
#RODO2018
w Twojej firmie

Nasi eksperci

Aleksander Adamus
Kraków
Radca prawny, Senior Associate
e-mail: aleksander.adamus@roedl.pro

Grzegorz Gęborek
Gliwice
Radca prawny, Senior Associate
e-mail: grzegorz.geborek@roedl.pro

Jarosław Kamiński
Warszawa
Adwokat, Associate Partner
e-mail: jaroslaw.kaminski@roedl.pro

Katarzyna Małaniuk
Poznań
Radca prawny, specjalista ds. prawa pracy, Manager
e-mail: katarzyna.malaniuk@roedl.pro

Tomasz Pleśniak
Wrocław
Radca prawny, Senior Associate
e-mail: tomasz.plesniak@roedl.pro

Przemysław Rogiński
Gdańsk
Prawnik
e-mail: przemyslaw.roginski@roedl.pro

Marta Wiśniewska
Warszawa
Radca prawny
e-mail: marta.wisniewska@roedl.pro

Spis treści

Szanowni Państwo,

oddajemy w Państwa ręce broszurę poświęconą unijnemu Rozporządzeniu Ogólnemu o Ochronie Danych Osobowych (RODO). Obowiązuje ono od 25 maja 2018 r. i dotyka wielu kwestii związanych z funkcjonowaniem Państwa organizacji.

Prawodawca unijny nie podaje gotowych rozwiązań wyjaśniających jak dostosować swoją firmę do nowych przepisów. Mówi jedynie o przygotowaniu i wdrożeniu procedur oraz środków bezpieczeństwa, odpowiednich do charakteru prowadzonej działalności oraz ryzyka utraty czy ujawnienia danych. Jednak określenie poziomu tego ryzyka oraz koniecznych zabezpieczeń zależy od wewnętrznej oceny firmy. Pozornie daje to dużo wolności, faktycznie oznacza dużą odpowiedzialność, która spoczywa na przedsiębiorcy.

Chcemy zapoznać Państwa z wprowadzonymi zmianami i ułatwić dostosowywanie działalności do unijnych wymogów. Jest to zadanie wymagające szerokiej wiedzy, gdyż nowe obowiązki dotyczą wielu kwestii m.in. systemu zabezpieczeń, informowania pracowników o zagrożeniach, monitorowania bezpieczeństwa oraz niezwłocznego raportowania ewentualnych incydentów związanych z utratą danych osobowych.

Przygotowanie i wdrażanie procedur związanych z regulacjami RODO nie jest jednorazowym działaniem. Aby spełniać wymogi rozporządzenia, kwestie związane z ochroną danych osobowych powinny być traktowane jako proces na stałe wpisany w działania przedsiębiorstwa.

Życzymy owocnej lektury!
Zespół ekspercki RODO Rödl & Partner

1. Co RODO zmienia w Twojej firmie?

1.1. Kogo dotyczą nowe przepisy?

Nowe przepisy objęły znacznie szerszą grupę podmiotów niż dotychczasowe, dotyczą praktycznie wszystkich przedsiębiorców. Rozporządzenie określa obowiązki oraz zasady podejścia do bezpieczeństwa danych przetwarzanych nie tylko przez administratorów, lecz również firmy przetwarzające dane na zlecenie administratora, tzw. podmioty przetwarzające (np. firmy outsourcingowe). Każdy z tych podmiotów będzie zobowiązany do wprowadzenia procedur administracyjnych i środków technicznych zapewniających odpowiedni stopień bezpieczeństwa przetwarzanych danych.

RODO dotyczy wszystkich przedsiębiorców prowadzących działalność na terenie UE, również tych mających siedzibę poza jej granicami.

Nowe zasady dotyczą m.in. przedsiębiorstw oferujących usługi na terenie UE, a mających siedzibę poza jej granicami. W takim przypadku przepisy znajdą zastosowanie, gdy przetwarzanie wiąże się z oferowaniem towarów, usług lub monitorowaniem zachowania osób fizycznych na terenie UE.

Duża grupa przedsiębiorców będzie musiała uwzględniać element ochrony danych już na etapie planowania konkretnej usługi. Będą mieć obowiązek oceny skutków swoich działań pod kątem ochrony danych osobowych jeszcze zanim rozpoczną ich przetwarzanie. W pewnych wypadkach obowiązkowe będą też konsultacje z organem nadzorczym. Reasumując, każdy przedsiębiorca, który przetwarza dane osobowe, czy to swoich pracowników/współpracowników, czy kontrahentów (lub potencjalnych kontrahentów) zobowiązany jest do przestrzegania przepisów RODO.

1.2. Zmiana zakresu obowiązków

Z perspektywy przedsiębiorców (jako administratorów danych) jedną z najbardziej wymagających zmian będzie obowiązek zgłaszania naruszenia danych osobowych do organu nadzorczego w ciągu 72 godzin od wykrycia takiego naruszenia. Włączając czas potrzebny na analizę skali problemu, oznacza to konieczność natychmiastowego działania, które możliwe jest jedynie w przypadku sprawnie funkcjonującego systemu bezpieczeństwa. Potrzeba także adekwatnych procedur oraz wysokiego poziomu wiedzy i świadomości pracowników. Jeżeli z jakiegoś powodu nie uda się przesłać zawiadomienia o incydencie w wyznaczonym terminie, konieczne będzie dołączenie wyjaśnienia z jakiego powodu doszło do opóźnienia.

Przedsiębiorca ma 72 godziny na zgłoszenie naruszenia danych osobowych od wykrycia takiego naruszenia.

Przedsiębiorca będzie zobowiązany do dokumentowania skutków naruszeń oraz podjętych działań zaradczych. Jeżeli incydent spowoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przedsiębiorca musi zawiadomić o tym osobę, której dane dotyczą. Przekazując tę informację musi działać bez zbędnej zwłoki, a także uczynić to jasnym i prostym językiem. Przy wycieku znacznej liczby danych będzie można dokonać powiadomienia za pomocą mediów.

Istotnie rozszerzony zostanie obowiązek informacyjny wobec osób trzecich, których dane są przetwarzane. Niezbędne będzie podawanie m.in. podstawy prawnej przetwarzania czy informacji dotyczącej okresu przechowywania danych. W efekcie przedsiębiorcy będą musieli znacząco rozszerzyć treść formularzy dotyczących zgody na przetwarzanie danych osobowych.

RODO wprowadza **rozszerzenie katalogu danych wrażliwych** (w szczególności o dane biometryczne) i nowe regulacje dotyczące **przetwarzania danych osobowych dzieci.**

1.3. Zgoda na przetwarzanie danych osobowych

Gruntowne zmiany dotyczą zgody na przetwarzanie danych osobowych, jej formy, sposobu wyrażania oraz, co jest nowością, możliwości jej wycofania (w tak samo łatwy sposób, w jaki zgoda została udzielona). Taka zgoda, udzielona przez osobę której dane dotyczą, stanowi jedną z podstaw prawidłowego przetwarzania danych osobowych.

Wyrażenie zgody następuje w dowolnej formie, musi jedynie być dobrowolne, świadome i jednoznaczne. Jest skutkiem oświadczenia bądź zachowania, które w danej sytuacji jasno pokazuje akceptację dla proponowanego przetwarzania danych. Ponadto osoba zgadzająca się powinna znać przynajmniej tożsamość administratora oraz cele przetwarzania jej danych osobowych.

Zgoda może być wyrażona w dowolnej formie, jej wyrażenie ma być dobrowolne, świadome, jednoznaczne i konkretne.

Dotychczas, na podstawie ustawy o ochronie danych osobowych (UODO) dorozumienie udzielenia zgody było zabronione. RODO przewiduje możliwość domniemania zgody, o ile da się jednoznacznie określić intencję osoby, której dane dotyczą.

W praktyce:

Zgoda może polegać np. na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej. W takiej jednak sytuacji okienka domyślnie zaznaczone nie powinny być traktowane jako wyrażenie zgody.

Uzyskanie zgody nie będzie wymagane, gdy spełniony zostanie któryś z pozostałych warunków legalności przetwarzania danych osobowych. Przykładowo, gdy ich przetwarzanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą. Administrator zobowiązany jest wskazać podstawę, na której dokonuje przetwarzania danych, nie powinien natomiast tych podstaw dublować. Przykładem złej praktyki jest pozyskiwanie zgody jako warunku zawarcia umowy o świadczenie usług, gdyż przetwarzanie danych niezbędnych do wykonania umowy jest legalne i nie ma potrzeby uzyskania zgody.

Wszelkie informacje i komunikaty związane z przetwarzaniem danych powinny być łatwo dostępne, zrozumiałe oraz sformułowane jasnym i prostym językiem. **Wyrażenia zgody nie należy uznawać za dobrowolne jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez konsekwencji.** W praktyce ustalenie, czy wyrażenie zgody nastąpiło dobrowolnie może nastręczać trudności. Faktyczna nierówność stron może podawać w wątpliwość istnienie swobody podejmowania decyzji.

Wycofanie zgody powinno być równie łatwe jak jej wyrażenie.

Przepisy RODO wprost przewidują prawo do wycofania udzielonej zgody w wybranym momencie. Jeszcze przed wyrażeniem zgody należy poinformować osobę, która ją wyraża o prawie wycofania takiej zgody w przyszłości. Samo wycofanie zgody musi być równie łatwe jak jej wyrażenie. Jednocześnie nie wpływa ono na zgodność z prawem przetwarzania danych, którego dokonano jeszcze przed wycofaniem, na podstawie obowiązującej wcześniej zgody. **W sytuacji wycofania zgody administrator powinien zaprzestać przetwarzania i usunąć dane osobowe, jeżeli nie są już niezbędne do celów, w których były zbierane lub przetwarzane.** Porównanie dotychczasowego reżimu prawnego z regulacjami RODO prowadzi do wniosku, że uzyskane dotychczas zgody w większości pozostaną w mocy. Nowe przepisy kładą przy tym wyraźny nacisk na możliwość wycofania zgody w dowolnym momencie.

1.4. Prawo do bycia zapomnianym, prawo do przenoszenia danych

RODO wprowadza nowe uprawnienia dla osób fizycznych, w tym prawo do bycia zapomnianym. Na tej podstawie klient będzie mógł żądać od administratora niezwłocznego usunięcia dotyczących go danych. W przypadku upublicznienia danych na administratorze będzie ciążył obowiązek poinformowania innych podmiotów przetwarzających te dane, że osoba której dotyczą żąda ich usunięcia. Dotyczy to także wszelkich łączy do danych, ich kopii lub replikacji.

Nowe uprawnienia osób fizycznych:
każdy może zażądać niezwłocznego usunięcia dotyczących go danych (prawo do bycia zapomnianym) oraz przekazania swoich danych innemu podmiotowi (prawo do przenoszenia danych).

Prawo do przenoszenia danych oznacza natomiast, że klient (osoba fizyczna) będzie mógł zwrócić się z żądaniem, aby administrator przekazał mu dane dotyczące jego osoby, które są przetwarzane. Przekazanie musi zostać wykonane w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego. Klient będzie mógł przechowywać dane we własnych celach bądź przekazać je innemu administratorowi. Będzie mógł też żądać, by jego dane osobowe zostały przesłane bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

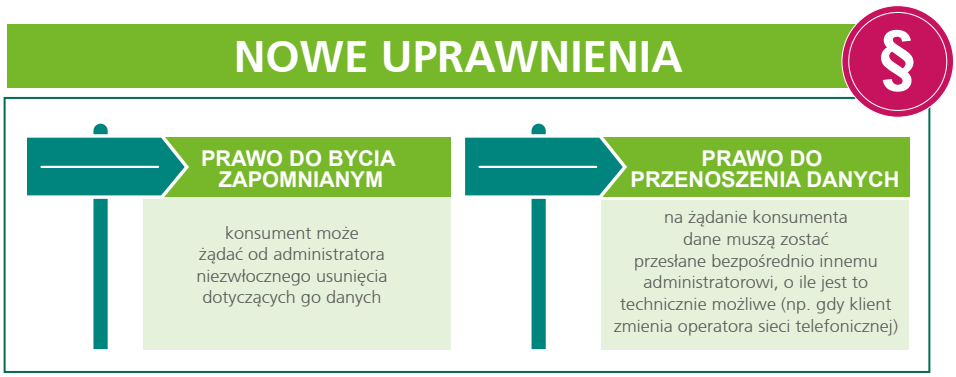
W praktyce:

Klient zmienia operatora sieci komórkowej i żąda, aby dotychczasowy operator przesłał dane klienta nowemu operatorowi. Z perspektywy administratorów danych nowe prawa osób fizycznych oznaczają obowiązek zapewnienia ich skutecznej i terminowej realizacji.

1.5. Ważność dotychczas uzyskanych zgód na przetwarzanie danych osobowych po 25 maja 2018 r.

Wcześniej uzyskane zgody na przetwarzanie danych osobowych, które zostały zebrane w oparciu o dotychczas obowiązującą UODO, ustawę Prawo telekomunikacyjne oraz ustawę o świadczeniu usług drogą elektroniczną, nie stracą ważności po wejściu w życie RODO, jeśli były zbierane zgodnie z ww. przepisami.

Główny Inspektor Ochrony Danych Osobowych (GIODO) zachęcał przedsiębiorców do uważnego przejrzenia dotychczas stosowanych przez nich klauzul i mechanizmów pozyskiwania zgód na przetwarzanie danych osobowych w celu upewnienia się, że spełniają one standardy RODO. Konieczne jest poinformowanie osób, których dane dotyczą o nowych uprawnieniach z RODO, w tym o prawie do wycofania zgody w każdym momencie.



Jak prawidłowo przeprowadzić taki proces?

Należy skoncentrować się na następujących elementach:

- zdolność do złożenia oświadczenia,
- forma i treść,
- okoliczności towarzyszące.

Udzielona zgoda nie może być zgodą milczącą, ani wynikającą z domyślnie ustawionego zaznaczenia okienek na stronie internetowej. Ważność zachowa ta zgoda, która została złożona dobrowolnie, jednoznacznie, świadomie i konkretnie dla określonych celów. Rolą administratora danych jest weryfikacja, czy powyższe wymagania zostały spełnione.

Jak rozumieć powyższe warunki?

- **Dobrowolność**
  Zgoda dobrowolna to taka, która została złożona **bez wpływu, nacisku ani przymusu osób trzecich.** Przy jej udzielaniu musi zostać zapewniona możliwość swobodnego wyboru, a wyrażenie odmowy nie może mieć wpływu na inne uprawnienie wyrażającego zgodę. Zgoda na przetwarzanie danych w głównym celu nie może być połączona ze zgodą na np. cele marketingowe. Zatem gdy przetwarzanie danych jest prowadzone w kilku celach, to należy uzyskać odrębną zgodę dla każdego celu.

- **Jednoznaczność**
  Zasada jednoznaczności wymaga **wyraźnego i zamierzonego działania potwierdzającego.** Aktualnie obowiązujące przepisy dotyczące zgody i wytyczne GIODO nie odbiegają mocno od wymogów RODO. Dzięki temu jest szansa, że otrzymane dotychczas zgody zachowają swoją ważność, jeśli były zbierane zgodnie z obowiązującym prawem. Należy jednak pamiętać o konieczności informowania osób fizycznych o możliwości wycofania zgody.

Czy zatem należy spełnić powyższy warunek informacyjny wobec osób, których dane są obecnie przetwarzane?

Przepisy RODO nie wykluczają ważności zebranych zgód w sytuacji, kiedy w momencie pozyskiwania zgody nie wszystkie informacje zostały przekazane. Niemożliwe jest jednak jednoznaczne stwierdzenie, które zgody zachowają swoją ważność, a które nie. Wynika to z faktu, że zależy to nie tylko od samej treści klauzuli zgody, ale także pozostałych dokumentów i mechanizmów stosowanych przez administratora danych.

Aby wykluczyć ryzyko zarzutu przetwarzania danych osobowych bez podstawy prawnej po 25 maja 2018 r. wskazane jest, aby przedsiębiorcy dokonali weryfikacji treści i warunków dotychczas pozyskanych zgód pod kątem RODO. Przetwarzanie danych bez podstawy prawnej wiąże się z ryzykiem nałożenia kary administracyjnej w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa – do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa).

- **Świadomość**
  Zgody świadomej udziela osoba, która **została prawidłowo poinformowana** przez administratora danych. W tym celu należy w sposób jasny i precyzyjny udzielić niezbędnych informacji osobom udzielającym zgody. Należy mieć pewność, że osoba wie na co wyraża zgodę i w jaki sposób jej dane osobowe będę przetwarzane.

Nie wszystkie elementy wymienione w artykułach 13 i 14 RODO muszą zawsze występować jako warunek świadomej zgody, zatem rozszerzone obowiązki informacyjne na mocy RODO niekoniecznie przeciwstawiają się ciągłości zgody wyrażonej przed wejściem w życie RODO.

› **Konkretność**
W zgodzie konkretnej został precyzyjnie określony cel przetwarzania danych oraz wskazany ich zakres. Szczegółowość w zapytaniach ma również umożliwić użytkownikom wyrażenie konkretnej zgody na konkretne cele. Ponadto, aby wymóg konkretności został spełniony należy wyraźnie oddzielić informacje związane z uzyskaniem zgody na działania niezbędne w zakresie przetwarzania danych od informacji dotyczących innych kwestii.

1.6. Profilowanie

RODO reguluje zasady profilowania, wprowadzając po raz pierwszy definicję tego pojęcia. Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych i ich wykorzystanie do oceny niektórych czynników osobowych. Ma to miejsce np. przy analizie efektów pracy danej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, lokalizacji itp.

Profilowanie będzie legalne, gdy:

› wyraźnie dopuszcza je prawo,

› jest niezbędne do zawarcia i wykonania umowy między osobą, której dane dotyczą, a administratorem danych,

› osoba, której dane dotyczą, wyraziła zgodę.

Przedsiębiorcy, stosując profilowanie, będą zobowiązani do przekazania osobom fizycznym informacji na ten temat, a także rozważenia w ramach własnej oceny ryzyka konieczności uzyskania stosownej zgody. Będą też musieli wskazać zasady podejmowania zautomatyzowanych decyzji, ich znaczenie i przewidywane konsekwencje dla danej osoby.

Profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych.

1.7. Częściowa liberalizacja

Jeden z motywów RODO brzmi: „Prawo do ochrony danych osobowych nie jest prawem bezwzględnym. Należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności". Obok zaostrzania obowiązujących regulacji, przepisy liberalizują niektóre kwestie w porównaniu do polskiej Ustawy o ochronie danych osobowych (UODO).

Liberalizacja dotyczy wspomnianej już możliwości dorozumiewania zgody. RODO dopuszcza wyrażenie zgody poprzez działania osoby, ujawniające zgodę na przetwarzanie danych w sposób wyraźny. Tego rodzaju dorozumiewanie zostało wprost wykluczone w UODO.

Inny przykład liberalizacji dotyczy braku konieczności rejestracji baz danych osobowych w GIODO. Zgodnie z europejskimi przepisami przedsiębiorcy nie będą już mieli takiego obowiązku.

1.8. Nowa ustawa o ochronie danych osobowych

Ustawa z 29 sierpnia 1997 r. była implementacją dyrektywy 95/46/WE. W celu dostosowania polskich przepisów do RODO, ustawodawca zdecydował się na jej nowelizację. Nowa ustawa z 10 maja 2018 r. zaczyna obowiązywać równolegle z RODO tj. 25 maja 2018 r. Należy pamiętać, że akt ten reguluje głównie kwestie techniczne i organizacyjne odpowiednie do warunków polskich (np. funkcjonowanie Urzędu o Ochronie Danych Osobowych), a RODO nadal będzie aktem bezpośrednio stosowanym dla wszystkich podmiotów w UE. Oprócz nowej ustawy, istnieje także projekt ustawy zapewniającej stosowanie RODO, której celem jest zmiana przepisów w poszczególnych sektorach (np. Kodeks Pracy, Prawo bankowe) w celu realizacji rozporządzenia. Jednak ustawa nie trafiła jeszcze do Sejmu.

1.9. Inspektor Ochrony Danych

W określonych przypadkach RODO zobowiązuje przedsiębiorców do powołania wewnętrznego Inspektora Ochrony Danych (IOD). Jest to osoba odpowiedzialna za bezpieczeństwo przetwarzania danych w konkretnym przedsiębiorstwie oraz za prowadzenie rejestru czynności przetwarzania danych. W obecnym stanie prawnym taką rolę pełni Administrator Bezpieczeństwa Informacji.

Rozporządzenie RODO przewiduje sytuacje, w których administrator danych osobowych i podmiot przetwarzający w jego imieniu dane, mają obowiązek wyznaczenia IOD. Do takich sytuacji należą:

- przetwarzanie danych przez organ lub podmiot publiczny,
- regularne i systematyczne monitorowanie osób, których dane dotyczą,
- przetwarzanie danych na dużą skalę,
- przypadki gdy główna działalność organizacji polega na przetwarzaniu szczególnych kategorii danych osobowych na dużą skalę.

Inspektor Ochrony Danych Osobowych (IOD) zastępuje Administratora Bezpieczeństwa Informacji (ABI). Jest to osoba odpowiedzialna za:
➔ bezpieczeństwo przetwarzania danych,
➔ prowadzenie rejestru czynności przetwarzania danych.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Obowiązek powołania IOD dotyczy organizacji, w których występuje co najmniej jedna z poniższych sytuacji:

- przetwarzanie danych przez organ lub podmiot publiczny,
- regularne i systematyczne monitorowanie osób, których dane dotyczą,
- główna działalność organizacji polega na przetwarzaniu szczególnych kategorii danych osobowych na dużą skalę.

Zadania IOD:

- bieżące przeprowadzanie wewnętrznych audytów w zakresie procesów przetwarzania danych, jak również w zakresie innych dysfunkcji zachodzących w organizacji,
- odpowiedzialność za przestrzeganie zasad RODO oraz dbanie o zgodność z pozostałymi przepisami o ochronie danych osobowych.

Niepowołanie IOD może spowodować nałożenie kary administracyjnej

Inspektor, jako strażnik procesów związanych z ochroną danych osobowych, jest odpowiedzialny nie tylko za przestrzeganie RODO, ale również za zgodność z pozostałymi przepisami o ochronie danych osobowych. Do jego zadań należy **bieżące przeprowadzanie wewnętrznych audytów** w zakresie procesów przetwarzania danych, ale również w zakresie innych dysfunkcji zachodzących w organizacji. Inspektorem może być osoba z personelu administratora lub podmiotu przetwarzającego, jak również zewnętrzny profesjonalista. W drugim przypadku, poza oceną przetwarzania danych osobowych, może on ocenić pozostałe procesy funkcjonujące w ramach organizacji np. finansowe, informatyczne, logistyczne.

Większość przedsiębiorców prowadzących działalność gospodarczą na terytorium Polski i UE nie ma obowiązku powołania inspektora, jego ustanowienie będzie dobrowolne. W praktyce IOD może się okazać bardzo pomocny przy bieżących operacjach biznesowych związanych z przetwarzaniem danych oraz przy wykazywaniu zgodności przetwarzania danych z RODO, np. w razie kontroli.

W praktyce:

Inspektor Ochrony Danych Osobowych (IOD) powinien zapewnić przestrzeganie przepisów, wprowadzając mechanizmy rozliczania (np. przeprowadzania audytów i ocen skutków dla ochrony danych). Będzie także pełnił rolę pośrednika pomiędzy zainteresowanymi stronami (np. między organem ochrony danych osobowych, osobami, których dane dotyczą i jednostkami w ramach przedsiębiorstwa).

Działania IOD mogą zmierzać do poprawy efektywności biznesowej administratora lub podmiotu przetwarzającego dane w celu zwiększenia ich konkurencyjności i nie mogą prowadzić do konfliktu interesów. Inspektor nie może określać sposobów i celów przetwarzania danych w organizacji. Powinien być włączany od samego początku we wszelkie projekty, w których dochodzi do przetwarzania danych osobowych (począwszy od procesu rekrutacji i spraw kadrowych, poprzez kwestie marketingowe, po wybór dostawców usług). Istotne będzie zapewnienie mu określonej pozycji w strukturze organizacyjnej firmy oraz środków finansowych i personalnych, do wykonywania zadań.

2. Nowe zasady kontroli i zmiany w karach

2.1. GIODO i PUODO

Do czasu wejścia w życie RODO zagadnienia związane z ochroną danych w Polsce uregulowane były w UODO. Zgodnie z nią organem odpowiedzialnym za ochronę danych osobowych był Generalny Inspektor Ochrony Danych Osobowych (GIODO).

Nowy organ ochrony danych osobowych **(PUODO) ma pełnić bardziej znaczącą rolę niż dotychczas GIODO.** Istotnym narzędziem w jego rękach będzie możliwość nakładania dotkliwych kar administracyjnych.

2.2. Rozpoczęcie kontroli

Dotychczas postępowanie kontrolne było rozpoczynane przez GIODO np. wskutek złożonej skargi, doniesień medialnych czy kontroli sektorowych. W zakresie kontroli sektorowych GIODO co roku publikował komunikat, w którym wskazywał jakie podmioty i w jakim zakresie będą kontrolowane. Zgodnie z nową ustawą, postępowania kontrolne PUODO będą prowadzone w oparciu o: plan kontroli, uzyskane informacje i przeprowadzone analizy.

2.3. Kontroler i jego uprawnienia

Dotychczas GIODO był zobligowany np. do poinformowania kontrolowanego o planowanej kontroli co najmniej 7 dni przed jej rozpoczęciem. W nowej ustawie wskazano, że PUODO będzie miał, m.in. możliwość przeprowadzić kontrolę:

- bez wcześniejszego zawiadamiania kontrolowanego,
- nawet jeżeli w tym samym czasie u kontrolowanego będzie przeprowadzana inna kontrola (np. Państwowej Inspekcji Pracy),
- nawet jeżeli zostanie przekroczona maksymalna liczba dni w roku, podczas których przedsiębiorca może być kontrolowany.

Nowa ustawa przewiduje też rozszerzenie katalogu osób upoważnionych do przeprowadzania kontroli. Dotychczas mogli ją przeprowadzać tylko kontrolerzy polskiego organu kontrolnego. Według nowej ustawy również pracownicy organu nadzorczego odpowiedzialnego za ochronę danych osobowych z innego państwa unijnego mogą przystąpić do kontroli. Taka możliwość zostanie ograniczona do tzw. wspólnych operacji organów nadzorczych.

Rozszerzeniu ulega również zakres uprawnień osób kontrolujących. Będą one mogły korzystać z pomocy funkcjonariuszy, innych organów kontroli państwowej oraz policji. Będą także miały możliwość wydawania polecenia towarzyszącym im funkcjonariuszom. W uzasadnionych przypadkach, czynności kontrolne mogą zostać utrwalane za pomocą urządzeń rejestrujących obraz.

2.4. Protokół kontroli

Po zakończeniu przez GIODO czynności kontrolowany otrzymywał protokół z kontroli. Wówczas mógł wnieść umotywowane zastrzeżenia i wnioski do protokołu, przekazywane następnie do GIODO. Mógł także odmówić podpisania protokołu i w ciągu 7 dni przedstawić swoje stanowisko na piśmie, wskazując dlaczego odmówił złożenia podpisu.

W nowym projekcie zrezygnowano z możliwości przedstawienia swojego stanowiska. Kontrolowanemu ma być przedstawiany protokół, do którego w ciągu 7 dni będzie mógł złożyć pisemnie zastrzeżenia. Jeżeli tego nie uczyni, straci możliwość składania zastrzeżeń. Co więcej, **podpisanie protokołu przez kontrolowanego nie będzie warunkiem jego skuteczności i ważności.** Jeżeli odmówi on podpisania, kontrolujący zaznaczy odmowę, a sam protokół będzie przekazywany dalej do PUODO. Docelowo jedynym narzędziem ochrony kontrolowanego na etapie postępowania będzie możliwość składania zastrzeżeń do protokołu w terminie 7 dni.

Kary za niedochowanie zasad przetwarzania danych będą sięgać 20 mln euro lub 4% całkowitego rocznego obrotu firmy. Zastosowanie będzie miała kwota wyższa.

2.5. Administracyjne kary pieniężne

Dotkliwe kary są najbardziej drastyczną zmianą w stosunku do dotychczas obowiązującego prawa, gdzie relatywnie niewielka ilość nieprzestrzegających go podmiotów była poddawana odpowiedzialności karnej. Od wejścia w życie RODO odpowiedzialność ma być głównie finansowa. Dotychczas, jeżeli w wyniku kontroli GIODO stwierdził niedochowanie zasad przetwarzania danych osobowych, podejmował decyzję nawołującą do przywrócenia stanu zgodnego z prawem. Dopiero niepodporządkowanie się takiej decyzji mogło skutkować nałożeniem grzywny. PUODO, w razie niedochowania wspomnianych zasad, będzie przeprowadzał postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych. Postępowanie to będzie się toczyło równolegle do postępowania kontrolnego lub po nim. Jeżeli rzeczywiście zostaną wykryte naruszenia, PUODO wyda decyzję, mając możliwość:

- udzielić upomnienia, jeżeli strona zaprzestała naruszeń, a ich waga będzie znikoma,
- nałożyć w drodze decyzji karę pieniężną – określoną w przepisach o RODO.

Wysokość kar, w porównaniu do obecnych kwot, jest znacznie wyższa. W zależności od rodzaju naruszenia, będą mogły one sięgać 20 mln euro lub 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Oczywiście, nie odbiera to prawa do dochodzenia swoich racji przed sądem.

Za co będą nakładane kary?

Kary mogą być nakładane za działanie sprzeczne z przepisami dotyczącymi podstawowych zasad przetwarzania danych oraz praw osób, których dotyczą. Są to w szczególności: prawo dostępu do danych, ich sprostowania lub usunięcia oraz przenoszenia. Dodatkowo, karze podlegać będą jednostki nieprzestrzegające nakazu tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy lub niezapewniające temu organowi określonego w przepisach dostępu (np. do wszelkich danych osobowych, do pomieszczeń administratora danych, do sprzętu, na którym dane są przetwarzane itp.)

Przewidziane są również niższe kary: 10 mln euro lub 2% obrotu, które będą nakładane za naruszenie przepisów dotyczących obowiązków administratora lub podmiotu przetwarzającego oraz obowiązków podmiotu certyfikującego i monitorującego. Państwa członkowskie UE mają obowiązek przyjąć przepisy określające także inne sankcje za naruszenie postanowień RODO oraz podjąć środki niezbędne do ich wykonania.

Równocześnie w nowej ustawie **ograniczono wysokość kary do 100 000 zł wobec podmiotów publicznych,** jak np. organy administracji rządowej, jednostki samorządu terytorialnego czy państwowe uczelnie. Takie podmioty, nawet w przypadku rażącego naruszania przepisów, nie będą musiały płacić wielomilionowych kar.

Kto będzie nakładać kary?

Organ nadzorczy ma zostać powołany na podstawie obowiązującej w danym państwie ustawy. W Polsce organem nadzorczym nakładającym kary będzie Prezes Urzędu Ochrony Danych Osobowych (PUODO). Tym samym kary pieniężne będą nakładane w drodze decyzji administracyjnej i będą stanowiły dochód Skarbu Państwa.

Obecnie nie ma jeszcze pewności jak wyglądać będą regulacje prawne związane z nakładaniem kar w Polsce. Praktyka PUODO pokaże w przyszłości, jakie będzie podejście nowego regulatora w tym zakresie.

KARY ADMINISTRACYJNE

20 mln euro lub 4%
całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego

ZA CO?

- działania sprzeczne z prawem dostępu do danych, ich sprostowania, usunięcia oraz do przenoszenia
- nieprzestrzeganie nakazu tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy
- niezapewnienie organowi nadzorczemu określonego w przepisach dostępu

10 mln euro lub 2%
całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego

ZA CO?

- naruszenie przepisów dotyczących obowiązków administratora lub podmiotu przetwarzającego
- naruszenie obowiązków podmiotu certyfikującego i monitorującego.

OD WEJŚCIA W ŻYCIE RODO ODPOWIEDZIALNOŚĆ JEST GŁÓWNIE FINANSOWA

Kary mogą być nakładane za działanie sprzeczne z przepisami dotyczącymi:
› podstawowych zasad przetwarzania › praw osób, których dotyczą

3. Jak być w zgodzie z RODO?

3.1. Podstawy

Przede wszystkim należy wprowadzić wewnętrzne regulacje w zakresie procedury zgłaszania naruszeń, tak aby firma mogła się wywiązać z obowiązków względem organu nadzorczego. Istotne jest także podnoszenie ogólnego poziomu świadomości zagrożeń wśród pracowników. Ważne, aby zapobiegać incydentom, a w przypadku ich wystąpienia, rozpoznać je i niezwłocznie zgłosić odpowiednim osobom.

W pierwszej kolejności zweryfikowane powinny zostać następujące obszary i zagadnienia:

- podstawy i kategorie przetwarzanych danych osobowych,
- konieczność powołania Inspektora Ochrony Danych,
- dokumentacja kadrowa i zasady procesu rekrutacji,
- strony internetowe pod kątem przetwarzania danych,
- umowy powierzenia przetwarzania danych osobowych,
- treść stosowanych klauzul informacyjnych i ewentualna konieczność ich uzupełnienia,
- treść stosowanych klauzul zgód na przetwarzanie danych osobowych i ewentualne ich uzupełnienie,
- stosowane zabezpieczenia organizacyjne i techniczne przetwarzanych danych osobowych,
- wewnętrzna dokumentacja związana z ochroną danych i konieczność jej modyfikacji.

3.2. Analiza ryzyka

Przed wdrożeniem systemu bezpieczeństwa sieci wysoce wskazane jest przeprowadzenie analizy ryzyka związanego z przetwarzaniem danych osobowych w firmie. Choć obowiązek przeprowadzenia formalnej oceny ryzyka dotyczy jedynie niektórych podmiotów, w każdej firmie warto przeprowadzić taką analizę. Poza potencjalnie większą skutecznością systemu zabezpieczeń, przeprowadzenie jej będzie dobrym argumentem wobec organu nadzorczego, wskazującym na wysoki poziom dbałości o zabezpieczenie danych osobowych w firmie.

3.3. Samokontrola

Kluczową zmianą systemową jest wprowadzenie dla administratorów danych obowiązku przeprowadzenia samooceny pod kątem skutków przetwarzania danych dotyczącego ich ochrony i ewentualnego ryzyka. Oznacza to konieczność przeprowadzania gruntownej weryfikacji przetwarzanych danych, szczegółowej oceny zagrożeń oraz zaplanowania odpowiednich środków technicznych i organizacyjnych.

RODO wprowadza dla administratorów obowiązek samokontroli, dotyczący weryfikacji zabezpieczeń przetwarzanych danych i oceny ewentualnego ryzyka.

Nie wystarczy wypełnienie minimalnych wymogów określonych w przepisach prawa. Administratorzy danych i podmioty je przetwarzające będą musieli zrobić wszystko, co uznają za właściwe w oparciu o własne sposoby przetwarzania danych oraz swoją ocenę. Konieczne też będzie wykazanie, że przyjęte rozwiązania i środki o charakterze technicznym i organizacyjnym są odpowiednie dla danego przypadku przetwarzania danych osobowych. Co istotne, kluczowe znaczenie w kontekście RODO będzie mieć podnoszenie świadomości pracowników i współpracowników, a także prowadzenie dla nich regularnych szkoleń z zakresu przetwarzania danych osobowych. Doświadczenie pokazuje, że po przeprowadzeniu weryfikacji okazuje się, iż wprowadzenie nowych rozwiązań nie wystarczy – niezbędne jest także dostosowanie ogólnego modelu biznesowego (w tym rozwiązań technicznych) oraz stosunków z podmiotami trzecimi (klientami oraz dostawcami) do nowych regulacji.

Dodatkowo RODO przewiduje, że pewne szczególne kwestie (np. pracownicze) mogą i powinny zostać uregulowane w ustawodawstwie krajowym. Konieczne jest zatem monitorowanie zmian w polskich przepisach i ich uwzględnienie w bieżących działaniach przedsiębiorstwa.

JAK ŻYĆ W ZGODZIE Z RODO?

4. Jak RODO wpływa na prawa pracowników?

4.1. Monitorowanie pracowników a obowiązek informacyjny

Czy RODO będzie miało wpływ na tak powszechnie stosowaną praktykę, jaką jest monitorowanie pracowników? Do tej pory w Polsce nie istniały konkretne przepisy normujące monitorowanie miejsca pracy. Zazwyczaj pracodawcy kontrolujący pracowników usprawiedliwiali swoje działania ustawą o ochronie danych osobowych. Jednak polski ustawodawca, dostosowując polskie przepisy do RODO, zdecydował się także na nowelizację Kodeksu pracy w zakresie ochrony danych osobowych. Wprowadzona została legalna definicja monitoringu zwykłego, a także monitoringu poczty elektronicznej pracownika. Monitoring wizyjny może służyć jedynie bezpieczeństwu pracowników oraz ochronie mienia pracodawcy. Monitoring co do zasady nie powinien obejmować takich miejsc jak np. stołówka, szatnia lub palarnia. Przetwarzanie obrazu uzyskanego powinno trwać maksymalnie trzy miesiące, ewentualnie do momentu prawomocnego zakończenia postępowania, jeżeli nagranie stanowi środek dowodowy w sprawie. Po tym czasie nagrania powinny zostać trwale usunięte. Dodatkowo pracodawca powinien poinformować swoich pracowników o stosowaniu monitoringu w układzie zbiorowym pracy, regulaminie pracy, a jeżeli nie jest zobligowany do posiadania tych dokumentów, w formie obwieszczenia.

Jednakże podstawową zmianą wprowadzaną przez RODO jest regulacja obowiązku informacyjnego. Zgodnie z rozporządzeniem pracodawca będzie zobowiązany przekazać pracownikowi między innymi następujące informacje dotyczące przetwarzania danych osobowych:

- adres, pełną nazwę administratora danych osobowych,
- dane kontaktowe administratora (np. adres email, telefon),
- cel przetwarzania danych osobowych,
- informację o odbiorcach danych osobowych,
- informację o zamiarze przekazania danych osobowych do państwa trzeciego,
- informację o okresie przechowywania danych osobowych,
- informację o prawie do cofnięcia zgody na przetwarzanie danych,
- informację, czy podanie danych osobowych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Dzięki obydwu rozwiązaniom wzrośnie świadomość pracowników dotycząca przetwarzania ich danych osobowych.

4.2. RODO a proces rekrutacyjny

Rozporządzenie nakłada na rekrutujących obowiązek otrzymania od kandydata dwóch oddzielnych zgód na przetwarzanie jego danych. Pierwsza z nich ma dotyczyć obecnego postępowania rekrutacyjnego, a druga ewentualnych przyszłych procesów. Co więcej, obowiązek ten musi zostać spełniony zarówno w przypadku aplikacji składanych online, jak i przy tradycyjnym CV. Zgoda kandydata na oba postępowania jest w pełni dobrowolna, jednak ta dotycząca obecnego procesu jest niezbędna w celu uczestnictwa w procesie rekrutacyjnym.

W procesie rekrutacji konieczne będzie uzyskanie dwóch zgód od kandydata.

Nowością wprowadzoną przez RODO jest pojęcie tzw. **działania potwierdzającego**. Opisuje ono sytuację w której pomimo braku pisemnej zgody kandydata jego świadome czynności oznaczają zgodę na przetwarzanie danych. Jak to rozumieć?

Ten zapis sprawia wrażenie ułatwiającego pracę działów HR. Istnieje jednak wiele ograniczeń dotyczących tej zasady. Przede wszystkim tak uzyskana zgoda na przetwarzanie danych dotyczy jedynie obecnego postępowania rekrutacyjnego. Jeśli kandydat chciałby, żeby jego CV mogło być wzięte pod uwagę w równolegle trwających lub przyszłych rekrutacjach, musi wyrazić na to dodatkową zgodę. W takim przypadku powinien dodać do CV specjalną klauzulę. Istotne jest także to, że **w przypadku wątpliwości lub sporu, to potencjalny pracodawca będzie musiał wykazać, że zgoda została udzielona** poprzez jednoznaczne działanie potwierdzające.

W praktyce:

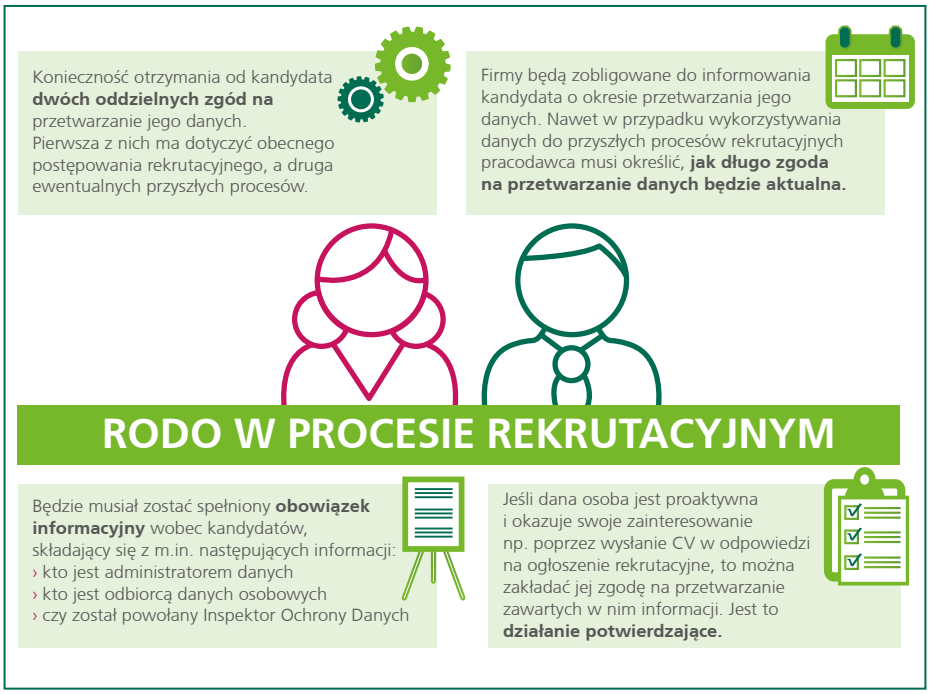
Jeśli dana osoba jest proaktywna i okazuje swoje zainteresowanie np. poprzez wysłanie CV w odpowiedzi na ogłoszenie rekrutacyjne, to można zakładać jej zgodę na przetwarzanie zawartych w nim informacji.

4.3. Obowiązek informacyjny wobec kandydatów

Wobec kandydatów będzie musiał zostać spełniony szeroki obowiązek informacyjny, składający się z m.in. następujących informacji:

- kto jest administratorem danych (tj. potencjalny pracodawca), czy został powołany Inspektor Ochrony Danych,
- kto będzie odbiorcą danych osobowych kandydatów,
- jakie prawa przysługują kandydatowi w zakresie jego danych osobowych, a w szczególności możliwość wycofania zgody (dotyczy w szczególności zgody na przyszłe rekrutacje), prawa do złożenia skargi do organu nadzorczego, prawa do modyfikacji danych i ich usunięcia.

Firmy będą zobligowane do informowania kandydata do pracy o okresie przetwarzania jego danych. Według założeń RODO, dane osobowe nie powinny być przetwarzane dłużej niż jest to niezbędne – tu należy rozróżnić, czy dane przetwarzane są na potrzeby jedynie konkretnej rekrutacji, czy też na podstawie dodatkowej zgody, na cele przyszłych procesów rekrutacyjnych. Nawet w drugim przypadku, **pracodawca musi określić jak długo zgoda na przetwarzanie danych będzie aktualna.**



4.4. Zabezpieczenie danych

Warto pamiętać, że dokumentacja składana przez kandydatów powinna być udostępniona jedynie pracownikom rekrutującym oraz kierownictwu. Dodatkowo, dane kandydatów powinny podlegać tym samym środkom zabezpieczającym co dane pracowników firmy. Rozumiemy przez to np. trzymanie ich w zamykanych szafkach oraz skuteczne usuwanie za pomocą niszczarek lub specjalistycznych programów komputerowych. W przypadku wycieku danych osobowych (w tym również do osób niepowołanych wewnątrz firmy) pracodawca ma obowiązek zgłosić okoliczność naruszenia ochrony danych osobowych do organu nadzorczego w terminie 72 godzin od stwierdzenia naruszenia.

Dodatkowo pracodawca może żądać podania innych danych osobowych, gdy jest to niezbędne do wypełniania obowiązku pracodawcy nałożonego przepisem prawa.

4.5. Elektronizacja akt pracowniczych

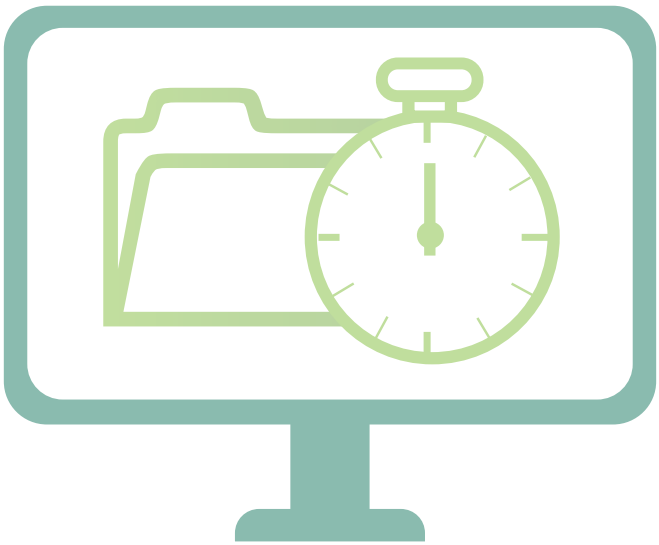
Kolejną zmianą wprowadzoną przez RODO jest możliwość przechowywania i przetwarzania przez pracodawcę akt osobowych w wersji elektronicznej. Umożliwia to nowelizacja art. 94 pkt 9a Kodeksu pracy, który otrzymał następujące brzmienie: „prowadzić i przechowywać w postaci papierowej lub elektronicznej dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników (dokumentacja pracownicza)".

W dotychczas obowiązującym ustawodawstwie wymagana była dokumentacja pracownicza w formie papierowej. Przedsiębiorcy byli przez to zobligowani do przechowywania akt pracowniczych w przysłowiowych teczkach. Jednak część pracodawców stosowała równolegle również bardziej wydajną dokumentację w formie elektronicznej. Nowe przepisy mogą pozytywnie wpłynąć na dotychczasową praktykę poprzez usunięcie problemu zbędnego dublowania przechowywanych informacji.

Warto podkreślić, że nowe przepisy gwarantują równoważność dokumentacji prowadzonej i przechowywanej w postaci elektronicznej i papierowej.

Pracodawcy zyskują też możliwość zmiany postaci dokumentacji pracowniczej z papierowej na elektroniczną poprzez **sporządzenie odwzorowania cyfrowego, w szczególności skanu i opatrzenie go kwalifikowanym podpisem elektronicznym, kwalifikowaną pieczęcią elektroniczną pracodawcy lub kwalifikowanym podpisem elektronicznym upoważnionej przez pracodawcę osoby.** Pracodawca będzie zobowiązany poinformować pracowników o zmianie postaci dokumentacji pracowniczej oraz o możliwości odbioru poprzedniej postaci dokumentacji w terminie 30 dni.

Ważnym aspektem wprowadzanym przez nowe przepisy jest konieczność posiadania programów do digitalizowania akt pracowniczych w sposób gwarantujący odpowiedni poziom bezpieczeństwa. Można przypuszczać, że nowe przepisy wpłyną pozytywnie na podaż programów do prowadzenia dokumentacji. Przewiduje się znaczący wzrost liczby dostępnych na rynku rozwiązań, które będą umożliwiać kompleksowe i bezpieczne przechowywanie danych.



5. RODO, czyli więcej niż prawo

Choć Rozporządzenie o Ochronie Danych Osobowych to przede wszystkim rewolucja prawna, w znacznej mierze wywiera wpływ na technologiczny aspekt funkcjonowania firmy.

Zgodnie z nowymi przepisami część organizacji będzie musiała powołać Inspektora Ochrony Danych (IOD), który bywa porównywany do funkcjonującego w dotychczas obowiązującym ładzie prawnym Administratora Bezpieczeństwa Informacji (ABI). Są to jednak odmienne role, które wymagają innych kompetencji.

Dotąd ABI był przede wszystkim prawnikiem, specjalistą w zakresie ochrony danych osobowych. W przypadku IOD konieczne jest posiadanie kompetencji zarówno w zakresie prawa, jak i technologii. Konieczność mierzenia się z tego typu wyzwaniami będzie stanowić codzienność pracy IOD. Z tego względu ustawodawca pozostawił możliwość outsourcowania usług świadczonych przez osoby o takich kompetencjach.

Zespół IOD – hakerzy i prawnicy

Nowe prawo przewiduje nie tylko możliwość zlecenia zadań IOD na zewnątrz, ale również powierzenie ich zespołowi specjalistów. Wśród nich może się znaleźć zarówno prawnik, jak i specjalista od cyberbezpieczeństwa oraz administrator systemów informatycznych.

Do zadań IOD należało będzie choćby regularne testowanie sieci pod kątem bezpieczeństwa. Według danych firmy Gemalto w samym tylko 2017 roku doszło do ujawnienia ponad 2,6 mld rekordów z baz danych w ramach 1765 różnych wycieków. Co więcej, w 55,9% przypadków firma nawet nie zauważyła takiego incydentu. Raport firmy Kaspersky Lab wskazuje, że w ubiegłym roku firma zidentyfikowała ponad 15 mln różnego rodzaju niebezpiecznych programów komputerowych. Nowe odmiany złośliwego oprogramowania powstają codziennie. Z tego względu regularne wykonywanie testów bezpieczeństwa jest konieczne.

W zależności od skali przetwarzania danych oraz ich natury (dane medyczne, dane wrażliwe itp.) częstotliwość wymaganego skanowania może być różna. Ważne by przeprowadzane ono było regularnie i przez specjalistów. W branży finansowej, gdzie filozofia i praktyka regularnego przeprowadzania testów penetracyjnych jest już powszechna, jedynie 5,3% cyberataków kończy się sukcesem. Z kolei w służbie zdrowia odsetek ten wynosi 38,9%, a w branży online jest to 35,1%.

Testami tego typu mogą się zajmować zarówno pracownicy zatrudnieni na stałe, jak i zewnętrzny zespół, choćby działający w ramach Managed Security Service.

Twierdza w chmurach

Zabezpieczenie firmowej infrastruktury wiąże się z wydatkami na oprogramowanie, sprzęt i specjalistów, którzy potrafią zbudować szczelny system. Alternatywą jest migracja danych do chmury obliczeniowej, na przykład Amazon Web Services czy Microsoft Azure.

Pozornie przekazanie danych zewnętrznemu podmiotowi wiąże się z ryzykiem, a trzymanie ich „u siebie" jest bezpieczniejsze. W praktyce jednak chmury obliczeniowe oferują swoim użytkownikom poziom bezpieczeństwa nieosiągalny dla większości przedsiębiorstw. Najwięksi dostawcy usług chmurowych już w tej chwili dostosowali swoje systemy do wymagań RODO.

Jednym z narzędzi pozwalających skuteczniej chronić dane osobowe jest oferowany przez Microsoft Azure Information Protection. Dzięki systemowi klasyfikowania i oznaczania plików rozwiązanie to zapobiega ich otwieraniu przez nieuprawnione osoby. Nawet, jeśli przez pomyłkę taki dokument zostanie wysłany do niewłaściwej osoby, odbiorca go nie otworzy. Również uprawnionemu adresatowi można dać możliwość otwarcia pliku tylko do odczytu oraz w określonym czasie.

Migracja do chmury obliczeniowej jest najprostszym i najtańszym sposobem na dostosowanie się do wymogów RODO. Zamiast budować coraz bardziej skomplikowane rozwiązania, które i tak zawsze będą słabsze niż zabezpieczenia internetowych gigantów, można skorzystać z ich już gotowej infrastruktury.

Cybercom Poland

6. Pytania i odpowiedzi

Skąd wzięło się RODO?

Jest to rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Od 25 maja 2018 r. obowiązuje na terenie całej Unii Europejskiej, w tym w Polsce.

Dlaczego tak ważna jest ochrona danych osobowych każdej osoby?

Ochrona danych osobowych jest przywilejem wynikającym z Karty Praw Podstawowych, w świetle dorobku prawnego UE. Ochrona ta jest jednym z podstawowych elementów praw i wolności, które to stanowią jeden z głównych celów Unii Europejskiej.

Jakie są cele tworzenia regulacji takich jak RODO?

Prawodawca unijny wskazuje, że cele które mają być osiągnięte to m.in. stworzenie przestrzeni do wolności, bezpieczeństwa i sprawiedliwości, unii gospodarczej czy też postępu społeczno-gospodarczego.

Różnice w stopniu ochrony praw i wolności osób fizycznych w państwach członkowskich, w szczególności prawa do ochrony danych osobowych – w związku z przetwarzaniem danych osobowych mogą utrudniać swobodny ich przepływ w ramach Unii. RODO ma na celu zapewnić wysoki, spójny i równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych oraz usunąć przeszkody w przepływie takich danych w Unii.

Jak dane osobowe były chronione w Unii do tej pory?

Na poziomie unijnym obowiązywała dyrektywa 95/46/WE. Akt ten został uchylony wraz z wejściem w życie RODO. Cele i zasady wyrażone w dyrektywie pozostają co prawda aktualne, jednak przy dotychczasowym jej wdrażaniu nie uniknięto negatywnych elementów, wśród których można wskazać fragmentaryzację czy też brak jednolitości w implementacji. Powszechny jest także pogląd, że ochrona osób fizycznych, w szczególności związana z działaniami w Internecie, jest zagrożona.

Czy przy braku wyrażonej zgody zakaz przetwarzania danych osobowych oznaczonych jako szczególne jest bezwzględny?

Rozporządzenie wskazuje, że należy zezwolić na wyjątki od zakazu przetwarzania szczególnych kategorii danych osobowych – o ile przewiduje to prawo Unii lub prawo państwa członkowskiego. Wyjątek musi podlegać odpowiednim zabezpieczeniom chroniącym dane osobowe i inne prawa podstawowe. Będzie miał miejsce, jeżeli uzasadnia

go interes publiczny, w szczególności polegający na przetwarzaniu danych osobowych w zakresie prawa pracy, prawa zabezpieczeń społecznych, w tym emerytur. Może wystąpić także w celach m.in bezpieczeństwa, monitorowania i ostrzegania zdrowotnego, zapobiegania chorobom zakaźnym i innym poważnym zagrożeniom zdrowotnym. Należy również przewidzieć wyjątek pozwalający przetwarzać szczególne dane osobowe, jeżeli jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń w postępowaniu sądowym, administracyjnym lub innym postępowaniu pozasądowym.

Czy ze względu na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, administrator danych może odmówić udzielenia informacji o przetwarzanych danych?

Uważa się, że prawo do ochrony danych osobowych nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym np. tajemnice handlowe lub własność intelektualną. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni takiej osobie bezpośredni dostęp do jej danych osobowych.

Jednocześnie administrator, w odpowiedzi na takie żądanie może nakazać, by osoba której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

Na czym polega nasze prawo do informacji i dostępie do zebranych o nas danych?

Każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji na ich temat, w szczególności:

- celów, w jakich dane osobowe są przetwarzane,
- okresu przez jaki dane osobowe są przetwarzane (w miarę możliwości),
- odbiorców danych osobowych,
- założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych,
- w przypadku profilowania, konsekwencji takiego przetwarzania.

Czy osoba fizyczna ma prawo do sprzeciwu wobec przetwarzania jej danych osobowych?

Nawet gdy dane osobowe są przetwarzane zgodnie z prawem, każdej osobie, której dotyczą, powinno przysługiwać prawo sprzeciwu wobec przetwarzania danych dotyczących szczególnych sytuacji. Wówczas administrator musi wykazać, że jego ważne i prawnie uzasadnione interesy mają nadrzędny charakter wobec interesów lub podstawowych praw i wolności tej osoby.

Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba której dane dotyczą, powinna mieć prawo wnieść, bezpłatnie i w dowolnym momencie, sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego. Prawo to powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji.

O czym dokładnie administrator powinien powiadomić osobę, której dane przetwarza, w razie wystąpienia naruszenia zasad ochrony danych?

Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą tak szybko, jak jest to możliwe, w ścisłej współpracy z organem nadzorczym i z poszanowaniem wskazówek przekazanych przez ten organ (lub inne odpowiednie organy, np. ścigania).

Jak zmieni się obowiązek informowania organów nadzorczych w porównaniu do obecnego stanu prawnego?

Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten, powodując obciążenia administracyjne i finansowe, nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Zgodnie z założeniami RODO nastąpi większa koncentracja na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele przetwarzania mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, np. monitoring na dużą skalę, przetwarzanie danych wrażliwych, śledzenie zachowań użytkowników w Internecie i kierowanie do nich spersonalizowanych reklam.

7. Słowniczek RODO

Administrator danych osobowych

Organ, jednostka organizacyjna, podmiot lub osoba decydująca (samodzielnie) o celach i środkach przetwarzania danych osobowych (art. 7 pkt 4).

Dane genetyczne

Jest to specyficzny rodzaj danych opisujących cechy dziedziczne osoby fizycznej. Ujawniają one unikalne informacje dotyczące stanu zdrowia oraz cech genetycznych danej osoby. Dane te można pozyskać w wyniku analizy próbki biologicznej. Źródłem takich informacji może być w szczególności analiza chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) albo analiza innych elementów umożliwiających pozyskanie równoważnych informacji.

W polskiej ustawie o ochronie danych osobowych dane genetyczne nie zostały wprost zaliczone do grupy danych wrażliwych.

Dane osobowe

Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie (art. 4 ust. 1). Zalicza się do nich między innymi: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy, czynniki określające: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane wrażliwe

Termin używany w języku potocznym, odnosi się do danych szczególnie chronionych. Przez RODO nazwane Szczególnymi Kategoriami Danych Osobowych. Będą dotyczyć danych o stanie zdrowia, pochodzeniu etnicznym, jak również kwestii światopoglądowych i danych biometrycznych. Przetwarzanie tych danych będzie prawnie zabronione poza sytuacjami gdy będzie to niezbędne do ochrony życia konkretnej osoby lub po uzyskaniu jednoznacznej zgody.

Działanie potwierdzające

Wyrażenie dotyczy ochrony danych osobowych podczas procesu rekrutacyjnego pracowników. Są to świadome czynności, które pomimo braku pisemnej zgody kandydata oznaczają zgodę na przetwarzanie jego danych. Takim postępowaniem może być np. proaktywna postawa oraz okazane zainteresowanie na zamieszczoną ofertę pracy. Działanie potwierdzające dotyczy jedynie obecnego postępowania rekrutacyjnego, nie może być rozumiane jako stała zgoda kandydata na przetwarzanie danych również w przyszłych procesach rekrutacyjnych.

Główna jednostka organizacyjna

Jednostka w której zapadają decyzje dotyczące celów i sposobów przetwarzania danych osobowych (najczęściej jest nią centralna administracja) znajdująca się na terenie UE. Powinna zostać określona na podstawie obiektywnych kryteriów takich jak np. skuteczność i faktyczność podejmowania najważniejszych decyzji przy wykorzystaniu stabilnych struktur.

Definicja głównej jednostki organizacyjnej jest silnie powiązana z regulacjami dotyczącymi grup kapitałowych. W ich przypadku należy wskazać spółkę matkę, która będzie główną jednostką organizacyjną grupy. Jednocześnie wymusi to wyznaczenie wiodącego organu nadzorczego, który będzie zajmował się sprawami związanymi z transgranicznymi procesami przetwarzania danych.

W praktyce:

Dla przykładu spółka ze Szwecji posiada kilka spółek córek w całej UE i to szwedzka spółka decyduje o zasadach przetwarzania danych osobowych w grupie kapitałowej. W związku z tym zostaje ona wskazana u szwedzkiego organu nadzorczego jako główny podmiot w grupie kapitałowej odpowiedzialny za procesy przetwarzania i ochrony danych osobowych, a szwedzki organ nadzorczy będzie organem właściwym w sprawach związanych z transgranicznym przetwarzaniem danych osobowych w ramach tej grupy kapitałowej.

Naruszenie ochrony danych osobowych

Szerokie pojęcie opisujące wszystkie sytuacje w których dochodzi do przypadkowego lub niezgodnego z prawem dostępu a w jego efekcie utracenia, zniszczenia, zmodyfikowania czy ujawnienia danych osobowych. Naruszenie ochrony danych dotyczy danych przechowywanych, przesyłanych oraz przetwarzanych. Najczęściej jako przykłady powyższych podaje się kradzież danych lub sfałszowanie tożsamości, odwrócenie pseudonimizacji, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub bezpieczeństwa danych osobowych mogące skutkować naruszeniem dobrego imienia danej osoby fizycznej, stratą finansową lub inną znaczną szkodą gospodarczą lub społeczną. Należy pamiętać, że ten termin obejmuje również przypadkowe przesłanie lub przetworzenie danych, które skutkuje ich zniszczeniem lub nieuprawnionym ujawnieniem. Takim incydentem może być dla przykładu zgubienie laptopa lub telefonu służbowego, na którym są zapisane dane osobowe kontrahentów, klientów czy dostawców.

W praktyce:

Każda organizacja powinna mieć stosowne procedury regulujące te kwestie, począwszy od zgłoszenia incydentu przez pracownika, podjęcie stosownych działań zaradczych przez zarząd (inspektora ochrony danych) i dział IT, np. zdalne usunięcie kontaktów w telefonie.

Naruszenie ochrony danych osobowych należy zgłosić organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Każdy incydent, niezwłocznie po jego wykryciu, musi zatem zostać przeanalizowany wewnętrznie w firmie, w szczególności w aspekcie konieczności jego zgłoszenia do organu nadzorczego.

Ograniczenie przetwarzania

Oznacza oznakowanie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Taka sytuacja może mieć miejsce w kilku przypadkach:

- Osoba fizyczna ma wątpliwości co do prawidłowości danych osobowych, które dana spółka przechowuje na jej temat. Zgłasza wtedy swoje uwagi spółce, która na okres wyjaśnienia sprawy, pozwalający sprawdzić zasadność wniosku i prawidłowość posiadanych przez nią danych ogranicza ich przetwarzanie.

- Administrator danych chce niezgodnie z prawem usunąć przechowywane dane, jednak osoba fizyczna sprzeciwia się temu i żąda ograniczenia ich przetwarzania.

- Dane osobowe nie są już potrzebne administratorowi, jednak są potrzebne osobie fizycznej podczas dochodzenia lub obrony roszczeń – np. w przypadku sporu pracownika z pracodawcą.

- Organy nadzorcze posiadają uprawnienia nadane im w RODO do zastosowania w stosunku do administratora czasowego lub całkowitego ograniczenia przetwarzania. W ramach uprawnień kontrolnych Prezes Urzędu Ochrony Danych Osobowych może nałożyć na administratora zakaz przetwarzania jeśli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki.

W praktyce:

Ograniczenie przetwarzania może spowodować „paraliż organizacyjny" danej firmy, zastopować jej działanie na kilka miesięcy, jeśli określone zbiory danych zostaną wyłączone spod bieżącej pracy firmy.

Organ nadzorczy

Organ wyznaczany indywidualnie i niezależnie w każdym kraju członkowskim. Jego głównym zadaniem będzie ochrona praw i wolności osób fizycznych dotyczących przetwarzania danych osobowych w Unii Europejskiej. W Polsce tę funkcję będzie pełnił Urząd Ochrony Danych Osobowych na czele z prezesem (PUODO). Dodatkowo, organ nadzorczy ma monitorować zasady przestrzegania wymogów RODO.

Podmiot przetwarzający (tzw. procesor)

Podmiot, który przetwarza dane osobowe w imieniu ich administratora. Może nim być zarówno osoba fizyczna, prawna jak i organ publiczny. RODO wprowadza definicję podmiotu, który do tej pory nie był dokładnie regulowany w polskim ustawodawstwie. Zgodnie z przepisami unijnymi procesor przetwarza dane osobowe na zlecenie administratora.

W praktyce:

Każda firma korzysta z procesorów, np. firm outsourcingowych świadczących usługi kadrowo-płacowe, finansowe, usługi hostingowe, agencje zatrudnienia. Co więcej, RODO przewiduje minimalny zakres informacji, które muszą znaleźć się w umowie pomiędzy administratorem danych a podmiotem przetwarzającym. Zatem w praktyce konieczna jest weryfikacja własnych umów i ich ewentualna renegocjacja.

Profilowanie

Automatyczne przetwarzanie danych osobowych. Wykorzystuje dane osobowe do analizy lub prognozy różnych aspektów działalności konkretnej osoby fizycznej. Analizie podlegają profile jawne, natomiast prognozie profile predykcyjne. Celem profilowania jest poznanie między innymi: efektów pracy osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Ważnym aspektem jest legalność tego przetwarzania, która będzie spełniona pod trzema warunkami:

1. prawo wyraźnie dopuszcza profilowanie,
2. profilowanie jest niezbędne do zawarcia umowy pomiędzy osobą fizyczną, a administratorem danych,
3. zgoda osoby fizycznej na przeprowadzenie profilowania. Zgoda musi jednak zostać wyrażona po uzyskaniu od administratora informacji o zasadach profilowania, ich znaczeniu oraz o przewidywanych konsekwencjach profilowania dla osoby, której dane dotyczą.

W praktyce:

Przykładami profilowania może być stosowanie określonego rodzaju plików cookies na stronie internetowej, które w powiązaniu z innymi narzędziami pozwalają śledzić określone zachowania użytkowników strony w celu proponowania im spersonalizowanych produktów, reklam, ofert handlowych, a także oceny zdolności kredytowej, leasingowej danej osoby itp.

Przedstawiciel

Podmiot wyznaczany w przypadku, gdy administrator lub procesor nie posiada jednostek organizacyjnych w UE, a świadczone przez niego usługi lub oferowane produkty są dostępne dla osób fizycznych w UE. Podmiot jest wyznaczany pisemnie przez administratora lub procesora w zgodzie z ich obowiązkami wynikającymi z RODO. Podmiotem może zostać osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę w UE.

W praktyce:

Dla przykładu, sklep internetowy z siedzibą w USA sprzedaje swoje produkty konsumentom w UE, nie mając jednocześnie swojej spółki córki w UE. Wówczas taki sklep będzie podlegać przepisom RODO i będzie musiał wyznaczyć przedstawiciela.

Przetwarzanie

Wszystkie operacje przeprowadzane na danych osobowych. Zalicza się do nich między innymi: pozyskiwanie, przechowywanie, modyfikowanie, przeglądanie, udostępnianie, upublicznianie oraz niszczenie danych.

Pseudonimizacja

Jedna z form zabezpieczenia danych osobowych zalecana przez RODO. Ma zapewniać bezpieczeństwo danych podczas ich przetwarzania oraz ograniczać ryzyko naruszenia praw lub wolności osób fizycznych. Ta forma zabezpieczeń ma polegać na przetworzeniu danych w sposób uniemożliwiający przypisanie ich konkretnej osobie. Do identyfikacji mają być niezbędne dodatkowe informacje, które będą przechowywane osobno oraz zostaną objęte środkami technicznymi uniemożliwiającymi zidentyfikowanie na ich podstawie osoby fizycznej.

W praktyce:

Dla przykładu, pseudonimizacja może polegać m.in. na zastąpieniu określonej kategorii danych innymi danymi (np. Jana Kowalskiego zmieni się na Adriana Nowaka) albo numerem identyfikacyjnym (np. Jana Kowalskiego oznaczy się numerem 2343). Działanie takie może być wskazane np. w wypadku podmiotów świadczących usługi call center. Nie jest konieczne, aby określony pracownik widział realne dane, jeśli w celu wykonywania pracy potrzebny jest mu wyłącznie np. numer telefonu.

Strona trzecia

Termin opisujący każdą osobę fizyczną lub prawną oraz wszelkie podmioty których konkretne dane osobowe nie dotyczą, ale ze względu na upoważnienia administratora lub podmiotu przetwarzającego mogą te dane przetwarzać. Pojęcie „strona trzecia" określa podmiot zewnętrzny względem operacji przetwarzania danych osobowych. W zależności od indywidualnych działań podejmowanych przy pracy nad danymi osobowymi może stać się on ich administratorem lub podmiotem przetwarzającym. Wyznacznikiem jest stopień samodzielności podejmowanych działań: gdy działa na zlecenie administratora to jest podmiotem przetwarzającym, natomiast gdy autonomicznie wyznacza sobie cele, staje się administratorem.

Ustawodawca unijny zdecydował zdefiniować pojęcie strony trzeciej od strony negatywnej.

W praktyce:

Oznacza to, że oceniając, czy dany podmiot jest stroną trzecią, należy zbadać, czy można go zakwalifikować jako jeden z podmiotów wskazanych powyżej. Jeżeli w wyniku takiej analizy zostanie stwierdzone, że dany podmiot nie jest osobą, której dane dotyczą, administratorem danych, podmiotem przetwarzającym na zlecenie administratora ani osobą, która przetwarza dane osobowe z upoważnienia administratora lub podmiotu przetwarzającego, wówczas podmiot ten będzie stroną trzecią.

Transgraniczne przetwarzanie

Opisuje ono przetwarzanie danych na terenie Unii Europejskiej, nie obejmując przesyłania ich poza granice Unii.

Wiążące reguły korporacyjne

Polityki ochrony przyjmowane przez daną grupę spółek. Mają zapewniać stosowanie jednolitego prawa dotyczącego ochrony przepływu i przetwarzania danych osobowych w całej grupie. Będą wprowadzane przez administratora lub procesora z siedzibą w UE, który przesyła dane poza granice Unii do pozostałych podmiotów grupy kapitałowej, z którymi prowadzi wspólną działalność gospodarczą.

Zgoda

Powyższy termin jest już obecny w polskim prawodawstwie, jednak nabiera on nowego, bardziej praktycznego znaczenia w obliczu RODO. Zgoda w rozumieniu nowych przepisów musi być konkretna, świadoma, dobrowolna i jednoznaczna. Zgoda na przetwarzanie danych nie musi być jednak dostarczona w pisemnej formie, może być również uzyskana poprzez wyraźne działanie potwierdzające.

W praktyce:

Oznaczać to może, że wręczenie komuś wizytówki na określonym evencie może być traktowane jako dorozumiana zgoda na kontakt w celach ofertowych. Należy mieć jednak na uwadze, że zgodnie z zasadą rozliczalności także w takim przypadku administrator danych będzie musiał wykazać, że zgoda rzeczywiście została udzielona (w związku z tym warto np. wysłać do takiej osoby maila potwierdzającego, odnotować wewnętrznie skąd jesteśmy w posiadaniu określonych danych).

8. Wsparcie oferowane przez Cybercom Poland i Rödl & Partner

Zapewnienie kompleksowego wsparcia w przypadku RODO wymaga wiedzy i umiejętności z kilku dziedzin. Dlatego w ramach współpracy Cybercom Poland i Rödl & Partner powstała grupa ekspercka zajmująca się jednocześnie aspektami prawnymi i technologicznymi tego procesu. To połączenie gwarantuje skuteczność prowadzonych działań i wysoką jakość naszej usługi doradztwa i wdrożenia zmian związanych z RODO.

AUDYT RODO

Kompleksowe zbadanie sytuacji w firmie i zaprojektowanie odpowiednich rozwiązań realizujemy w czterech etapach:

1. **Wstępne warsztaty** – zebranie informacji o celach i metodach wykorzystywania danych osobowych
2. **Audyt** – dokładne sprawdzenie infrastruktury IT oraz procesu przetwarzania danych
3. **Raport i rekomendacje** – rekomendacje prawne i technologiczne
4. **Ponowny audyt** – weryfikacja poprawności wprowadzonych procedur

jeden
kompleksowy audyt technologiczny i prawny

profesjonalne
doradztwo

unikatowe
połączenie teorii i praktyki

OUTSOURCING IOD

Inspektor Ochrony Danych pełni ważną funkcję w przedsiębiorstwie. Jest odpowiedzialny za bieżące monitorowanie przestrzegania RODO i za współpracę z Urzędem Ochrony Danych, która obejmuje udział w kontrolach, udzielanie wyjaśnień, przekazywanie dokumentów i informacji.

Oferujemy outsourcing specjalistów z dziedziny prawa i technologii, którzy zadbają o prawidłowe funkcjonowanie firmy w obliczu RODO.

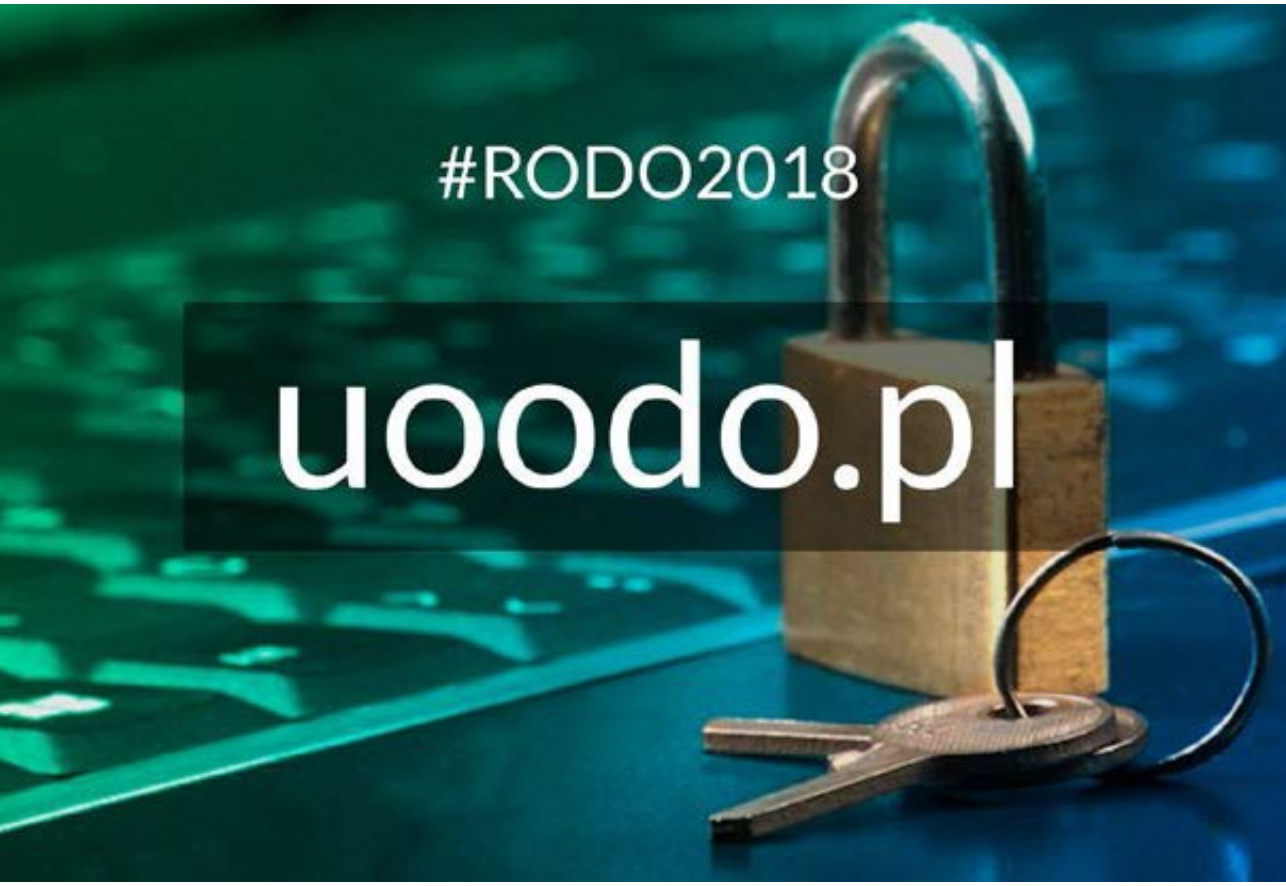
osoba kontaktowa dla Urzędu Ochrony Danych Osobowych

przeprowadza bieżące szkolenia dla pracowników z wymagań RODO

prowadzi rejestr czynności przetwarzania danych

Strona internetowa uoodo.pl

Specjaliści z Cybercom Poland i Rödl & Partner stworzyli platformę na której znajdują się informacje dla przedsiębiorców, chcących dostosować swoją firmę do wymogów nowego rozporządzenia.



Na tej stronie znajdują się najpotrzebniejsze informacje, opinie i komentarze ekspertów oraz dane kontaktowe do naszych specjalistów.

Szczegóły dotyczące usługi oraz więcej informacji znajdziesz na stronie: **uoodo.pl**

Rödl & Partner

Rödl & Partner to międzynarodowa firma świadcząca zintegrowane usługi profesjonalne w obszarach: audyt, Business Process Outsourcing, doradztwo podatkowe, doradztwo prawne, consulting. Rödl & Partner obecny jest w 51 krajach w 111 biurach. Na rynku polskim funkcjonuje z powodzeniem od ponad 25 lat, doradzając firmom z różnych branż i segmentów.

Rödl & Partner

Gdańsk
tel.: + 48 58 520 38 73
e-mail: gdansk@roedl.pro

Poznań
tel.: + 48 61 864 49 00
e-mail: poznan@roedl.pro

Gliwice
tel.: + 48 32 330 12 00
e-mail: gliwice@roedl.pro

Warszawa
tel.: + 48 22 696 28 00
e-mail: warszawa@roedl.pro

Kraków
tel.: + 48 12 378 66 00
e-mail: krakow@roedl.pro

Wrocław
tel.: + 48 71 606 00 00
e-mail: wroclaw@roedl.pro

www.roedl.pl