# Reforma ochrony danych osobowych w UE


Autor **Leszek Kępa**

# Spis treści

# Patron poradnika

ODO 24 sp. z o. o. oferuje kompleksowe rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Dzięki doświadczonemu zespołowi ekspertów z zakresu m.in. prawa, informatyki, zarządzania kryzysowego oraz ciągłości działania dostarcza organizacjom praktyczne rozwiązania, pozwalające skutecznie zabezpieczyć posiadane zasoby informacyjne.

Niniejszy poradnik powstał, aby poinformować polskich przedsiębiorców o zmianach w przepisach o ochronie danych osobowych, które wejdą w życie 25 maja 2018 r. oraz pozwolić im należycie i na czas się do nich przygotować.

**Autor poradnika**
Leszek Kępa – ekspert bezpieczeństwa informacji, autor kilku książek i wielu publikacji na temat ochrony danych osobowych i bezpieczeństwa informacji. Posiada, uznane na całym świecie, certyfikaty CISA (Certified Information Security Auditor), CISM (Certified Information Security Manager) oraz CEH (Certified Ethical Hacker). Jest członkiem ISACA oraz Podkomisji Ochrony Danych i Standaryzacji Informacji Polskiej Izby Ubezpieczeń. Absolwent Szkoły Głównej Handlowej, Politechniki Częstochowskiej oraz Akademii Podlaskiej.

**Ilustracje**
Karol Banach (www.karolbanach.com)

**Projekt i skład**
Radosław Zbytniewski (www.zbytniewski.com.pl)

**Redakcja i korekta**
Aleksandra Kaniewska

**ISBN: 978-83-943435-1-4**

**Warszawa, wrzesień 2016 r.**

**Wszyscy przedsiębiorcy oraz instytucje, które przetwarzają dane osobowe, powinni przygotować się na ważne zmiany. 25 maja 2018 r. zaczną obowiązywać przepisy unijnego rozporządzenia o ochronie danych osobowych.[1] Zastąpią one 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. Oddajemy w Państwa ręce przewodnik po kluczowych założeniach nowego prawa, w którym przedstawiamy, w jaki sposób wpłynie ono na codzienne funkcjonowanie biznesu. Radzimy w nim też instytucjom państwowym i przedsiębiorcom, jak przygotować się do funkcjonowania w nowej rzeczywistości prawnej. Pełna nazwa wyżej wspomnianego 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 (ogólne rozporządzenie o ochronie danych)*, które dalej określane jest jako Rozporządzenie.**

## Rys historyczny

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*.[2] W ten sposób zapowiedziana została kompleksowa nowelizacja unijnego 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. Dla zmian, które przedstawiane są w tym poradniku, jedną z ważniejszych dat jest 25 stycznia 2012 r. Komisja Europejska przedstawiła wówczas opis najważniejszych elementów reformy ochrony danych.[4] Miały się na nią składać dwa nowe akty prawne:

- **ogólne rozporządzenie o ochronie danych, zastępujące Dyrektywę 95/46/WE,[5]**
- **dyrektywa określająca przepisy o ochronie danych osobowych przetwarzanych do celów zwalczania przestępczości, zastępująca decyzję ramową 2008/977/WSiSW.[6]**

W marcu 2014 r. Parlament Europejski już w pierwszym czytaniu zajął pozytywne stanowisko w sprawie projektów Rozporządzenia i dyrektywy, a rok później, w czerwcu, Rada zgodziła się z wnioskami Parlamentu i zatwierdziła ogólne, całościowe podejście do ochrony danych osobowych w Unii.[7] Tuż przed świętami, 15 grudnia 2015 r., zakończyły się trójstronne negocjacje pomiędzy Radą Unii Europejskiej, Parlamentem Europejskim i Komisją Europejską, mające na

1. http://ec.europa.eu/health/data_collection/docs/com_2010_0609_pl.pdf
2. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL
3. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu ekonomiczno-społecznego i Komitetu regionów – Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku – http://orka.sejm.gov.pl/sue7.nsf/pliki-zal/com_2012_9_pl_acte_f.pdf/$file/com_2012_9_pl_acte_f.pdf
4. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady – Zawiera definicje podstawowych terminów odnoszących się do dziedziny danych osobowych, ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych. Określa zasady i warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą – http://www.giodo.gov.pl/568/id_art/603/j/pl/
5. http://www.giodo.gov.pl/234/id_art/2501/j/pl/
6. http://www.consilium.europa.eu/press-releases-pdf/2015/6/40802199180_pl.pdf oraz http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/pl/pdf

celu ustalenie ostatecznej wersji pakietu dokumentów.[8] Po przyjęciu przez Radę dokumentów, 14 kwietnia 2016 r. Parlament przegłosował pakiet nowych unijnych ram prawnych dla ochrony danych osobowych, czyli dyrektywę i rozporządzenie. Z perspektywy polskich podmiotów, istotniejszym dokumentem jest Rozporządzenie, ponieważ zmienia i ujednolica obowiązujące przepisy dotyczące ochrony danych osobowych w całej Unii Europejskiej. Aby zrozumieć, jaki wpływ na obywateli mają zapisy Rozporządzenia, warto zapoznać się z konstrukcją 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 przy tym 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*. Przypomnijmy też, 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. 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.**

## Czy wprowadzane zmiany są dobre dla biznesu?

W tej publikacji przedstawione zostaną:

- **zarys zmian i nowych obowiązków administratorów danych, które nowe przepisy wprowadzają,**
- **subiektywna opinia autora, który ocenia, jak zmiana wpłynie na działalność polskich przedsiębiorców: czy będzie negatywna, pozytywna, czy neutralna,**
- **wskazówki, jak zacząć przygotowania do wprowadzenia nowych przepisów.**

***Klucz opisu zmian jest następujący:***

***Zmiana jest korzystna dla przedsiębiorców***

***Zmiana jest negatywna dla przedsiębiorców***

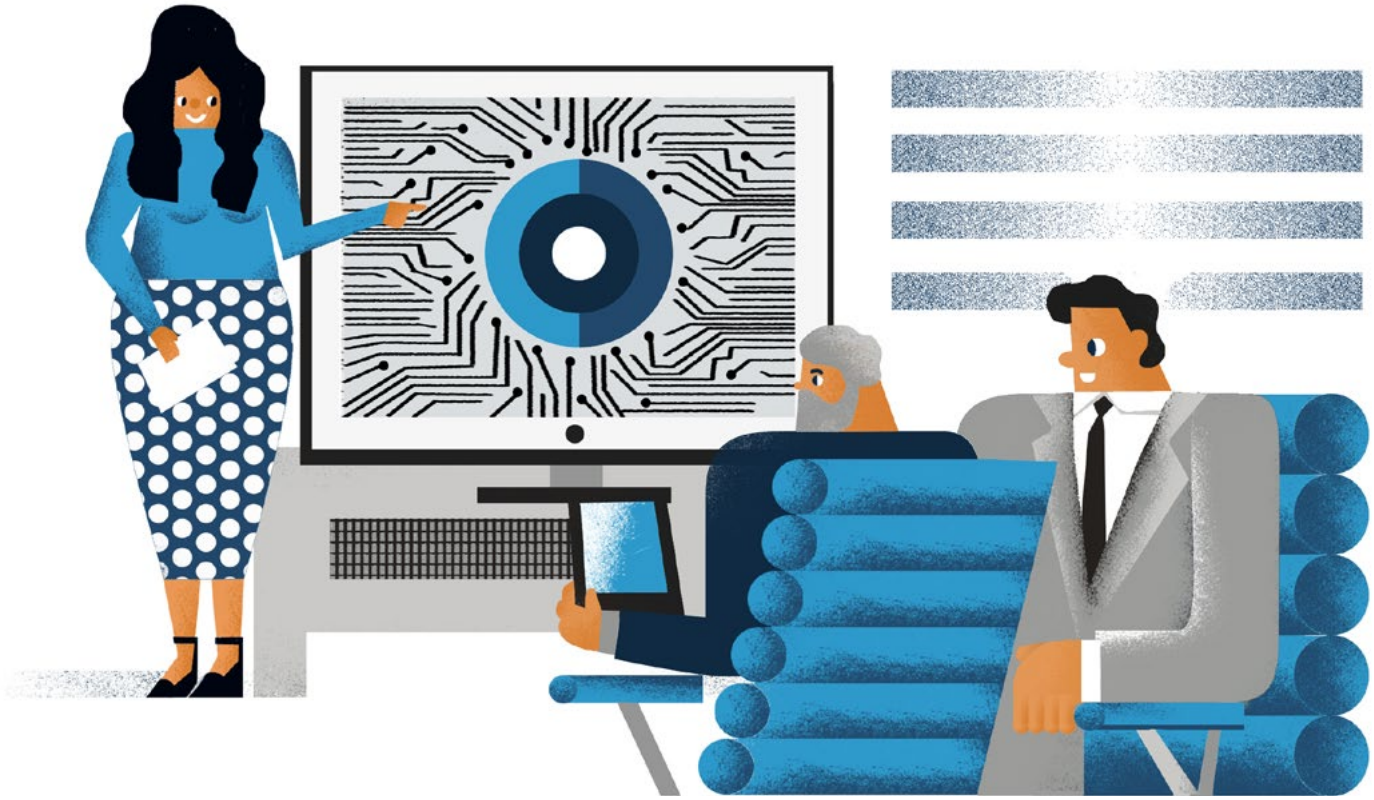
***Zmiana ma charakter neutralny***

Przy każdym opisie nowego przepisu przedstawiony będzie symbol określający charakter zmiany: pozytywny, negatywny lub neutralny. Po nim nastąpi skrótowy opis nowego prawa, a dalej informacje o tym, jak przedsiębiorca powinien się do tych zmian przygotować.

## 1 - Jednolite prawo w całej Europie

Mające obowiązywać od 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 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 podstawo-*

7. *http://www.consilium.europa.eu/press-releases-pdf/2015/6/40802199180_pl.pdf oraz http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/pl/pdf*
8. *Nawiasem mówiąc, w pewnym momencie śledzenie, na jakim etapie znajdują się zmiany, było ogromnym wyzwaniem, gdyż w obiegu były trzy projekty rozporządzenia.*
9. *W chwili przygotowania publikacji nie do końca jasne było, jak traktować deklarację wyjścia Wielkiej Brytanii z Unii Europejskiej (tzw. „Brexit"), dlatego przyjęto założenie, że jest ona wciąż formalnie członkiem Unii.*



*wych 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.

## 2 - Przystępny język

**Rozporządzenie napisano bardzo przystępnym językiem.** Zaczyna się preambułą, która stanowi wstęp do Rozporządzenia, wyjaśniający ogólne założenia i powody zmiany przepisów, a także dostarcza częściowej ich interpretacji. Polskie tłumaczenie dokumentu dobrze się czyta. Łatwo jest też zrozumieć poszczególne zapisy prawne, zwłaszcza jeśli porównać je do innych polskich aktów prawa. Doskonałym przykładem może być definicja firmy. Według Rozporządzenia jest to osoba fizyczna lub prawna, prowadząca działalność gospodarczą. To zgodne z potocznym rozumieniem słowa *firma*, za którą uważa się działające przedsiębiorstwo, czy zakład pracy. Natomiast w dotychczasowych przepisach o ochronie danych osobowych zamiast słowa firma pojawiał się dziwny twór językowy: osoby fizyczne i prawne oraz jednostki organizacyjne niebędące osobami prawnymi. Wracając do firmy – Kodeks cywilny w art. 432 określał, że *przedsiębiorca działa pod firmą*, czyli przez pojęcie firmy rozumiano nazwę, której w swojej działalności używał przedsiębiorca. W Rozporządzeniu pojawiają się też definicje, których wcześniej w polskich przepisach nie było. Mamy na przykład podmiot przetwarzający, w polskiej ustawie o ochronie danych osobowych określany jako podmiot, któremu administrator danych powierzył, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych. Ta definicja była zbyt długa, więc nie powinno dziwić, że w codziennym użytku przyjął się anglicyzm procesor. Nowa definicja jest krótsza, przez co łatwiejsza w użyciu. Przedsiębiorcy dużo łatwiej zinterpretują nowe przepisy, które mają ich obowiązywać już od 25 maja 2018 r. Wiele zagadnień, które wcześniej wymagały interpretacji specjalistów, jest wyjaśnionych wprost. Może to oznaczać mniejsze wydatki na pomoc ekspertów, m.in. doradztwo prawne.

## 3 - Prawo szyte na miarę

**Rozporządzenie w końcu zauważa małe i średnie przedsiębiorstwa.** Dotychczasowe prawo definiowało takie same wymagania ochrony danych osobowych zarówno osobom fizycznym prowadzącym działalność gospodarczą, jak i dużym, międzynarodowym korporacjom. Skutkowało to tym, że większość małych podmiotów prawie w ogóle nie przestrzegała przepisów z zakresu ochrony danych osobowych. Przykładem, jak prawo nie zauważało małych podmiotów, były chociażby obowiązki agenta ubezpieczeniowego. Działał on jako osoba fizyczna prowadząca jednoosobową działalność gospodarczą, ale zgodnie z przepisami musiał sam dla siebie (sic!) przygotować politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dla jednej osoby było to nie lada wyzwanie, nie mówiąc o tym, że było to zupełnie nieracjonalne. Rozporządzenie zmienia tę sytuację i tak przykładowo:

- **organizacje, które nie przetwarzają danych osobowych na dużą skalę, nie będą musiały powoływać inspektora ochrony danych,**
- **rejestrowania czynności przetwarzania nie będą dokonywać**

**podmioty, które zatrudniają mniej niż 250 osób (art. 30 ust. 5),**
- **grupa przedsiębiorstw będzie mogła powołać jednego inspektora ochrony danych.**

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*. Wpływ tej zmiany na przedsiębiorców jest bez wątpienia pozytywny, chociażby dlatego, że większość podmiotów gospodarczych działających na polskim rynku zatrudnia mniej niż 250 osób. Ominie ich więc obowiązek rejestrowania czynności przetwarzania. Dobrym kierunkiem jest też uzależnienie obowiązków od rodzaju przetwarzania danych, a nie od formy organizacji. Do niedawna uznawano, że obowiązek powołania administratora bezpieczeństwa informacji (ABI) mają wszystkie organizacje posiadające osobowość prawną (np. spółki z o. o.). Było to o tyle nieracjonalne, że konieczność powołania ABI powinna zależeć od tego, ile i jakie dane osobowe się przetwarza, a także jak się to robi, a nie od formy prowadzenia organizacji. Rozporządzenie bierze tę zależność pod uwagę.

## 4 - Większy zasięg prawa

**Przedsiębiorcy spoza Unii Europejskiej też będą musieli stosować się do Rozporządzenia.** Obowiązki ochrony danych osobowych będą ich dotyczyć, 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.**

Do oceny, czy towary lub usługi są oferowane w Unii, wystarczy według Rozporządzenia m.in.:

- **udostępnienie strony w języku jednego z krajów UE,**
- ***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.***

Wpływ tej zmiany na polskie przedsiębiorstwa należy uznać raczej za neutralny czy też znikomy.

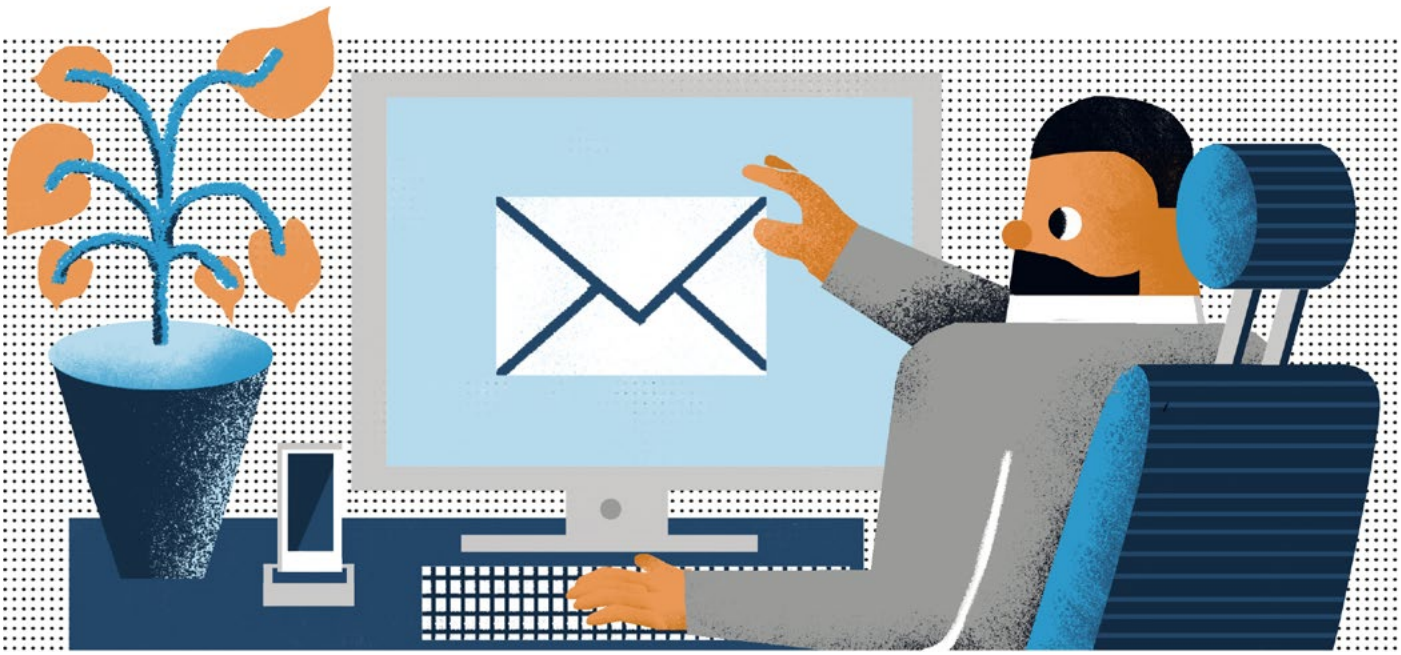
## 5 - Silny organ nadzorczy

Zgodnie z zapisami Rozporządzenia krajowe organy nadzorcze, których odpowiednikiem w Polsce jest GIODO – Generalny Inspektor Ochrony Danych Osobowych - będą musiały być wyposażone w odpowiednie zasoby techniczne, kadrowe i finansowe. Można przypuszczać, że biuro Generalnego Inspektora zostanie rozbudowane, szczególnie że obecnie instytucja wydaje się być niedofinansowana i z ograniczonymi zasobami kadrowymi. Na gruncie Rozporządzenia, GIODO stanie się organem, z którego decyzjami przedsiębiorcy muszą się liczyć. Zyska więc status podobny do UOKiK. Nowe uprawnienia GIODO nie będą różnić się znacząco od obecnych, chociaż pojawiły się pewne obowiązki wymienione wprost, które w dotychczasowych przepisach nie występowały, np. Generalny Inspektor będzie udzielać zaleceń dotyczących szczególnych operacji przetwarzania (art. 57 ust. 1 pkt l Rozporządzenia). Nowe przepisy dotyczące GIODO 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),**
- **zachęcaniu do tworzenia i stosowania kodeksów postępowania,**[10]
- **zachęcaniu do mechanizmów certyfikacji (dziś nie istnieją),**
- **akredytacji podmiotów certyfikujących,**
- **prowadzeniu rejestru naruszeń,**
- **obowiązku wzajemnej pomocy.**

Biuro GIODO zostanie 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 otwierają GIODO na taką możliwość. Preambuła (motyw 20) 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 GIODO podkreślone są też w treści art. 52 ust.4, 5 i 6 Rozporządzenia. Zapisy te określają nie tylko zasoby kadrowe, ale też niezależność organu, a także jego odrębność organizacyjną i polityczną. **Co również ważne, według nowego prawa, skargę do GIODO będzie można złożyć bezpłatnie.** Co więcej, odbiorcą takiej skargi będzie mógł też zostać dowolny organ nadzorczy w UE. W takim przypadku będzie on brał udział w sprawie jako tzw. organ nadzorczy, którego sprawa dotyczy.[11] Rozporządzenie określa, że GIODO

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



(i każdy jego odpowiednik w pozostałych państwach Unii) 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. Do tej pory złożenie skargi do GIODO wymagało wniesienia opłaty skarbowej w wysokości 10 zł. Eliminując opłaty, Rozporządzenie ułatwi ich składanie. Jako że większość kontroli GIODO następuje w efekcie postępowania skargowego, można zakładać, że łatwiejszy sposób składania skarg przełoży się na prawdopodobieństwo częstszych kontroli. Tę zmianę można ocenić dwojako. Dla przedsiębiorców będzie ona raczej negatywna, ale dla osób, których dane są przetwarzane – jest wyjątkowo pozytywna.

## 6 - Nowe sankcje to większa siła oddziaływania prawa

**Nowe rozporządzenie wprowadza bardzo surowe kary.** 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. Każdy przypadek będzie musiał być indywidualnie rozpatrzony przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO), który weźmie pod uwagę m.in.:

- **skalę naruszenia,**
- **umyślność działań,**
- **co zrobiono, żeby zminimalizować szkody poniesione przez osoby, których dane dotyczą,**
- **„recydywę", czyli czy to pierwsze, czy kolejne przewinienie,**
- **kategorie danych osobowych,**
- **stopień współpracy z GIODO.**

Obecne kary za nieprzestrzeganie przepisów są względnie niskie. Aby doszło do nałożenia grzywny, trzeba uparcie nie przywracać „stanu zgodnego z prawem", czyli nie stosować się do decyzji wydanej przez GIODO. W przepisach o ochronie danych osobowych istnieją jeszcze kary (w tym grzywny) wynikające z kodeksu karnego. Statystyki pokazują jednak, że zawiadomienia o podejrzeniu popełnienia przestępstwa należą do rzadkości, a jeśli już się zdarzają, postępowanie sądowe bardzo często jest umarzane ze względu na niską szkodliwość społeczną przewinienia. To dość wygodna sytuacja dla wielu administratorów danych, którzy często dochodzą do wniosku, iż korzyści z nieprzestrzegania przepisów z zakresu ochrony danych osobowych są zdecydowanie większe niż możliwe negatywne ich konsekwencje. Trzeba pamiętać, że w obecnym stanie prawnym GIODO nie może nakładać kar za niezgodność z przepisami, a może jedynie nakazać zapewnienie z nimi zgodności, a za uparte nie przywracanie „stanu zgodnego z prawem" wszcząć postępowanie egzekucyjne. Należy też podkreślić, że grzywna, czy ograniczenie lub pozbawienie wolności określone w art. 49 do art. 54a ustawy o ochronie danych osobowych mogły zostać nałożone wyłącznie w drodze postępowania sądowego. Nowe przepisy to zmieniają – teraz główny nacisk postawiono na kary finansowe, w których wszystko będzie zależeć od decyzji GIODO.[12] Przedsiębiorcy, którzy wcześniej mieli większy „apetyt na ryzyko", zmuszeni zostaną do ponownej jego kalkulacji. Można założyć, że wysokie kary zmotywują organizacje do przykładania większej wagi i respektowania przepisów o ochronie danych osobowych, a także – co za tym idzie – do inwestycji w bezpieczeństwo i ochronę informacji. Organizacje będą musiały zastanowić się nad zwiększeniem budżetów na rozwiązania informatyczne m.in. takie jak :

- **systemy monitorowania zdarzeń w systemach informatycznych (SIEM – Security Information and Event Management),**

*12. Nie do końca wiadomo, czy i jakie kary w postaci ograniczenia lub pozbawienia wolności będą stosowane za niestosowanie się do przepisów o ochronie danych osobowych.*

- **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 organizacjach zapewne trzeba będzie rozbudować zespoły bezpieczeństwa informacji i zarządzania incydentami. Konieczne będzie wdrożenie i przetestowanie procedur postępowania w sytuacjach kryzysowych, np. w przypadku wycieku danych. To o tyle ważne, że do ustalenia wysokości kary GIODO będzie brał pod uwagę wiele czynników, m.in. sposób, w jaki dane były zabezpieczone na poziomie technicznym lub organizacyjnym. Gdy o sankcjach mowa, trzeba pamiętać, że *osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów Rozporządzenia ma prawo do uzyskania od administratora lub procesora odszkodowania za poniesioną szkodę* (art. 82 Rozporządzenia).

## 7 - Kompleksowa współpraca organów

**Międzynarodowe organizacje, które działają na terenie wielu państw Unii Europejskiej, będą mogły załatwić wszystkie formalności w jednym punkcie, przy pomocy tzw. organu wiodącego.** *Organem wiodącym powinien być organ nadzorczy głównej jednostki organizacyjnej administratora lub podmiotu przetwarzającego lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego. Powinien on współpracować z innymi organami, których sprawa dotyczy (…)* W preambule Rozporządzenia (w różnych jej częściach) dowiadujemy się:

**(Motyw 130)** ***Jeżeli organ nadzorczy, do którego wniesiono skargę, nie jest wiodącym organem nadzorczym, wiodący organ nadzorczy powinien ściśle współpracować z organem nadzorczym, do którego wniesiono skargę.***

**(Motyw 133)** ***Organy nadzorcze powinny się wzajemnie wspierać w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie niniejszego rozporządzenia na rynku wewnętrznym.***

**(Motyw 105)** ***Należy ustanowić mechanizm spójności na potrzeby współpracy między organami nadzorczymi. Mechanizm ten powinien mieć zastosowanie w szczególności wtedy, gdy organ nadzorczy zamierza przyjąć środek mający wywoływać skutki prawne w odniesieniu do operacji przetwarzania, które znacznie wpływają na istotną liczbę osób, których dane dotyczą w kilku państwach członkowskich.***

**(Motyw 141)** ***Każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka ochrony prawnej przed sądem, (…) w szczególności w państwie członkowskim, w którym ma miejsce zwykłego pobytu (...)***

Zmiana bez wątpienia będzie korzystna dla grup kapitałowych, czy też przedsiębiorstw prowadzących biznes międzynarodowy, a także dla samych osób fizycznych, których dane dotyczą. Mniejsze przedsiębiorstwa mogą uznać tę zmianę za neutralną ze względu na brak wpływu na ich działalność.

## 8 - Nowe obowiązki i ograniczenia procesorów

**Ustawodawca w unijnym Rozporządzeniu wprowadził szereg nowych regulacji dla procesora, czyli podmiotu przetwarzającego dane w imieniu administratora danych. Nie wolno powierzać dalej przetwarzania danych osobowych bez zgody administratora.** *Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian*. **Podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu administratora. Podmiot przetwarzający (procesor) w razie stwierdzenia, iż doszło do naruszenia ochrony danych osobowych, zgłasza je administratorowi** (art. 33 ust. 2 Rozporządzenia). Już wcześniej umowa z podmiotem przetwarzającym dane osobowe w imieniu administratora (procesorem) musiała być zawarta na piśmie (art. 31 ust. 1 ustawy o ochronie danych osobowych). Rozporządzenie uzupełnia, że taka umowa może też zostać uregulowana innym instrumentem prawnym. Podmiot przetwarzający musi zgłaszać wszystkie naruszenia ochrony danych osobowych administratorowi. Obowiązkiem podmiotu przetwarzającego będzie prowadzenie rejestru wszelkich kategorii czynności przetwarzania, dokonywanych w imieniu administratora. Procesor będzie miał również obowiązek udostępnić taki rejestr na żądanie GIODO, a także powołać inspektora ochrony danych osobowych, jeśli zaistnieje przynajmniej jeden z czynników, o których stanowi art. 37 ust. 1 Rozporządzenia. Ten rodzaj zmian można ocenić jako negatywny dla przedsiębiorców. Jednak na plus warto zaliczyć fakt dokładnego sprecyzowania obowiązków wszystkich stron. Wcześniej takie zobowiązania trzeba było formułować samodzielnie. Na pochwałę zasługuje też fakt, że Rozporządzenie wskazuje: *jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.* Oznacza to przykładowo, że jeśli dane powierzy się agentowi oferującemu ubezpieczenia, a on postanowi zmienić pierwotny cel przetwarzania i wykorzysta te dane osobowe, żeby zaoferować konsumentom inne produkty i usługi, automatycznie stanie się administratorem tych danych. Taki stan już wcześniej obowiązywał, ale nie jako bezpośredni zapis prawny, ale efekt interpretacji przepisów. To kolejny dowód na to, że Rozporządzenie zostało napisane przystępnym językiem i w taki sposób, aby wyjaśniać i regulować kwestie niejasne i wymagające wcześniej interpretacji.

## 9 - Współadministratorzy i grupy przedsiębiorstw

W Rozporządzeniu pojawiają się nowe definicje: współadministratorów oraz grup przedsiębiorstw. *Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych osobowych, są oni współadministratorami. W drodze wspólnych uzgodnień w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.* Grupa przedsiębiorstw oznacza *przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane.* Wcześniej współadministratorzy mieli te same prawa i obowiązki, a więc tak naprawdę każdy z nich był odrębnym administratorem. Rozporządzenie pozwala podzielić się prawami i obowiązkami, ale osoby, których dane się przetwarza, należy poinformować, kto i za co dokładnie odpowiada. Stanowi o tym art. 26 ust. 2 Rozporządzenia: *zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.* Grupy przedsiębiorstw pojawiają się także przy kwestiach dotyczących tzw. wiążących reguł korporacyjnych, ułatwiających międzynarodowe transfery danych między przedsiębiorstwami w ramach grupy. Wspomniane reguły to *polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, który posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu lub przekazywaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą* (art. 4 pkt 20 Rozporządzenia).

## 10 - Inspektor ochrony danych zamiast administratora bezpieczeństwa informacji

Rozporządzenie zastępuje administratora bezpieczeństwa informacji inspektorem ochrony danych. Zmiana polega nie tylko na nowym „tytule". Zmieniają się także znacząco wymagania, jakie ma spełniać i sytuacje, w których należy go powołać. Inspektora ochrony danych należy wyznaczyć w przypadku, gdy:

- **przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w ramach sprawowania przez nie wymiaru sprawiedliwości, albo**
- **główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych na dużą skalę, albo**
- **główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę danych osobowych szczególnych kategorii, o których mowa w art. 9 ust. 1,**

Należy zwrócić uwagę na to, że także zleceniobiorcy (podmioty przetwarzające) będą musieli wyznaczać inspektora ochrony

danych, w przypadku zaistnienia jednego z powyższych czynników. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy. Informacje o sposobie kontaktu z inspektorem podaje się podczas zbierania danych osobowych. Rozporządzenie określa, że osoby, których dane się przetwarza, mogą kontaktować się z inspektorem ochrony danych *we wszystkich sprawach związanych z przetwarzaniem ich danych oraz z korzystaniem z praw przysługujących im na mocy niniejszego rozporządzenia.* Trzeba pamiętać, że tam, gdzie inspektor będzie powołany, osoby, których dane się przetwarza, będą mogły się z nim bezpośrednio kontaktować. Jego dane będą więc musiały znaleźć się na formularzach zgody. Rozporządzenie nie wskazuje, jakie dane kontaktowe inspektora trzeba będzie podać. Wydaje się jednak, iż wystarczy bezpośredni adres mailowy. Inspektora ochrony danych należy zaangażować, dokonując oceny skutków przetwarzania danych, o której mowa w art. 35 ust. 1 Rozporządzenia (np. gdy przetwarza się szczególne kategorie danych na dużą skalę), oczywiście, jeżeli został on wyznaczony. Niestety, mimo że Rozporządzenie podaje, kiedy powołać inspektora ochrony danych, nie do końca jasne są rzeczywiste sytuacje, kiedy to ma nastąpić. Przykładowo, według Rozporządzenia konieczność taka zachodzi wtedy, gdy główna działalność administratora polega na przetwarzaniu danych osobowych szczególnych kategorii. Ale gdzie znajduje się granica dla pojęcia „główna działalność"? Kto będzie to oceniał? Czy przetwarzanie danych osób zatrudnionych będzie można już uznać za operacje przetwarzania, które – ze względu na swój charakter, zakres i cele – wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą? Za naruszenie przez administratora obowiązku wyznaczenia inspektora ochrony danych Rozporządzenie wprowadza karę w wysokości do 10 mln EUR, a w przypadku przedsiębiorstwa – do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Dla funkcjonowania biznesu zmiana ta jest więc wyjątkowo istotna, choć niekorzystna. Dzisiaj powołanie ABI jest w pełni dobrowolne, dlatego wprowadzenie obowiązku powołania inspektora ochrony danych to dodatkowy obowiązek dla przedsiębiorstw i organizacji. Nowością jest konieczność powołania inspektora także przez procesora, czyli podmiot przetwarzający. Pojawiają się też jednak ułatwienia. Grupa przedsiębiorstw będzie mogła powołać jednego inspektora ochrony danych pod warunkiem, że *z każdej siedziby będzie można się z nim łatwo skontaktować.* Inspektor może być pracownikiem lub wykonywać zadania na podstawie umowy o świadczenie usług. Trzeba jednak podkreślić, że w każdym przypadku należy zapewnić mu zasoby *niezbędne do podtrzymania jego wiedzy fachowej.* To bez wątpienia dobra nowina dla inspektorów (w końcu ktoś podkreślił wyraźnie, że muszą się rozwijać zawodowo), a mniej dobra dla administratorów – teraz będą musieli uwzględnić plany rozwoju inspektorów i znaleźć na nie środki finansowe. Wedle nowych przepisów, inspektor ma być zaangażowany we wszystkie sprawy związane z ochroną danych osobowych. Ma mieć odpowiednie zasoby do wykonywania pracy, której wyniki raportuje do najwyższego kierownictwa. Może wykonywać inne obowiązki, o ile nie powodują konfliktu interesów.

## 11 - Ochrona prywatności (Projektowanie od podstaw i domyślność)

**Ochrona danych ma być wbudowywana w politykę przedsiębiorstwa już na etapie projektowania systemu ochrony danych osobowych** (by design), a także ma być aktywna domyślnie (by default), czyli bez konieczności podejmowania działań przez osoby, których dane dotyczą. W preambule (motyw 78) czytamy, że: *administrator 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.* Co więcej, zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych. Wywiązywanie się z tych obowiązków można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji, określonego w art. 42 Rozporządzenia. Co ciekawe, już wcześniej mówiło się o koncepcie *privacy by design,* ale skoro prawo dotyczy ochrony danych osobowych, a prywatność to szersze pojęcie, przemianowano go później na *data protection by design and by default* – w polskiej wersji przetłumaczone jako *uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych* (art. 25). Kwestia tak pojętej domyślności ochrony danych funkcjonuje już gdzieniegdzie w praktyce. Przykładowo, producenci domowych routerów sieci bezprzewodowej nie ustalają już takich samych haseł dla każdego urządzenia, ponieważ użytkownicy często korzystali z ustawień domyślnych. Ułatwiało to dostęp do sieci, a przez to też do informacji prywatnych, osobom nieupoważnionym. Teraz przyszedł czas na dane osobowe. Domyślną ochronę danych osobowych można łatwo zobrazować przykładem z serwisów społecznościowych. Każdy nowy post, który tam umieszczamy, powinien być z założenia niewidoczny. Dopiero użytkownik sam powinien móc każdorazowo zmieniać ustawienia prywatności, decydując się np. na widoczność tylko dla znajomych, czy dla wszystkich osób. Co ta zmiana w przepisach oznacza dla przedsiębiorców? Bez wątpienia ostrożniej należałoby projektować nowe produkty czy usługi. Bardzo ważnym elementem jest tu technologia komputerowa – zwłaszcza programiści powinni być świadomi nowych regulacji. Za naruszenie przez administratora lub podmiot przetwarzający obowiązku uwzględniania ochrony danych osobowych w fazie projektowania i ustanawiania mechanizmów ochrony domyślnej Rozporządzenie wprowadza administracyjną karę pieniężną w wysokości do 10 mln EUR, a w przypadku przedsiębiorstwa – do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

## 12 - Ocena skutków przetwarzania danych

Art. 35 ust. 1 Rozporządzenia określa, że **jeżeli dany rodzaj przetwarzania danych – zwłaszcza z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym**


**prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.** Oceny skutków trzeba będzie dokonywać zawsze, kiedy:

- **stosuje się profilowanie,**
- **przetwarza się dane szczególnej kategorii na dużą skalę,**
- **monitoruje się na dużą skalę miejsca publiczne,**
- **przetwarza się dane określone przez GIODO na mocy art. 35 ust. 4 jako podlegające wymogowi dokonania oceny skutków pod kątem ochrony danych.**

Organizacje i przedsiębiorcy powinni konsultować się z GIODO, *jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka* (…). (art. 36 ust. 1) Dokonanie oceny skutków wymagać będzie zaangażowania inspektora ochrony danych, jeśli został powołany. Jeśli nie, jest mało prawdopodobne, żeby przedsiębiorca, który nie posiada specjalistycznej wiedzy eksperckiej, sam dokonał odpowiedniej analizy skutków przetwarzania danych. Na taką ocenę, powinny się składać m.in.:

- **systematyczny opis planowanych operacji przetwarzania i ich celów,**
- **ocena proporcjonalności operacji przetwarzania w stosunku do celów,**
- **ocena zagrożenia dla praw i wolności osób,**
- **ocena środków mających zmniejszyć zagrożenia i chronić dane osobowe.**

Co więcej, *w stosownym przypadku administrator zasięga opinii osób, których dane dotyczą lub ich przedstawicieli w sprawie zamierzonego przetwarzania.* Zaś jeśli ocena skutków wskaże, że *przetwarzanie niosłoby duże zagrożenie, gdyby administrator nie przedsięwziął środków w celu zminimalizowania tego zagrożenia, to przed przetworzeniem danych osobowych administrator konsultuje się z organem nadzorczym.* Oznacza to, że zawsze w razie wątpliwości warto skonsultować się z GIODO. Za naruszenie przez administratora obowiązku dokonania oceny skutków przetwarzania danych Rozporządzenie wprowadza karę w wysokości do 10 mln EUR, a w przypadku przedsiębiorstwa – do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Bez wątpienia niezbędne będzie przygotowanie się przedsiębiorców do tego, w jaki sposób dokonywać oceny skutków. Czy będą to jakieś szablony? Formularze? W jaki sposób GIODO będzie w tę działalność zaangażowany? Te kwestie na razie wydają się niejasne, bo o ile całe rozporządzenie jest względnie zrozumiałe, ta jego część jest wyjątkowo enigmatyczna.

## 13 - Raportowanie naruszenia bezpieczeństwa danych do GIODO

Przez *naruszenie ochrony danych osobowych* należy rozumieć *naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.* Takim zdarzeniom poświęcony jest art. 33 Rozporządzenia. **W sytuacji, w której naruszenie ochrony danych osobowych prawdopodobnie będzie skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, zgłasza się je do GIODO bez zbędnej zwłoki – ale nie później niż w ciągu 72 godzin (3 dni).** W ust. 5 omawianego przepisu ustanowiono obowiązek prowadzenia przez administratora danych dokumentacji wszelkich naruszeń ochrony danych osobowych. Oznacza to, że nawet jeśli administrator danych osobowych nie ma obowiązku poinformowania GIODO o konkretnym negatywnym zdarzeniu, musi i tak je odnotować we własnym rejestrze. **W sytuacji, w której przed-**

**miotowe naruszenie niesie wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator powinien również bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o takim naruszeniu – jasnym i prostym językiem** (art. 34 ust. 1 i 2 Rozporządzenia). Należy jednak pamiętać, **iż sposób, w jaki organ nadzorczy dowiedział się o naruszeniu,** w szczególności, czy i w jakim stopniu administrator danych lub podmiot przetwarzający zgłosili naruszenie, będzie brany pod uwagę przez organ nadzorczy przy ustalaniu wysokości ewentualnej kary finansowej. Raportowanie incydentów związanych z naruszeniami danych osobowych nie jest wcale nowe. Przepisy polskiego prawa nakazują np. zgłaszanie takich naruszeń operatorom telekomunikacyjnym. Według prawa telekomunikacyjnego (Dz. U. Nr 171, poz. 1800 z późn. zm.), w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych przedsiębiorca telekomunikacyjny ma obowiązek powiadomić o tym zdarzeniu GIODO, a także (w niektórych sytuacjach) abonenta lub użytkownika końcowego. W preambule Rozporządzenia (motyw 87) czytamy, że *należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych*. Nie bardzo wiadomo, co należy przez tę deklarację rozumieć. Być może takie przepisy będą uzupełniane przez dokładną interpretację GIODO. Możliwe też, że konieczne stanie się wdrażanie rozwiązań, pozwalających dokładnie monitorować stan bezpieczeństwa, takich jak systemy klasy SIEM. Jak biznes może się przygotować do tych nowych wymagań? Na pewno konieczne będzie przygotowanie planów awaryjnych, które pozwolą sprawnie zareagować w przypadku incydentu. Większe organizacje, które już dzisiaj doceniają konieczność zarządzania ciągłością działania, będą mieć ułatwione zadanie. Trzeba pamiętać, że informowanie o naruszeniu bezpieczeństwa, szczególnie wszystkich klientów, może być bardzo kosztowne, zarówno operacyjnie, jak i wizerunkowo. Dlatego warto dołożyć starań, aby zmniejszyć ryzyko zagubienia urządzeń z danymi osobowymi czy w ogóle wycieków danych. Z tym zaś wiąże się konieczność wdrożenia rozmaitych zabezpieczeń technicznych i organizacyjnych. Można śmiało powiedzieć, iż w świetle nowych przepisów organizacje będą musiały uwzględnić większy budżet na wdrożenie mechanizmów zabezpieczenia danych osobowych niż dotychczas. Pamiętajmy, że jeśli zostanie wykazane, iż do naruszenia doszło z rażącego zaniedbania administratora czy podmiotu przetwarzającego, można liczyć się z ryzykiem nałożenia administracyjnych kar finansowych (art. 83 Rozporządzenia).

## 14 - Pseudonimizacja danych

Rozporządzenie wprowadza pojęcie pseudonimizacji danych, które oznacza *przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.* W preambule (motyw 26) wskazano, *iż spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej.* Dodatkowo, ustawodawca wskazał w treści Rozporządzenia pseudonimizację jako przykład jednego z mechanizmów, mających za zadanie zapewnić taki stopień bezpieczeństwa danych, który odpowiada ryzyku ich naruszenia (art. 32 ust. 1 lit. a). Przykład danych pseudonimizowanych to stosowanie wewnętrznego numeru klienta zamiast jego danych osobowych. Nawet jeśli doszłoby do wycieku takich informacji jak np. ID 129871 = wynagrodzenie 3400zł, osoba nieupoważniona niewiele by się z nich dowiedziała. Cóż bowiem znaczyłaby dla niej informacja, że ktoś o numerze identyfikacyjnym 129871 zarabia 3400 zł? Okazuje się więc, że zastosowanie danych pseudonimizowanych zmniejsza możliwość naruszenia bezpieczeństwa informacji. Warto zwrócić uwagę, że Rozporządzenie zauważa też dane anonimowe już w samej preambule (motyw 26). Czytamy w niej, że: *zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Niniejsze rozporządzenie nie dotyczy więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych.* Opisaną wyżej zmianę należy uznać za pozytywną. Wcześniej prawo nie zauważało danych pseudoanonimowych, a GIODO czasem uznawał je za dane osobowe, a czasem nie. Nie było wiadomo, jak należy postępować. Teraz to się zmieni.

## 15 - Retencja i usuwanie danych

Rozporządzenie bardzo mocno podkreśla wagę retencji danych. Przykładowo podczas zbierania danych należy podać *okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.* Do tej pory konieczność podawania takich informacji nie pojawiała się w przepisach. Dalej przepisy stanowią, że *podmiot przetwarzający dane po zakończeniu świadczenia usług przetwarzania danych, zależnie od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują mu je przechowywać.* Jeśli mamy zacząć zbierać dane osobowe, wcześniej należy ustalić, jak długo dane będą przechowywane, a gdy nie jest to możliwe, przynajmniej określić kryteria ustalania tego okresu. Mimo, iż może się to wydawać utrudnieniem, tak naprawdę stanowi ułatwienie. Do tej pory organizacje często zapominały o konieczności usuwania danych, dowiadując się o takim obowiązku dopiero podczas kontroli GIODO (wynikającym z art. 26. ust.1 pkt 4 ustawy o ochronie danych osobowych) i próbując w pośpiechu wdrożyć mechanizmy ich usuwania. Teraz, w świetle nowych przepisów, nie da się o tym „zapomnieć". Natomiast mniej korzystne jest to, że należy informować osoby o tym, kiedy ich dane będą usunięte, a jeśli nie jest to możliwe, trzeba podać, jakie są warunki obliczania terminu usunięcia danych. Jedną z nowych zasad przetwarzania danych osobowych wskazanych w Rozporządzeniu jest prawo do usunięcia danych (nazywane „prawem do zapomnienia"), które określa kiedy dane osobowe należy usuwać. Art. 17 Rozporządzenia[13] podkreśla, *że osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe.*

Dane osobowe należy usunąć wtedy, kiedy m.in:

- **cel przetwarzania się skończył,**
- **zgoda została wycofana,**
- **dane są zebrane wbrew prawu.**

## 16 - Rejestr czynności przetwarzania

**Zamiast rejestrowania zbiorów w GIODO, administrator danych osobowych będzie musiał prowadzić rejestr czynności przetwarzania danych osobowych.** Obowiązek ten będzie także spoczywać na podmiotach przetwarzających (procesorach) – co jest absolutną nowością. W preambule (motyw 98) podkreśla się: *Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten powoduje jednak obciążenia administracyjne i finansowe, i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je skutecznymi procedurami i mechanizmami, koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą nieść duże zagrożenie dla praw i wolności osób fizycznych.* Rozporządzenie wskazuje, iż rejestr powinien być prowadzony w formie pisemnej, w tym w formie elektronicznej. Rejestr przetwarzania ma zawierać m.in. następujące kategorie informacji:

- **informacje o administratorze i ew. współadministratorach,**
- **dane inspektora ochrony danych,**
- **opis celów przetwarzania,**
- **kategorie osób, których dane się przetwarza,**
- **kategorie danych osobowych,**
- **informacje o odbiorcach (także w państwach trzecich),**
- **planowane terminy usuwania poszczególnych kategorii danych,**
- **opis środków bezpieczeństwa.**

Rozporządzenie zwalnia z obowiązku prowadzenia rejestru w sytuacji, gdy dana organizacja zatrudnia mniej niż 250 osób. Jest jednak od tego wyjątek: taki rejestr musi być prowadzony, jeśli przetwarzanie danych w organizacji może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, przetwarzanie nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa. Zmiana ta jest neutralna, dlatego że wysiłek, który przedsiębiorstwa i organizacje będą musiały włożyć w prowadzenie dokumentacji, można uznać za porównywalny z dotychczasowym obowiązkiem rejestracji (i aktualizacji) zbiorów danych osobowych. Za naruszenie przez administratora obowiązku rejestracji czynności przetwarzania Rozporządzenie wprowadza karę w wysokości do 10 mln EUR lub 2% całkowitego rocznego światowego obrotu przedsiębiorstwa.

## 17 - Większa wiarygodność podmiotów certyfikowanych

**Rozporządzenie wprowadza kodeksy postępowania i certyfikaty, które będą podnosić wiarygodność podmiotów przetwarzających dane osobowe.** W preambule określa się (motyw 100), że *aby zwiększyć przejrzystość i poprawić przestrzeganie niniejszego Rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz*

*13. Konstrukcja zapisu w postaci „osoba (…) ma prawo żądania (…) a administrator ma obowiązek (…)" sugeruje, że chodzi o usuwanie danych wyłącznie w sytuacji gdy występuje żądanie. Należy jednak pamiętać, że nie wolno danych przetwarzać, jeśli nie są potrzebne do osiągnięcia celów przetwarzania, zostały zebrane niezgodnie z prawem, czy też zgoda została wycofana i nie ma żadnych innych przesłanek legalności do przetwarzania tych danych.*

*do wprowadzenia znaków jakości i oznaczeń w dziedzinie ochrony danych, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić poziom ochrony danych, której podlegają stosowne produkty i usługi.* Art. 24 ust. 3 Rozporządzenia wyraźnie podkreśla, czemu te mechanizmy i oznaczenia mają służyć: *stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element stwierdzenia przez administratora ciążących na nim obowiązków.* Posiadanie kodeksów czy certyfikatów znacznie ułatwia też przekazywanie danych osobowych do państw trzecich. Absolutną nowością w sferze ochrony danych osobowych jest certyfikacja na mocy art. 42 Rozporządzenia. Może ona posłużyć także do wykazania przez administratora wywiązywania się z obowiązku uwzględniania ochrony danych w fazie projektowania oraz wdrażania mechanizmów domyślnej ochrony danych (art. 25 ust. 3 Rozporządzenia). Posiadanie zatwierdzonych kodeksów postępowania lub certyfikatów, o których mowa w Rozporządzeniu, może znacząco ułatwić przedsiębiorcom udowodnienie, iż wdrożyli wymagane przepisami mechanizmy ochrony danych osobowych. Wydaje się, że pomoże to również pozytywnie wpłynąć na klientów, którzy chętniej będą wybierać podmioty certyfikowane, jako te bardziej godne zaufania.

## 18 - Przekazywanie danych do państw trzecich

Postępująca globalizacja gospodarki światowej oznacza wzrost wymiany danych osobowych do państw trzecich lub organizacji międzynarodowych. Tą kwestią w całości zajmuje się rozdział V Rozporządzenia. Dowiadujemy się m.in., że przekazywanie danych osobowych do państwa trzeciego będzie mogło nastąpić na podstawie m.in:

- **wydanej przez Komisję Europejską decyzji stwierdzającej, iż dane państwo trzecie zapewnia odpowiedni stopień ochrony danych osobowych,**
- **zatwierdzonych przez właściwy organ nadzorczy (w Polsce – GIODO) wiążących reguł korporacyjnych,**
- **standardowych klauzul ochrony danych przyjętych przez Komisję Europejską,**
- **standardowych klauzul ochrony danych przyjętych przez organ nadzorczy (w Polsce – GIODO) i zatwierdzonych przez Komisję Europejską,**
- **zatwierdzonego kodeksu postępowania,**
- **zatwierdzonego mechanizmu certyfikacji.**

**Wymiana danych na podstawie wiążących reguł korporacyjnych albo z użyciem standardowych klauzul umownych będzie więc znacznie ułatwiona.** *Wiążące reguły korporacyjne to polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego Unii, przy jednorazowym lub wielokrotnym przekazaniu lub przekazywaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą.* Wciąż aktualne pozostaje przekazywanie danych na podstawie decyzji stwierdzającej odpowiedni poziom ich ochrony. **Możliwe będzie przekazywanie danych osobowych do podmiotu, który stosuje kodeks postępowania bądź posiada odpowiedni certyfikat.** Ma to się dziać *na podstawie zatwierdzonego kodeksu postępowania opartego na art. 40 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich gwarancji, w tym w odniesieniu do praw osób, których dane dotyczą;* lub zatwierdzonego mechanizmu certyfikacji opartego na art. 42 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. Zmiany w tym obszarze są w zasadzie kosmetyczne. To przede wszystkim harmonizacja prawa, na którą już wcześniej zostaliśmy przygotowani przez nowelizację polskiej ustawy o ochronie danych osobowych. Rozporządzenie wprowadza kodeksy postępowania i certyfikacji, uznawane jako odpowiednie gwarancje. Małą, choć uciążliwą zmianą, będzie ograniczone przekazywanie danych do państw trzecich na podstawie zgody. Według nowych przepisów, aby osoba, której dane dotyczą (czyli osoba fizyczna, najczęściej konsument) mogła wyrazić zgodę na przekazanie danych, musi wcześniej zostać poinformowana o ewentualnych zagrożeniach, wynikających z przetwarzania danych osobowych na terenie takiego państwa.

## 19 - Szerszy katalog danych szczególnej kategorii

**Tzw. dane wrażliwe, które w poprzednich przepisach nie miały własnej nazwy, zostały w nowych przepisach określone jako dane szczególnej kategorii i zostały poszerzone o dane biometryczne.** Dodatkowo, do tego katalogu Rozporządzenie dołącza też dane genetyczne. Już w polskiej ustawie dane o kodzie genetycznym uznawano za wrażliwe. Określenie to było jednak niefortunne, na co zwróciła uwagę unijna doktryna. Sam kod genetyczny jest bowiem uniwersalny dla całego świata ożywionego. W genetyce uznaje się, że kod genetyczny to nic innego jak odnalezienie sposobu odczytania informacji genetycznej. Stąd postulowano o wprowadzenie bardziej precyzyjnego sformułowania – dane genetyczne – na co ustawodawca przystał. Zgodnie z treścią art. 9 ust. 1 Rozporządzenia zabrania się przetwarzania danych osobowych ujawniających:

- **pochodzenie rasowe lub etniczne,**
- **poglądy polityczne,**
- **przekonania religijne lub światopoglądowe,**
- **przynależność do związków zawodowych;**

a także przetwarzania:

- **danych genetycznych,**
- **danych biometrycznych,**

w celu jednoznacznego zidentyfikowania osoby;
albo:

- **danych dotyczących zdrowia,**
- **seksualności i orientacji seksualnej.**

**Dane o skazaniach, w tym dane o niekaralności, można przetwarzać wyłącznie pod nadzorem.** Art. 10 mówi o tym, że *przetwarzania da-*


*nych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii 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.* Zupełną nowością jest włączenie do kategorii danych wrażliwych danych biometrycznych. Wcześniej były one uznane za dane zwykłe, a wszelkie ich ograniczenia miały charakter indywidualnych decyzji GIODO. Biometrię potocznie kojarzy się z odciskami palców bądź ze skanowaniem siatkówki lub tęczówki oka. Ta szeroka dziedzina nauki zajmuje się pomiarami istot żywych w celu określenia ich indywidualnych cech. Bada wszystko, co pozwala na identyfikowanie indywidualnych cech, wśród których znaleźć można m.in.:

- **owal twarzy, rozkład punktów charakterystycznych (oczy, usta) lub temperatur na twarzy,**
- **geometria (kształt) ucha,**
- **układ naczyń krwionośnych na dłoni lub przegubie ręki,**
- **kształt linii zgięcia wnętrza dłoni,**
- **układ linii papilarnych.**

Biometria interesuje się także cechami behawioralnymi, związanymi z zachowaniem, takimi jak:

- **sposób chodzenia,**
- **podpis odręczny,**
- **sposób pisania na klawiaturze,**
- **cechy charakterystyczne ruchu ust i poruszania gałki ocznej.**

Analiza danych biometrycznych wykorzystywana jest głównie w takich dziedzinach jak: weryfikacja tożsamości, autoryzacja dostępu do systemów informatycznych czy identyfikacja. Tutaj Rozporządzenie ma istotne znaczenie, ponieważ z pewnością utrudni korzystanie czy wdrażanie tego rodzaju systemów. Do tej pory zasady przetwarzania danych biometrycznych były dość niejasne, ponieważ brakowało odpowiednich przepisów. Prób jakiejkolwiek regulacji podejmowało się GIODO i Grupa robocza art. 29, ale tak naprawdę, jeśli czegoś nie ma w prawie, to jakby nie istniało, więc w tym obszarze panowała duża dowolność.

## 20 - Zakres i sposób informowania osób, których dane dotyczą

**Obowiązek informacyjny, narzucony na administratora podczas zbierania danych, zostanie znacznie poszerzony.** Będzie trzeba więc informować o:

- **inspektorze ochrony danych,**
- **nazwie i danych kontaktowych przedstawiciela, jeżeli istnieje,**
- **podstawie prawnej przetwarzania,**
- **prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywa się przetwarzanie,**
- **informacji o zamiarze przekazywania danych do państwa trzeciego,**
- **okresie, przez który dane osobowe będą przechowywane, bądź kryteria ustalania tego okresu,**
- **profilowaniu,**
- **o prawie wniesienia skargi do organu nadzorczego,**
- **w przypadku istnienia obowiązku podania danych osobowych: wskazaniu ewentualnych konsekwencji niepodania danych,**
- **prawach osoby, której dane dotyczą, tj. prawie do:**
  - usunięcia danych,
  - ograniczenia przetwarzania,
  - prawie przenoszenia danych,
  - prawie do cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).

Jeśli pozyskujemy dane osobowe nie bezpośrednio od osoby, której dane dotyczą, obowiązek informacyjny poszerza się jeszcze o informację o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. Poszerza się również prawo do udzielenia informacji na żądanie. Rozporządzenie **narzuca obowiązek komunikowania się z osobami w sposób przyjazny, przystępnym i zrozumiałym językiem,** tak aby przekaz do nich kierowany można było odebrać i zrozumieć bez wysiłku. Preambuła Rozporządzenia (motyw 39) stanowi: *zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozu-*

*miałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz podawania innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących.* W motywie 58 zaś czytamy: *zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane.* Także art. 12 Rozporządzenia podkreśla to wyjątkowo dobitnie: *aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji* Administrator danych musi udzielić im informacji:

- **na piśmie, elektronicznie lub ustnie, jeżeli podmiot danych tego zażąda,**
- **w terminie jednego miesiąca od otrzymania wniosku,**
- **bezpłatnie.**

Ta zmiana może być kosztowna dla przedsiębiorców, gdyż oznaczać będzie wymianę wszelkich formularzy, zarówno tych papierowych, jak i elektronicznych, zawierających zgody na przetwarzanie danych osobowych. Rozbudowanie klauzuli informacyjnej przełoży się na nawet dwukrotne zwiększenie objętości obecnie istniejących formularzy. Dla organizacji może to oznaczać większe trudności przy pozyskiwaniu zgód na przetwarzanie danych osobowych. Już teraz przedsiębiorcy często podkreślają, że klienci narzekają na obszerność klauzul zgód na przetwarzanie danych osobowych.

## 21 - Ograniczenie profilowania

Przez „profilowanie" należy rozumieć *dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu tych danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.* Profilowanie, które polega na wykorzystywaniu danych osobowych do analizy lub prognozowania osobistych preferencji czy przyszłych zachowań klientów, jest procesem automatycznym, co wynika z definicji potwierdzonej dalej w art. 22 Rozporządzenia: *osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na niego wpływa. Należy jednak zwrócić uwagę, że ten zapis nie ma zastosowania, jeśli decyzja jest niezbędna do zawarcia lub wykonania umowy między podmiotem danych, a administratorem lub opiera się na wyraźnej zgodzie osoby. Przy automatycznym przetwarzaniu administrator wdraża właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania danej decyzji.* **Do profilowania co do zasady nie wolno używać danych wrażliwych,** chyba, że osoba, której dane dotyczą:

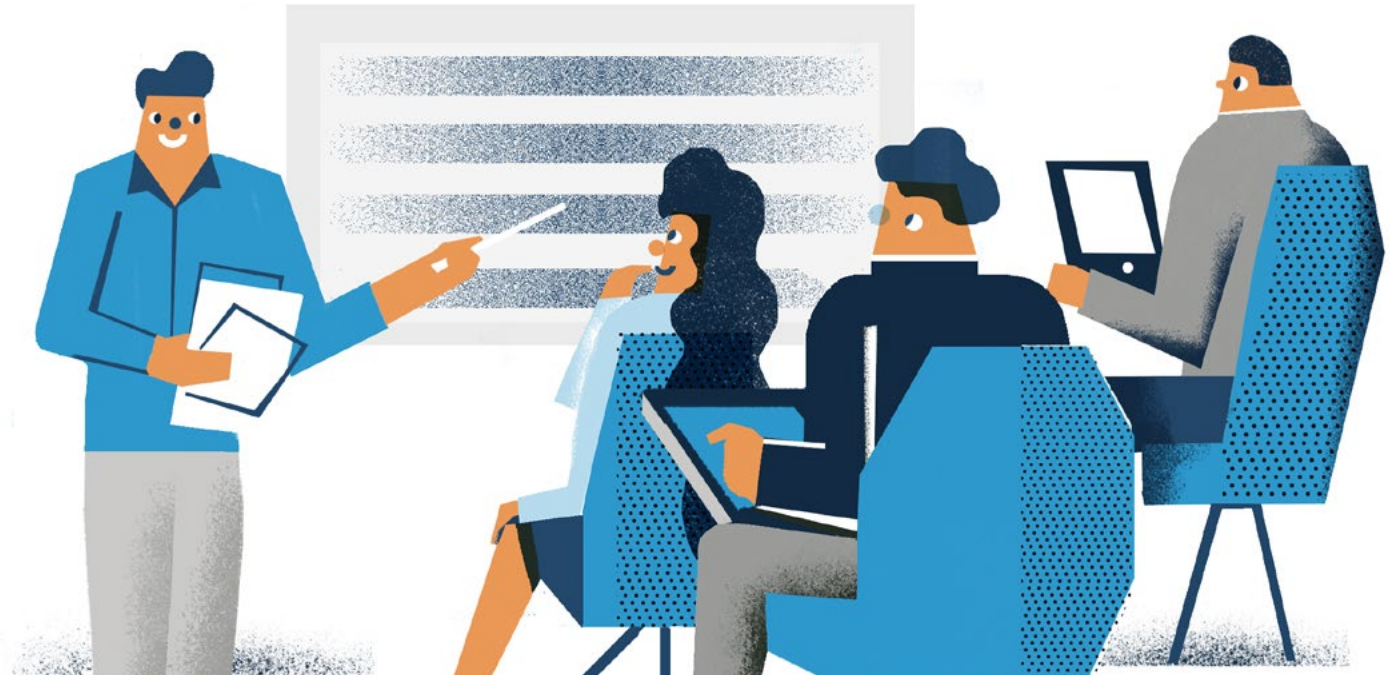
- **wyraziła na to zgodę,**
- **jest to podyktowane ważnym interesem publicznym.**

W Polsce pojęcie automatycznego przetwarzania danych obecne jest w obowiązującej ustawie o ochronie danych osobowych. Unijne Rozporządzenie uszczegółowiło cały proces i warunki, w jakich może do niego dochodzić. Jeżeli profilowanie odbywa się w celu marketingu bezpośredniego (który do tej pory stanowił w polskim prawie tzw. usprawiedliwiony prawnie cel przetwarzania, zaś Rozporządzenie określa go jako tzw. cel wynikający z uzasadnionych interesów administratora danych[14]), można zgłosić sprzeciw w związku z takim przetwarzaniem. Niekorzystny wpływ tej zmiany na funkcjonowanie przedsiębiorstw łagodzi możliwość korzystania z profilowania, o ile jest to niezbędne do zawarcia umowy – tak będzie zapewne w przypadku np. ubezpieczeń. O profilowaniu należy informować na etapie zbierania danych osobowych, a także na wniosek osoby fizycznej, której dane dotyczą. Spowoduje to z pewnością konieczność modyfikacji istniejących formularzy i pism dotyczących zbierania oraz przetwarzania danych osobowych.

## 22 - Doprecyzowane warunki uzyskiwania zgody na przetwarzanie danych osobowych, w tym danych osobowych dzieci

Rozporządzenie zgodę definiuje następująco: *to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.* W polskich przepisach, dotychczasowa definicja brzmiała następująco: *to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.* Jeśli dobrze przyjrzeć się obu definicjom, widać w nich wyraźne podobieństwa. Rozporządzenie podkreśla w preambule (motyw 32), że *zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście klarownie wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jego danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda*

14. *Ta zmiana bardzo cieszy autora tego poradnika, bo określanie marketingu bezpośredniego mianem czegoś prawnie usprawiedliwionego (a więc wynikającego z prawa) było nienaturalne.*



*powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma udzielić zgody w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.* Dalej czytamy, że (motyw 43): *zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą a administratorem, zwłaszcza gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgody udzielano dobrowolnie we wszystkich przypadkach.* W Polsce wprowadzenie rozszerzonej definicji zgody zmienia w zasadzie niewiele, ponieważ już wcześniej zgoda była przez istniejące przepisy zdefiniowania w podobny do Rozporządzenia sposób. Zauważalną zmianą jest zaakcentowanie w motywie 32 preambuły, że okienka zgody nie mogą być domyślnie zaznaczone. I dobrze, bo rzeczywiście nie wynikało to jednoznacznie z dotychczasowych przepisów prawa. Kolejną kwestią wyróżniającą nową definicję zgody jest pewna kategoria zachowań, określona jako wyraźne działanie potwierdzające. Oznacza to, że zgodę można wyrazić także poprzez działanie, a nie jedynie oświadczenie. Przykładowo, wręczenie wizytówki podczas spotkania bądź przesłanie aplikacji do potencjalnego pracodawcy może stanowić wyrażenie zgody na przetwarzanie danych. W świetle obecnie obowiązującego prawa takie czynności wymagały zgody, której zwyczajowo nie udzielało się, gdyż wydawało się to nienaturalne i niepotrzebne. Według nowych przepisów **zgodę na przetwarzanie danych osobowych przy świadczeniu usług społeczeństwa informacyjnego** (takich jak Facebook, poczta elektroniczna, gry w sieci czy sprzedaż internetowa) **może wyrazić dziecko, które ukończyło 16 lat,** w przeciwnym wypadku zgodę musi wyrazić zaaprobować lub wyrazić w jego imieniu osoba sprawująca władzę rodzicielską lub opiekę prawną. **Konieczne będą rozsądne starania, aby zweryfikować czy opiekun prawny dziecka rzeczywiście udzielił zgody lub ją zaaprobował.** Nowe przepisy podkreślają w preambule:

Motyw 38: ***Zgoda osoby sprawującej odpowiedzialność rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku.***

Motyw 58: ***Zważywszy, że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło go bez trudu zrozumieć.***

Z jednej strony, dotychczasowa niejasność przepisów mogła działać na korzyść przedsiębiorców. Podczas świadczenia usług społeczeństwa informacyjnego pojawiały się pewne wymogi wiekowe, na przykład w treści regulaminów, ale nie wydaje się, żeby przedsiębiorcy przykładali szczególną wagę do ich weryfikacji. Z drugiej strony, po wprowadzeniu nowych przepisów trzeba będzie podejmować racjonalne działania, żeby zweryfikować wiek użytkownika, uwzględniając dostępną technologię. Oznacza to, że częściej będzie dochodzić do zbierania dat urodzenia. W przypadku dziecka gromadzić będzie się informacje głównie o rodzicu lub opiekunie prawnym, tym bardziej, że administrator powinien wykazać fakt, że zebrane zgody są prawidłowe. Opisywana zmiana jest korzystna głównie dla obywateli, w tym przede wszystkim dzieci. Od przedsiębiorców zaś będzie wymagała analizy dotychczasowego podejścia do zbierania i weryfikowania danych. Warto dodać, że Rozporządzenie pozostawia wszystkim krajom prawo do wprowadzenia niższej granicy wiekowej (co najmniej 13 lat), poniżej której wymagana będzie zgoda rodzica/opiekuna.

## 23 - Prawo do przenoszenia danych

Art. 20 Rozporządzenia wskazuje, że *osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane innemu administratorowi bez przeszkód ze strony administratora, któremu dane te dostarczono.* Będzie to możliwe wtedy, kiedy:

- **przetwarzanie odbywa się w sposób zautomatyzowany**
- **dane przetwarza się na podstawie zgody osoby, której dane dotyczą lub w celu realizacji umowy, której stroną jest osoba, której dane dotyczą**

Ogólną zasadą jest to, że można przenosić takie dane, które przetwarzane są w pełni automatycznie i wyłącznie na podstawie zgody osoby, której dotyczą. Jednak nie jest do końca jasne, co należy rozumieć przez „w pełni automatyczne przetwarzanie"? Czy są to np. dane przetwarzane przez serwis aukcyjny Allegro? A może inne? Niezależnie od tych wątpliwości, tę zmianę przepisów uznać należy za niekorzystną dla przedsiębiorców. Teraz będą bowiem musieli odpowiednio zmodyfikować systemy, aby te były w stanie wygenerować dane do przeniesienia. Co więcej, można przypuszczać, iż osoby, których dane są przetwarzane, chętniej będą decydować się na migrację między administratorami/firmami.

## 24 - Rozszerzone prawo do usunięcia danych i ograniczenia przetwarzania

Usuwaniu danych poświęcono w Rozporządzeniu całą sekcję 3. Rozdziału III. W preambule (motyw 66) stwierdza się, że, *aby wzmocnić prawo do bycia zapomnianym w internecie, należy rozszerzyć prawo do usunięcia danych, poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe, o usunięciu wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji.* Art. 17. Rozporządzenia stanowi zaś: Osoba, której dane dotyczą, ma prawo żądania od administratora, aby dane zostały usunięte jeśli:

- **nie są już potrzebne do celu przetwarzania,**
- **zgoda na przetwarzanie została cofnięta,**
- **dane są przetwarzane niezgodnie z prawem,**
- **dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego,**
- **osoba, której dane dotyczą wnosi sprzeciw wobec przetwarzania,**
- **dane osobowe musza zostać usunięte ze względu na prawo Unii lub państwa członkowskiego, któremu podlega administrator.**

Uwagę zwraca **możliwość zażądania, aby usunięto dane zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.** Wedle nowych przepisów, jeśli administrator upublicznił dane osobowe, musi też podjąć *racjonalne działania, 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 lub ich replikację.* Widać więc **wyraźne wzmocnienie prawa do usunięcia danych upublicznionych.** Art. 18 Rozporządzenia podkreśla, że przetwarzanie danych osobowych można ograniczyć wyłącznie do przechowywania, jeśli osoba kwestionuje prawdziwość danych lub gdy cel przetwarzania wygasł, ale dane należy dalej przechowywać, na wypadek potencjalnych roszczeń. Prawo do usunięcia danych było wyjątkowo ciekawym tematem, o którym głośno dyskutowano przez ostatnie lata. Jeśli przyjrzeć się proponowanym rozwiązaniom prawnym, tak naprawdę pojawia się tu niewiele nowych elementów. Prawo do usunięcia danych było obecne i w polskiej ustawie o ochronie danych osobowych, jednak tam pojawiało się w wersji znacznie uproszczonej (art. 35 ustawy o ochronie danych osobowych). Rozporządzenie znacznie rozszerzyło zakres tych przepisów. Najciekawszą zmianą jest obowiązek informowania innych podmiotów przetwarzających dane, że osoba, której dane dotyczą, zawnioskowała o „bycie zapomnianym".

## Podsumowanie: Nowe rozporządzenie – dobre, czy złe?

Nowe rozporządzenie wprowadza szereg zmian w codziennym funkcjonowaniu organizacji i przedsiębiorstw, które mają do czynienia z przetwarzaniem danych osobowych. Ci, którzy zajmują się ochroną danych profesjonalnie, mogą powiedzieć, że to ewolucja, bo podstawy, na jakich opiera się cały system ochrony danych osobowych, nie ulegają zmianom. Jednakże dla administratorów danych osobowych, a także przeciętnego Kowalskiego, użytkownika sieci czy właściciela biznesu, nowe rozporządzenie europejskie jest po prostu rewolucją! Zmianom przyświecało kilka bardzo szczytnych celów, które miały uwzględnić postęp technologiczny oraz nowy sposób życia i prowadzenia biznesu w UE. Były to:

- **harmonizacja prawa,**
- **ułatwienie przepływu danych osobowych w Unii Europejskiej,**
- **uproszczenie funkcjonowania przedsiębiorstw.**

Najkorzystniejsze są zmiany dla międzynarodowego i globalnego biznesu, m.in. jeden punkt kontaktu (one-stop-shop) w sprawie międzynarodowego przetwarzania danych czy uniwersalne i jednorodne przepisy dla całej Unii. I ten kierunek zmian należy docenić. Małych przedsiębiorców ucieszy na pewno fakt, że rozporządzenie łagodniej traktuje mniejsze biznesy rozumiejąc, że przy małej skali przetwarzania danych wcześniejsze przepisy były dla nich zbyt wymagające. Miejmy nadzieję, że polski ustawodawca nie zmieni tej tendencji. Podsumowując – oto subiektywna ocena nowego prawa z punktu widzenia przedsiębiorcy:

- **zmiany korzystne – 9,**
- **zmiany negatywne – 11,**
- **zmiany neutralne – 4.**

Nikt na pewno nie spodziewał się, że nowe prawo będzie bardzo łagodne dla przedsiębiorców. Wśród wprowadzanych zmian jest jednak sporo plusów. Gdyby te przepisy oceniać tylko z perspektywy osób, których dane będą przetwarzane (np. konsumentów) – na pewno można by znaleźć ich więcej. Nie ma jednak co narzekać. Na pewno warto już dzisiaj zacząć się przygotowywać do zmian, planując nowe obowiązki i przygotowując budżet na najbliższe dwa lata, tak aby od 2018 r. bez problemów zapewnić swojej organizacji czy przedsiębiorstwu funkcjonowanie zgodnie z nowymi przepisami unijnymi. Poziom ochrony danych osobowych oraz bezpieczeństwo informacji na pewno na tym skorzysta.

# Notatki

POLECAMY

# „Unijna reforma przepisów ochrony danych osobowych – analiza zmian”

Książka opisuje najważniejsze zmiany jakie zajdą w przepisach ochrony danych osobowych po 25 maja 2018 r. Przedsiębiorcy do tego czasu muszą dostosować procesy przetwarzania danych osobowych poprzez sukcesywne wdrażanie wytycznych zawartych w ogólnym rozporządzeniu o ochronie danych. Książka ma ułatwić organizacjom zrozumienie głównych motywów i założeń nowych przepisów w celu ich jak najefektywniejszej implementacji w funkcjonujący u nich model przetwarzania danych. Publikacja skierowana jest do wszystkich przedsiębiorców, osób piastujących funkcję administratorów bezpieczeństwa informacji oraz osób odpowiedzialnych za ochronę danych w organizacji.


## Książka zawiera:

- **analizę zmian jakie zajdą w przepisach o ochronie danych,**
- **omówienie nowych obowiązków nałożonych na administratorów danych,**
- **wzory dokumentów,**
- **wzory nowych klauzul zgód na przetwarzanie danych;**
- **analizę zmiany statusu administratora bezpieczeństwa informacji na inspektora ochrony danych,**
- **omówienie nowych uprawnień GIODO, w tym wytycznych dotyczących nakładania kar na administratorów danych i podmioty przetwarzające;**
- **wyjaśnienie nowych zagadnień takich jak profilowanie czy prawo do bycia zapomnianym,**
- **omówienie nowych obowiązków nałożonych na podmiot przetwarzający (procesora),**
- **omówienie procedury postępowania w razie wystąpienia incydentu w zakresie ochrony danych osobowych.**

## Autorzy

Specjaliści ds. ochrony danych w ODO 24 sp. z o.o., adwokaci, członkowie Okręgowej Rady Adwokackiej w Warszawie, absolwenci Wydziału Prawa i Administracji Uniwersytetu Warszawskiego. Zajmują się szeroko pojętym zagadnieniem bezpieczeństwa informacji. Doradzają w zakresie stosowania przepisów o ochronie danych osobowych oraz prowadzą w tym obszarze szkolenia. Współpracują m.in. z dużymi grupami kapitałowymi gdzie przeprowadzają audyty w zakresie bezpieczeństwa informacji, tworzą wewnętrzne procedury, dokumentację oraz opinie prawne. Posiadają wieloletnie doświadczenia w prowadzeniu spraw rozstrzyganych przed sądami powszechnymi.

adw. Anna Dmochowska

adw. Marcin Zadrożny

# Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

**AUDYT**

Zakończony raportem zawierającym niezależną ocenę stanu faktycznego, opis niezgodności oraz praktyczne rekomendacje.

**DOKUMENTACJA**

Zestaw indywidualnie przygotowanych procedur i wymaganych dokumentów, uwzględniających strukturę organizacyjną oraz spełniających szczegółowe wymagania przepisów prawa.

**SZKOLENIA**

Administratorów (ABI, ADO i ASI) w formule otwartej - szkolenia i warsztaty. Dla pracowników w formie szkoleń zamkniętych lub e-learning.

**WSPARCIE** lub **PRZEJĘCIE**

Aktywna pomoc w wypełnianiu obowiązków nałożonych na ABI lub ADO.

ODO 24.pl

tel. 22 740 99 00

Wspieramy FUNDACJA WIEDZA TO BEZPIECZEŃSTWO

szlachetna PACZKA