędów i instytucji publicznych mogą wynosić do 100 tys. złotych (w przypadku jednostek kultury kara może wynieść maksymalnie 10 tys. zł) – takie obniżenie wysokości kar przewidzianych przez RODO wprowadziła nowa ustawa o ochronie danych osobowych w art. 102.

Za jakie naruszenia można otrzymać karę		
Wysokość kary	Jednostki sektora finansów publicznych, instytuty badawcze, Narodowy Bank Polski – do 100 tys. zł	Instytucje kultury – do 10 tys. zł
Treść naruszeń	1) złamanie zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych (*privacy by design / by default*), 2) naruszenia w przetwarzaniu danych z upoważnienia administratora danych lub podmiotu przetwarzającego, 3) naruszenia w zakresie rejestracji czynności przetwarzania,	

	4) złamanie zasad współpracy z organem nadzorczym, 5) złamanie zasad bezpieczeństwa danych, 6) złamanie zasad przetwarzania danych osobowych, 7) naruszenie warunków wyrażania zgody na przetwarzanie danych, 8) naruszenia w dostępie do danych dla osób, których dane są przetwarzane, 9) złamanie prawa osób do korygowania i usuwania przetwarzanych danych.

Przykłady zaniedbań podlegających grzywnie:

- administrator nie wdrożył odpowiednich środków technicznych i organizacyjnych mających na celu ochronę praw osób, których dane dotyczą,
- administrator nie uwzględnił ochrony danych w fazie projektowania (na etapie projektowania systemu informatycznego),
- administrator nie zgłosił incydentu w ciągu 72 godzin po stwierdzeniu naruszenia, organowi nadzorczemu, a incydent ten skutkował naruszeniem praw lub wolności osób fizycznych.

Okoliczności brane pod uwagę

Każdy przypadek będzie indywidualnie rozpatrywany i pod uwagę będą brane m.in. następujące elementy:

- skala naruszenia,
- umyślność działań,
- co administrator zrobił, żeby zminimalizować szkody poniesione przez osoby, których dane dotyczą,
- „recydywa", czyli czy jest to pierwsze, czy kolejne przewinienie,
- kategorie przetwarzanych danych osobowych,
- stopień współpracy z Prezesem UODO.

Organ nadzorczy może uwzględniać wszelkie okoliczności obciążające lub łagodzące. Jeśli działanie było celowe, nie zdarzyło się pierwszy raz, a winny nie będzie chciał z Prezesem UODO współpracować, to można zakładać wyższe kary, przy czym trzeba pamiętać, że „jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie" (art. 83 ust. 3 RODO).

Do tej pory w przypadku naruszenia bezpieczeństwa danych winowajca miał czas na uszczelnienie luk w ich ochronie. Przekroczenie wyznaczonego terminu lub niedopełnienie wymogów prawnych skutkowało karą administracyjną.

Odpowiednie zabezpieczenia

Zgodnie z RODO „państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania".

Instytucje publiczne będą zatem musiały zastanowić się nad zwiększeniem budżetów na zabezpieczenie informacji, a w szczególności na rozwiązania informatyczne takie jak m.in.:

- systemy monitorowania zdarzeń w systemach informatycznych (*SIEM – Security Information and Event Management*),
- systemy zapobiegania wyciekom informacji (tzw. *DLP* – ang. *Data Lost Prevention*),
- rozwiązania wykrywające i blokujące ataki sieciowe (*IDS/IPS – Intrusion Detection/Prevention Systems*),
- mechanizmy wspierające zarządzanie dostępami do informacji (*IdM – Identity Management*).

W większych instytucjach konieczne może okazać się rozbudowanie zespołów bezpieczeństwa informacji i zarządzania incydentami, szczególnie w świetle obowiązku prowadzenia rejestru incydentów oraz raportowania tych poważniejszych do organu nadzorczego (Prezesa UODO). Konieczne będzie wdrożenie i przetestowanie procedur postępowania w sytuacjach kryzysowych, np. w przypadku wycieku danych. To o tyle ważne, że do ustalenia wysokości kary organ nadzorczy będzie brał pod uwagę wiele czynników, m.in. sposób, w jaki dane były zabezpieczone na poziomie technicznym lub organizacyjnym oraz jakie działania zostały podjęte, żeby zminimalizować szkody.

W uzasadnieniu do ustawy podkreśla się, że organ nadzorczy powinien przywiązywać ogromne znaczenie do zebrania w toku postępowania dowodów przemawiających nie tylko za wymierzeniem administracyjnej kary pieniężnej, ale również wymierzeniem kary o takiej, a nie innej wysokości.

Wydane rozstrzygnięcia mają też być wyczerpująco uzasadniane. Na tej podstawie powstanie z pewnością istotna baza wiedzy dla wszystkich zainteresowanych.

Autor:
Katarzyna Czajkowska-Matosiuk

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-7621-6
E-book nr:	2HH0773
Firma:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł, Nr rejestrowy BDO: 000008579