Reforma ochrony danych osobowych w UE

Uwzględnia projekt ustawy o ochronie danych osobowych

Autor **Leszek Kępa**

Spis treści

Wszyscy przedsiębiorcy oraz instytucje, które przetwarzają dane osobowe, powinni przygotować się na rewolucyjne zmiany. 25 maja 2016 r. weszły w życie, a od 2018 r. zaczną obowiązywać przepisy europejskiego rozporządzenia o ochronie danych osobowych.[1] Pełna nazwa tego aktu to: Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[2] (ogólne rozporządzenie o ochronie danych), które dalej określane jest w skrócie jako Rozporządzenie lub RODO.

RODO to europejskie rozporządzenie o ochronie danych osobowych

Zastąpi ono Dyrektywę 95/46 WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, której zapisy sięgają 1995 roku, kiedy internet dopiero raczkował, a sposób prowadzenia biznesu mocno różnił się od dzisiejszego. Czas między przyjęciem przepisów, a ich stosowaniem ma służyć głównie dostosowaniu przepisów krajowych, a także umożliwić administratorom danych przygotowanie się do realizacji nowych obowiązków, co też zostało wybitnie podkreślone w motywie 171 preambuły: *przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów.*
Proces dostosowywania jest długotrwały, przygotowania należy zacząć jak najszybciej i dlatego oddajemy w Państwa ręce przewodnik po kluczowych założeniach nowego prawa, w którym przedstawiamy, w jaki sposób wpłynie ono na funkcjonowanie organizacji oraz w którym radzimy jak przygotować się do funkcjonowania w nowej rzeczywistości prawnej.

Rys historyczny

Reforma przepisów o ochronie danych osobowych, której jesteśmy świadkami, następuje po ponad 20 latach od uchwalenia dyrektywy 95/46/WE , która jest fundamentalnym aktem prawnym regulującym kwestie ochrony danych osobowych w całej Europie.
Wszystko zaczęło się 4 listopada 2010 r., kiedy Komisja Europejska – po przeprowadzeniu szeroko zakrojonych konsultacji społecznych – opublikowała komunikat zatytułowany *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej.* W ten sposób zapowiedziana została kompleksowa nowelizacja europejskiego prawa w zakresie ochrony danych osobowych, która odpowiadałaby zmieniającej się rzeczywistości jednolitego rynku cyfrowego. Niedługo później, 6 lipca 2011 r., Parlament Europejski przyjął rezolucję, w której poparł stanowisko Komisji[3], a 24 lutego 2011 r. swoje poparcie dla zmian wyraziła Rada Unii Europejskiej. Wśród unijnych instytucji panowała zgodność co do tego, że przepisy o ochronie danych osobowych potrzebują odświeżenia i ujednolicenia.

1) http://ec.europa.eu/health/data_collection/docs/com_2010_0609_pl.pdf
2) http://eur-lex.europa.eu/legal-content/pl/ALL/?uri=CELEX:31995L0046
3) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL

przepisów prawa Unii Europejskiej. Składają się na nie:

- rozporządzenia,
- dyrektywy,
- decyzje,
- opinie,
- zalecenia.

Dyrektywy europejskie mają moc wiążącą wyłącznie co do rezultatu, dlatego ich rolą jest harmonizacja prawa. Oznacza to, że państwa członkowskie mają obowiązek wdrożyć opisane w dyrektywie przepisy, ale posiadają przy tym swobodę sposobu ich implementacji. Przykładowo, Dyrektywa 95/46/WE weszła do polskiego porządku prawnego przez uchwalenie w 1997 r. ustawy o ochronie danych osobowych.

Rozporządzenia europejskie są podobne do polskich ustaw, mają charakter wiążący i — co najważniejsze — obowiązują bezpośrednio. Oznacza to, że do rozporządzenia UE w Polsce (i w innych krajach Unii Europejskiej) należy stosować się tak samo, jakby to była polska ustawa.

Warto pamiętać, że władze krajowe mają obowiązek uchylenia wszelkich przepisów niezgodnych z treścią rozporządzenia, mają też zakaz wydawania aktów prawnych niezgodnych z jego postanowieniami. Hasłem przyświecającym idei stworzenia jednego unijnego rozporządzenia w zakresie ochrony danych osobowych była bowiem zasada: *jeden kontynent – jedno prawo.*

Rozporządzenie pozostawiło państwom członkowskim, w tym Polsce, pewną swobodę w stosowaniu przepisów i dlatego w marcu 2017 r. pojawił się projekt ustawy o ochronie danych osobowych, jako uzupełnienie Rozporządzenia. W uzasadnieniu do tego projektu podkreśla się, że „przepisy nowej ustawy o ochronie danych osobowych, mają zapewnić skuteczne stosowanie w polskim porządku prawnym rozporządzenia".

Do RODO należy stosować się tak, jakby to była polska ustawa

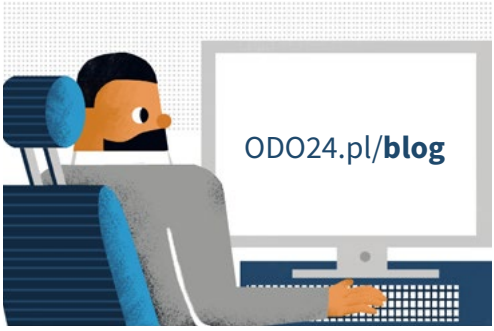
Analizowane w niniejszym poradniku Rozporządzenie jest próbą odpowiedzi na nowe wyzwania ery cyfrowej, m.in.:

- wzrost skali wymiany danych,
- szybki postęp technologiczny,
- różnice w poziomie ochrony danych osobowych w państwach Unii.

Ujednolicenie i uproszczenie przepisów nie oznacza jednak, że Rozporządzenie zastąpi całkowicie krajowe przepisy o ochronie danych osobowych – przewiduje się bowiem pewien obszar dla lokalnych regulacji krajowych, które mogą dotyczyć kwestii takich jak np. ustanowienie niezależnego organu nadzorczego (dzisiaj GIODO) i zapewnienia mu odpowiednich środków technicznych, kadrowych i finansowych. Kraje członkowskie mają również prawo uregulować indywidualnie (jednak w określonych ramach) granicę wieku dziecka, od którego może ono samodzielnie wyrazić zgodę na przetwarzanie danych.

Należy przypomnieć, że głównym celem Dyrektywy 95/46/WE, która jest matką europejskich ustaw o ochronie danych osobowych, była harmonizacja podstawowych praw i wolności osób fizycznych oraz gwarancja swobodnego przepływu danych osobowych w ramach Unii Europejskiej. Mimo rewolucji w europejskich przepisach o ochronie danych osobowych, te cele wciąż są aktualne i pozostały niezmienione.

Warto zauważyć, że w chwili gdy znana była propozycja zmian w europejskich przepisach, w Polsce rozpoczęto działania tworzące grunt pod rewolucję i w listopadzie 2014 r. znowelizowano ustawę o ochronie danych osobowych wprowadzając wiele rozwiązań, które widzimy dzisiaj w Rozporządzeniu.



Kiedy i jak zacząć się przygotowywać

Obecne przetwarzanie danych osobowych należy dostosować w ciągu dwóch lat od wejścia w życie nowych przepisów. Proces dostosowywania jest długotrwały, dlatego przygotowania należy zacząć jak najszybciej.

Przygotowania do RODO trzeba zacząć już teraz, aby 25 maja 2018 być w zgodzie z przepisami

Aby być dobrze przygotowanym należy m.in:

- zapewnić zgodność przetwarzania z obecnie obowiązującymi przepisami, tj. ustawą o ochronie danych osobowych – ułatwi to przygotowania do zapewnienia zgodności z Rozporządzeniem,
- poznać dobrze wymagania Rozporządzenia, by wiedzieć do czego należy się przygotować – niniejszy Poradnik powinien ułatwić to zadanie,
- przeszkolić zespół który będzie koordynował przygotowania do Rozporządzenia,
- zrozumieć gdzie i jakie dane są przetwarzane,
- dokonać przeglądu własnych zleceniobiorców (tzw. procesorów) i współpracować z nimi, aby także dostosowali swoje procesy do Rozporządzenia,
- przeanalizować obecne procesy zbierania danych,
- przejrzeć istniejące procedury i dokumentację,
- przeanalizować kto i za co jest odpowiedzialny w procesach przetwarzania,
- wdrożyć procesy analizy i szacowania ryzyka,
- wzmocnić zabezpieczenia (tam gdzie to potrzebne, bazując na ocenie ryzyka) i zapewnić, że bezpieczeństwo będzie wbudowane we wszystkie nowe procesy,
- dokumentować naruszenia bezpieczeństwa i prowadzić rejestr incydentów,
- przygotować procesy zarządzania incydentami bezpieczeństwa.

Nie trzeba tłumaczyć, że dostosowanie się do Rozporządzenia nie jest kwestią wyłącznie działu prawnego czy IT. Zapewnienie zgodności wymaga współpracy w całej organizacji – poziom kar oraz potencjalny wpływ na funkcjonowanie organizacji uczynił z Rozporządzenia problem na poziomie zarządu, a nie pojedynczych działów.

Administratorzy oraz podmioty przetwarzające dane muszą się przygotować

Podkreślenia wymaga to, że przygotować muszą się zarówno administratorzy danych jak i podmioty, które przetwarzają dane na zlecenie, szczególnie że w stosunku do tych ostatnich Rozporządzenie definiuje bardzo dużo nowych obowiązków.

24 najważniejsze zmiany w prawie

Przygotowanie się do zapewnienia zgodności z Rozporządzeniem, to nie tylko unikanie wysokich kar. Coraz więcej uczestników rynku zdaje sobie sprawę z tego, jaka jest ekonomiczna wartość danych, które dzięki nowym technologiom pozyskiwane i przetwarzane są z każdym rokiem coraz szybciej. Rośnie też świadomość klientów (osób, których dane są przetwarzane), którzy zdają sobie sprawę z zagrożeń wynikających z udostępniania danych. W związku z tym, coraz ważniejszym staje się zapewnienie ochrony ich prywatności, a tym samym zdobycie ich zaufania.

Klienci oczekują ochrony ich danych osobowych

Każda organizacja, która chce spełnić oczekiwania swoich klientów, powinna zapoznać się z nowymi regulacjami, w odpowiedni sposób przygotować się, a następnie wdrożyć przepisy Rozporządzenia. Poniżej przedstawiam w skrócie najważniejsze zmiany, wraz z poradami, które powinny ułatwić cały proces.

1 Jednolite prawo w całej Europie

Mające obowiązywać od maja 2018 r. Rozporządzenie będzie spójnym narzędziem do stosowania we wszystkich państwach członkowskich. Oznacza to, że 28 porządków prawnych z dziedziny ochrony danych osobowych zostanie zastąpione jednym, obowiązującym w całej Unii, aktem prawnym.[9] W efekcie wszyscy przedsiębiorcy z każdego z unijnych państw członkowskich będą zobowiązani do stosowania się do tych samych zasad ochrony danych osobowych.

Do tej pory kwestie przetwarzania danych osobowych w Europie regulowała Dyrektywa 95/46/WE. Jak wiemy, dyrektywy wiążą w odniesieniu do rezultatu, który ma być osiągnięty, co oznacza, że państwa członkowskie muszą wprowadzić w życie przepisy opisane w danej dyrektywie, mając jednak przy tym swobodę wyboru metod i środków jej wdrożenia. Tłumacząc obrazowo: w przypadku Dyrektywy 95/46/WE każdy miał wybudować most na rzece, ale jego ostateczny kształt i rodzaj użytych materiałów pozostawiono decyzji każdego z państw.

W preambule Rozporządzenia, w motywie 10, podkreślono, że: *aby zapewnić wysoki i spójny poziom ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych.*

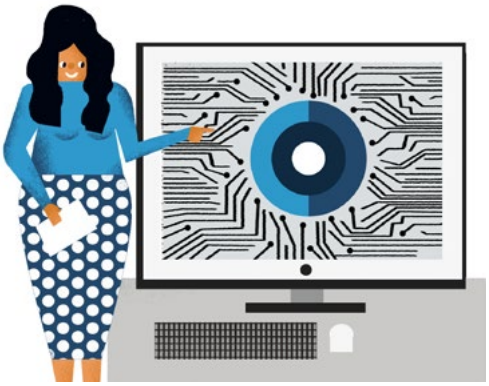
Fakt, że dyrektywę zastąpi Rozporządzenie, należy uznać za dobry kierunek zmian. Ujednolici to przepisy dotyczące ochrony danych w krajach, które – wracając do wcześniejszej obrazowej metafory – w końcu będą miały identyczne mosty. Zmiany przepisów są szczególnie korzystne dla wszystkich przedsiębiorców, którzy aktywnie działają na terenie całej Unii Europejskiej, tj. mają międzynarodowych partnerów, oddziały i sieć sprzedaży.

Do 25 maja 2018 r. należy (wciąż) przestrzegać obecnie obowiązujących przepisów o ochronie danych osobowych

Trzeba podkreślić, że przyjęcie rozporządzenia to zaledwie początek zmian w przepisach. Dzisiaj zasady przetwarzania danych osobowych uregulowane są w kilkuset aktach prawnych, nie tylko w ustawie o ochronie danych osobowych, jak zwykło się uważać – wszystkie te przepisy muszą zostać dostosowane do Rozporządzenia. Oprócz tego wraz z Rozporządzeniem pojawią się nowe krajowe przepisy, na które zezwala, bądź których wymaga owe Rozporządzenie. Przykładowo w marcu 2017 r. pojawił się projekt ustawy o ochronie danych osobowych.[10] Wszystkie te zmiany warto śledzić, aby wiedzieć jak się przygotować.

Dobrze też analizować sukcesywnie pojawiające się interpretacje i objaśnienia dotyczące Rozporządzenia, np. opinie i wytyczne przygotowane przez Grupę Roboczą Art. 29 czy też Europejską Radę Ochrony Danych, która docelowo Grupę Robocza ma zastąpić.[11]

Należy zaznaczyć, że do 25 maja 2018 r. nadal powinno



9) W chwili przygotowania publikacji nie do końca jasne było, jak traktować deklarację wyjścia Wielkiej Brytanii z Unii Europejskiej (tzw. „Brexit"). Do czasu wyjścia jest ona członkiem Unii i musi szanować i przestrzegać europejskiego prawa.
10) https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych
11) Więcej na temat Grupy Roboczej Art. 20 na stronie internetowej GIODO – http://www.giodo.gov.pl/261/id_art/920/j/pl/

niało wymagania przepisów z zakresu ochrony danych osobowych, gdyż wymagało to dużych nakładów pracy i nierzadko sporych nakładów finansowych. Doskonałym przykładem jest agent ubezpieczeniowy. Działa on jako osoba fizyczna prowadząca jednoosobową działalność gospodarczą, ale zgodnie z przepisami musi sam dla siebie (sic!) przygotować politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dla jednej osoby jest to nie lada wyzwanie, nie mówiąc o tym, że nie do końca jest to racjonalne. Rozporządzenie zmienia tę sytuację i tak przykładowo:

- organizacje, które nie przetwarzają danych osobowych na dużą skalę, nie będą musiały powoływać inspektora ochrony danych osobowych,
- rejestrowania czynności przetwarzania nie będą dokonywać podmioty, które zatrudniają mniej niż 250 osób i spełniają warunki określone w art. 30 ust. 5 Rozporządzenia,
- grupa przedsiębiorstw będzie mogła powołać jednego inspektora ochrony danych osobowych.

W preambule Rozporządzenia, w motywie 13, podkreślono, że: *aby zapewnić spójny poziom ochrony osób fizycznych w Unii oraz zapobiegać rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym – w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom – pewność prawa i przejrzystość (…). Z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw niniejsze rozporządzenie przewiduje wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników. Ponadto zachęca się instytucje i organy Unii, państwa członkowskie i ich organy nadzorcze, by stosując niniejsze rozporządzenie, uwzględniały szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.*

Obowiązki w zakresie ochrony danych będą zależeć od rodzaju i skali przetwarzania, a nie od formy organizacji

Dobrym kierunkiem jest też uzależnienie obowiązków od rodzaju przetwarzania danych, a nie od formy organizacji.

4 Większy zasięg prawa

Przedsiębiorcy spoza Unii Europejskiej też będą musieli stosować się do Rozporządzenia, jeśli:

- oferują towary lub usługi osobom w UE,
- monitorują („obserwują") zachowania i zwyczaje osób z obszaru UE, na przykład przy pomocy geolokalizacji, o ile do zachowania tego dochodzi w Unii.

Przedsiębiorcy spoza Unii Europejskiej też będą musieli stosować się do RODO

Do oceny, czy towary lub usługi są lub mogą być oferowane w Unii, wystarczy według Motywu 23 Rozporządzenia m.in.: posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii.

Organizacje spoza Unii zobowiązane będą dokładnie przeanalizować w jaki sposób powinny dostosować się do nowych wymagań, w tym wyznaczyć swojego przedstawiciela na terenie Unii.

5 Nowa nazwa organu i większa moc sprawcza

Dotychczasowy GIODO – Generalny Inspektor Ochrony Danych Osobowych – zyska nową nazwę: Prezes Urzędu

Ochrony Danych Osobowych. Zmianę wprowadza projekt ustawy o ochronie danych osobowych. W uzasadnieniu do niego dowiadujemy się, że zmiana nazwy urzędu wynika z tego, że Rozporządzenie wprowadza inspektora ochrony danych osobowych i mogło to prowadzić do niejasności jaka jest relacja między „zwykłym" inspektorem a inspektorem „generalnym". Co więcej zaproponowano aby dawnych inspektorów GIODO nazwać „kontrolującymi", aby nie mylono ich z inspektorami ochrony danych, o których mowa w Rozporządzeniu.

Dla ułatwienia dalej w Poradniku będzie używane określenie UODO – Urząd Ochrony Danych Osobowych – mając na myśli Prezesa Urzędu, a tam gdzie mowa o dzisiejszym organie nadzoru, stosowana będzie dotychczasowa nazwa GIODO. Trzeba pamiętać, że UODO jest propozycją nazwy i może w przyszłości jeszcze się zmienić.

Zgodnie z zapisami Rozporządzenia krajowe organy nadzorcze, których odpowiednikiem w Polsce jest obecnie GIODO będą musiały być wyposażone w odpowiednie zasoby techniczne, kadrowe i finansowe. Można przypuszczać, że biuro Generalnego Inspektora zostanie rozbudowane. Na gruncie Rozporządzenia, GIODO stanie się organem, z którego decyzjami przedsiębiorcy będą musieli się liczyć. Zyska „powagę" i nazwę podobną do UOKiK.

GIODO stanie się UODO - organem, z którym trzeba będzie się liczyć

Nowe uprawnienia UODO nie będą różnić się znacząco od obecnych, chociaż pojawiły się pewne obowiązki wymienione wprost, które w dotychczasowych przepisach nie występowały, np. Prezes Urzędu będzie udzielać zaleceń dotyczących szczególnych operacji przetwarzania (art. 57 ust. 1 Rozporządzenia). Nowe przepisy dotyczące organów nadzorczych mówią o:

- przyjmowaniu standardowych klauzul umownych,
- prowadzeniu wykazu ocen skutków przetwarzania,
- udzielaniu zaleceń jak przetwarzać dane osobowe, o których mowa w art. 36 ust. 2 Rozporządzenia w związku z uprzednimi konsultacjami,
- zachęcaniu do tworzenia i stosowania kodeksów postępowania,[12]
- zachęcaniu do mechanizmów certyfikacji (dziś nie istnieją),
- akredytacji podmiotów certyfikujących,

- prowadzeniu rejestru naruszeń,
- obowiązku wzajemnej pomocy i współpracy z innymi organami nadzorczymi.

Struktury Urzędu Ochrony Danych Osobowych zostaną zapewne rozbudowane. Już wcześniej o to postulowano, w efekcie czego w ramach rozporządzenia z dn. 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych, ustalone zostały siedziby dwóch jednostek zamiejscowych – w Katowicach oraz w Gdańsku. Siedziby te co prawda jeszcze nie powstały, ale przepisy otworzyły taką możliwość. Motyw 127 Rozporządzenia podkreśla, że każde państwo członkowskie będzie musiało zapewnić organowi nadzorującemu ochronę danych osobowych warunki i możliwości operowania odpowiednimi zasobami ludzkimi. Czytamy tam: *każdy organ nadzorczy powinien zostać 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. Każdy organ nadzorczy powinien dysponować odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu krajowego lub państwowego.*

Te specjalne warunki pracy UODO podkreślone są też w treści art. 52 ust.4, 5 i 6 Rozporządzenia.

Skargę do UODO będzie można złożyć bezpłatnie, więcej skarg to większe ryzyko kontroli

12) GIODO obecnie także zachęca i wspiera tworzenie kodeksów postępowania, ale nie ma to prawnego umocowania, takiego jakie wprowadza Rozporządzenie
13) We wcześniejszym tłumaczeniu określony jako zainteresowany organ nadzorczy, co wydaje się było lepszym tłumaczeniem terminu „supervisory authority concerned".

Co również ważne, według nowego prawa, skargę do UODO będzie można złożyć bezpłatnie, a odbiorcą takiej skargi będzie mógł też zostać dowolny organ nadzorczy w UE. W takim przypadku będzie on, upraszczając, brał udział w sprawie jako tzw. *organ nadzorczy, którego sprawa dotyczy.*[13]

Osoby będą mogły skarżyć się bezpośrednio do sądu, z pominięciem organu nadzorczego (UODO) (art. 79 Rozporządzenia). Dzisiaj wielu przedsiębiorców „korzystało" z tego, że GIODO posiada ograniczone zasoby kadrowe i skargi rozpatruje bardzo powoli. To na pewno się zmieni. Również dlatego, że art. 24 projektowanej 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, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki.

Kolejnym ciekawym 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 KPA, ale również gdy przemawia za tym interes osoby, której prawa zostały naruszone". Może to oznaczać wysyp organizacji wyszukujących wszelakich potknięć w przetwarzaniu danych i szantażujących przedsiębiorców. Doświadczyliśmy tego wszyscy w związku z ustawą o świadczeniu usług drogą elektroniczną.

Rozporządzenie określa, że organ nadzoru ma wykonywać *zadania na rzecz osób, których dane dotyczą i jeżeli istnieje, inspektora ochrony danych w sposób wolny od opłat.* Opłaty za wniesienie skargi mogą się pojawić tylko wtedy, gdy wnioski skarżącego są ewidentnie nieuzasadnione lub nadmierne, ale uwaga – to na organie nadzorczym będzie spoczywać ciężar udowodnienia, że mają taki charakter.

Jako że większość kontroli następuje w efekcie postępowania skargowego, można zakładać, że łatwiejszy sposób składania skarg przełoży się na większe prawdopodobieństwo kontroli, gdyż skargi do tej pory są jednym z najważniejszych „wyzwalaczy" przeprowadzanych przez organ kontroli. Na pewno przygotowując się do wdrożenia nowych przepisów warto przeanalizować sposób reagowania na skargi klientów, szczególnie na te związane z przetwarzaniem danych osobowych.

Warto rozważyć prowadzenie rejestru wszelkich skarg na przetwarzanie danych osobowych, aby móc poznać skalę potencjalnego problemu, szczególnie że w przyszłości w procesie obsługi takich skarg będzie brał udział inspektor ochrony danych.

Trzeba zauważyć, że w projektowanych przepisach przewiduje się, że w toku kontroli UODO kontrolujący może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji, a organy kontroli państwowej lub Policja wykonują czynności na polecenie kontrolującego. Co więcej, Prezes Urzędu będzie uprawniony do przeprowadzania kontroli bez uprzedniego zawiadomienia o tym fakcie kontrolowanego.

6 Nowe sankcje jako większa siła oddziaływania prawa

Za naruszenie istotnych przepisów ochrony danych osobowych, Rozporządzenie przewiduje grzywnę do 20 mln EUR, a w przypadku przedsiębiorstwa – do 4% całkowitego światowego obrotu z poprzedniego roku. Niższe kary do 10 mln EUR lub do 2% światowego obrotu, przewidziane są w sprawach mniejszej wagi.

Nowe rozporządzenie wprowadza bardzo surowe kary

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

- skala naruszenia,
- umyślność działań,
- co zrobiono, żeby zminimalizować szkody poniesione przez osoby, których dane dotyczą,

ODO 24

Oferujemy pakiet usług przygotowujących do RODO

KOMPLEKSOWE WDROŻENIE ROZPORZĄDZENIA
Kilkuetapowy proces przygotowujący organizację do funkcjonowania w zgodzie z obowiązującymi i przyszłymi przepisami prawa.

AUDYT ZGODNOŚCI
Ekspercka analiza systemów informatycznych, procesów biznesowych i dokumentacji. Szczegółowy raport zawierający praktyczne rekomendacje i harmonogram dostosowania.

ANALIZA RYZYKA
Przeprowadzana według sprawdzonej metodologii. Zawierająca wnioski, rekomendacje zabezpieczeń oraz plan postępowania z ryzykiem. Pomaga uniknąć nieprzewidzianych strat biznesowych.

PRZYGOTOWANIE DOKUMENTACJI
Tworzymy nowe lub dostosowujemy istniejące polityki i procedury związane z zapewnieniem odpowiednich środków technicznych i organizacyjnych.

WSPARCIE lub **PRZEJĘCIE ABI/IOD**
RODO to szerszy zakres obowiązków. Oferujemy wsparcie, lub przejęcie funkcji ABI a w przyszłości IOD.

ODO 24.pl

tel. 22 740 99 00

Wspieramy FUNDACJA WIEDZA TO BEZPIECZEŃSTWO

szlachetna PACZKA