

Wymiana doświadczeń

Zuzanna Kosakowska – Administrator Bezpieczeństwa Informacji

Warszawa, 2017-04-21



**Ochrona danych osobowych oraz
danych medycznych –zmiany w prawie
oraz rola Administratora
Bezpieczeństwa Informacji**



Czym jest GDPR / RODO?

„GDPR”, zwane także „RODO” lub „Ogólnym Rozporządzeniem o Ochronie Danych” to Rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE1.



Od kiedy GDPR zacznie obowiązywać?

Rozporządzenie weszło w życie 17 maja 2016 r.

Zacznie ono obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r. Rozporządzenie wiązać będzie wszystkich, którzy przetwarzają dane osobowe w związku z prowadzoną działalnością gospodarczą.

Należy pamiętać, że przepisy RODO weszły już w życie, ale stosować mamy je od 25 maja 2018 roku.



Czy to oznacza, że do tego czasu nie musimy robić nic czy przygotowania do stosowania przepisów należy rozpocząć już dziś?

Przede wszystkim, **przepisy RODO nie przewidują okresu przejściowego.**

Z jednej strony, **roczny okres (dokładnie 13 miesięcy)**, który pozostało o rozpoczęcia ich stosowania to czas dla krajowego ustawodawcy, który powinien być wykorzystany na rewizję przepisów krajowych.

Z drugiej, **to czas dla administratorów danych i podmiotów przetwarzających dane do wykonywania nowych obowiązków.**



**25 maja 2018 roku administratorzy danych muszą
wykazać się pełną zgodnością
z przepisami rozporządzenia ogólnego.**

**Dlatego tak ważne jest, żeby przygotowania do
stosowania przepisów rozpocząć już dziś.**



Przepisy RODO zastąpią ustawę o ochronie danych osobowych, a w raz z nią przestaną obowiązywać rozporządzenia wykonawcze wydane na jej podstawie.



**28 marca 2017 r. Ministerstwo Cyfryzacji opublikowało
Projekt ustawy o ochronie danych osobowych**

<https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych>

Przepisy nowej ustawy o ochronie danych osobowych, mają zapewnić skuteczne stosowanie w polskim porządku prawnym rozporządzenia ogólnego o ochronie danych.



Udostępnieniu przez Ministra Cyfryzacji podlega projekt części przepisów regulujących:

- zagadnienia ogólne (niektóre przepisy),
- zagadnienia związane z postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych,
- europejską współpracą administracyjną,
- zagadnienia związane z postępowaniem kontrolnym,
- zagadnienia związane z administracyjnymi karami pieniężnymi, odpowiedzialnością cywilną
- regulacje w zakresie inspektorów ochrony danych.



Czekamy na projekty zmian w przepisach branżowych w tym w przepisach w zakresie ochrony zdrowia.

Tam gdzie przepis krajowy nie będzie wprowadzał odmiennych regulacji tam wprost stosowane są zapisy Rozporządzenia



Rozporządzenie ogólne przewiduje zamknięty katalog autonomicznych przesłanek przetwarzania danych zwykłych, do których zaliczane są:

1. zgoda osoby, której dane dotyczą obejmująca przetwarzanie w jednym lub większej liczbie celów

2. Niezbędność przetwarzania do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na wniosek tej osoby przed zawarciem umowy

3. Niezbędność przetwarzania do wypełnienia obowiązku prawnego ciążącego na administratorze

4. Niezbędność przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej

5. Niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

6. niezbędnosc przetwarzania do celów wynikających z uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych w szczególności, gdy osoba, której dane dotyczą jest dzieckiem

I. Poszerzony zakres stosowania

Rozporządzenie znajdzie zastosowanie do administratorów i podmiotów przetwarzających dane osobowe z siedzibą w Unii Europejskiej, jak również (co stanowi, co do zasady, nowość) poza jej granicami.

W przypadku podmiotów spoza UE, Rozporządzenie będzie stosowane w przypadku przetwarzania danych osób przebywających w UE, jeśli przetwarzanie będzie związane z oferowaniem takim osobom towarów lub usług lub jeśli będzie ono związane z monitorowaniem ich zachowania w UE.



II. Zasada One-Stop-Shop

W przypadku przetwarzania danych osobowych w więcej niż jednym państwie UE (również w przypadku posiadania przez administratora jednostek organizacyjnych w różnych państwach UE), organ nadzoru właściwy dla głównej jednostki organizacyjnej będzie zasadniczo działał jako wiodący organ we wszystkich sprawach dotyczących transgranicznego przetwarzania danych osobowych przez tego przedsiębiorcę.



III. Definicja danych osobowych

Definicja danych osobowych została doprecyzowana poprzez uwzględnienie wprost jako danych osobowych m.in. danych o lokalizacji, identyfikatora internetowego czy znaków szczególnych związanych z tożsamością fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną.



Rozporządzenie zachowuje znany dotychczas model zaostrożenia rygoru przetwarzania danych wrażliwych (szczególnych kategorii danych).

Zasadą jest zakaz przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby lub danych dotyczących zdrowia lub seksualności i orientacji seksualnej, a także danych o wyrokach skazujących i o przestępstwach.



Rozporządzenie precyzuje czym są dane o stanie zdrowia

Zgodnie z art. 4 pkt 15 RODO „*dane dotyczące zdrowia*” oznaczają *dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.*

W motywie 35 twórcy rozporządzenia RODO wyjaśniają, że *do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE (1); numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.*



Możliwość przetwarzania danych wrażliwych w tym danych o stanie zdrowia dopuszczona jest, gdy spełniono co najmniej jeden wymienionych w Rozporządzeniu wyjątków.

W przypadku usługodawców w zakresie opieki zdrowia jest to przesłanka :
niezbędność przetwarzania do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub społecznej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub społecznej na podstawie prawa Unii lub prawa krajowego lub zgodnie z umową z pracownikiem służby zdrowia.



IV. Rozszerzone obowiązki podmiotów zobowiązanych

a. Zgoda.

Zgoda na przetwarzanie danych musi być udzielona w formie oświadczenia lub wyraźnego działania, stanowiących przejaw dobrowolnego, konkretnego, świadomego i jednoznacznego przejawu woli, potwierdzającego przyzwolenie na przetwarzanie przez podmiot danych osobowych. Jeżeli osoba, której dane dotyczą, wyrażą zgodę na przetwarzanie danych w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę powinno zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, a także jasnym i prostym językiem.



b. Zgoda na przetwarzanie danych dziecka.

Do przetwarzania na podstawie zgody danych dziecka poniżej szesnastego roku życia konieczne będzie uzyskanie zgody jego opiekuna prawnego.

c. Powiadomianie o naruszeniach bezpieczeństwa danych osobowych.

W przypadku naruszenia zabezpieczeń danych osobowych, administratorzy będą zobowiązani niezwłocznie powiadomić o tym fakcie właściwy organ nadzoru, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – administratorzy będą musieli powiadomić o naruszeniu w jasny i prosty sposób również osoby, których dane są przetwarzane.



d. Dodatkowe obowiązki dla podmiotów przetwarzających dane osobowe.

Rozporządzenie nakłada szereg obowiązków bezpośrednio na podmioty przetwarzające dane osobowe – tj. na podmioty niebędące administratorami danych, a przetwarzające dane osobowe szczególnie na podstawie powierzenia przetwarzania przez administratorów.

Podmioty przetwarzające będą bezpośrednio odpowiedzialne za bezpieczeństwo danych osobowych w trakcie ich przetwarzania.

e. Obowiązki informacyjne.

Poszerzeniu ulega katalog informacji, które administratorzy zobowiązani będą dostarczyć podmiotom danych, a także – sprecyzowany zostaje sposób ich dostarczenia (tj. przy użyciu jasnego i prostego języka w sposób zwięzły, przejrzysty, czytelny i łatwo dostępny).



f. Ograniczenie profilowania

Profilowanie (tj. zautomatyzowane przetwarzanie danych osobowych, polegające na wykorzystaniu tych danych do oceny niektórych czynników osobowych osoby fizycznej, np. w celu analizy preferencji, czy też zachowań) będzie legalne jedynie wtedy, gdy administrator danych wykáže, że ma podstawę prawną do takiego działania np. wyraźną zgodę.

g. Wdrożenie programu zgodności przetwarzania danych.

Administratorzy będą musieli wprowadzić właściwe środki techniczne i organizacyjne, aby zapewnić i wykazać, że przetwarzanie danych osobowych jest wykonywane zgodnie z przepisami Rozporządzenia.



h. Inspektor ochrony danych osobowych.

Rozporządzenie wprowadza instytucję inspektora ochrony danych osobowych, którego zadaniem będzie zapewnienie zgodności działalności przedsiębiorcy z przepisami o ochronie danych osobowych.

i. Privacy impact assesment - ocena skutków przetwarzania danych dla prywatności.

W przypadku, gdy przetwarzanie danych osobowych niosło będzie za sobą wysokie ryzyko naruszenia praw i wolności podmiotów danych, administrator musiał będzie dokonać oceny skutków przetwarzania danych z perspektywy prywatności przed rozpoczęciem przetwarzania.



j. Ochrona prywatności by design i by default.

Rozporządzenie nakazuje administratorom danych wzięcie pod uwagę aspektu ochrony danych osobowych już od momentu projektowania nowych produktów oraz oceny ryzyka dla bezpieczeństwa danych osobowych przed wprowadzeniem ich na rynek.

Administrator danych wybierać takie rozwiązania, które domyślnie zapewniają przetwarzanie danych osobowych tylko w niezbędnym zakresie.



V. Uprawnienia osób fizycznych.

Rozporządzenie reguluje też kwestię uprawnień osób fizycznych do ochrony ich danych, w szczególności w następujących obszarach:

a. Prawo do przeniesienia danych.

Osoba fizyczna będzie miała prawo otrzymać od administratora swoje dane w ustrukturyzowanej formie, a także, o ile jest to technicznie możliwe, nakazać przesłanie danych innemu administratorowi.

b. Prawo sprzeciwu.

Podmioty, których dane są przetwarzane w interesie publicznym lub w związku z uzasadnionym interesem administratora będą mogły sprzeciwić się takiemu przetwarzaniu danych, chyba że administrator wykaże że podstawa do przetwarzania danych jest nadrzędna w stosunku do interesów jednostki.



c. Prawo do bycia zapomnianym.

Prawo do bycia zapomnianym – tj. prawo żądania usunięcia danych przez administratora, zostało wyraźnie określone w Rozporządzeniu i stanowi ono odzwierciedlenie najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej.

d. Wnoszenie skarg.

Rozporządzenie daje podmiotom danych prawo do składania skarg na działania administratorów i podmiotów przetwarzających dane. . Skargę będzie można złożyć do organu nadzoru (w Polsce do GIODO) w państwie pobytu lub pracy osoby fizycznej lub w państwie popełnienia naruszenia. Od decyzji organów nadzoru przysługiwać będzie odwołanie do sądu.

e. Prawo do odszkodowania.

Podmioty danych będą miały prawo do uzyskania odszkodowania za szkody majątkowe i niemajątkowe wynikające z naruszenia przez administratorów lub podmioty przetwarzające dane przepisów Rozporządzenia.



VI. Zwiększone uprawnienia organów i kary.

Organy nadzoru otrzymają szersze uprawnienia i możliwości działania w stosunku do nadzorowanych podmiotów. Możliwe będzie także bezpośrednie nakładanie kar za naruszenia.

Maksymalne wysokości kar przewidzianych w Rozporządzeniu będą kilkaset razy wyższe od obecnie obowiązujących progów, tj. maksymalnie do 20.000.000 EUR lub do 4% rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego.



Jakie będą nowe obowiązki związane z zabezpieczeniem danych osobowych?



Wiele obowiązków, przewidzianych dla administratorów na gruncie ustawy o ochronie danych osobowych, pozostanie w swej istocie niezmiennymi również po 25 maja 2018 r. (np. obowiązek informacyjny wobec podmiotów danych).

Co istotne, przepisy RODO przewidują dla administratorów danych również nowe zadania, zaś kilka obowiązków (w tym te szczególnie uciążliwe dla administratorów) przejdzie do historii.



Po 25 maja 2018 nie będzie trzeba:

- a. Prowadzić, w znanej z obecnie obowiązującego Rozporządzenia, dokumentacji ochrony danych osobowych w dotychczasowej postaci.
RODO nie przewiduje wprost zobowiązania Administratora Danych do opracowywania, wdrażania do stosowania i prowadzenia:
 - polityki bezpieczeństwa
 - instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych odpowiadającym wymogom szczegółowo określonym w przepisach prawa.
- b. RODO nie przewiduje wprost nadawania na piśmie upoważnień do przetwarzania danych osobowych.
- c. RODO nie przewiduje prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.
- d. Zapewniać spełnienia ściśle określonych w przepisach prawa wymagań technicznych czy informatycznych w przypadku przetwarzania danych osobowych przy użyciu systemu informatycznego.
Zniknie obowiązek przestrzegania ściśle określonych środków bezpieczeństwa, np. stosowania haseł składających się z co najmniej 6 lub 8 znaków oraz zmiany tych haseł do systemów informatycznych co 30 dni.

Ale...



Po 25 maja 2018 nie będzie trzeba:

- e. Zgłaszać zbiorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Zbiorów danych nie będzie trzeba zgłaszać do rejestracji w nowym GIODO niezależnie od tego, czy zawierały dane osobowe zwykłe, czy dane osobowe wrażliwe. Organ nadzorczy nie będzie prowadził jawnego rejestru zbiorów danych.

Ale.....



Jakie będą nowe obowiązki związane z zabezpieczeniem danych osobowych?

Stosownie do przepisów RODO, administrator zobowiązany jest do zapewnienia odpowiedniego stopnia bezpieczeństwa przetwarzanych danych osobowych. Przepisy RODO nie zawierają przy tym precyzyjnych wskazówek, jakie to konkretnie środki mając być w tym celu stosowane.

Ich wybór w całości pozostawiony został administratorowi.

Dokonując wyboru środków technicznych i organizacyjnych administrator powinien wcześniej ocenić czy gwarantowany przez te środki stopień bezpieczeństwa będzie adekwatny do ryzyka wiążącego się z przetwarzaniem danych osobowych. Dla zabezpieczenia danych w sposób zgodny z przepisami RODO, kluczowe znaczenie będzie miało rzetelne ocenienie ryzyka związanego z przetwarzaniem danych. Ocena ta, a w konsekwencji również dobranie adekwatnych środków bezpieczeństwa powinny być dokonywane przy uwzględnieniu wymienionych w RODO czynników.



Co należy uwzględnić wdrażając środki zabezpieczające dane osobowe:

- aktualny stan wiedzy technicznej
- koszt wdrażania środka
- charakter, zakres, kontekst i cele przetwarzania danych osobowych
- ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia
- ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych



PRZYKŁADOWE ŚRODKI BEZPIECZEŃSTWA WEDŁUG RODO:

pseudonimizacja i szyfrowanie danych osobowych

środki zdolne do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania

środki zdolne do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania



Istotnymi, z perspektywy bezpieczeństwa danych, nowościami na gruncie RODO są: obowiązek uwzględniania ochrony danych w fazie projektowania (privacy by design) oraz obowiązek realizowania domyślnej ochrony danych (privacy by default).

PRIVACY BY DESIGN:

Na etapie projektowania urządzenia, systemu lub oprogramowania (np. aplikacji bądź platformy internetowej), w wyniku używania którego dochodzić będzie do przetwarzania danych osobowych, należy uwzględniać potrzebę zapewnienia ochrony tym danym, wdrażając w tym celu odpowiednie środki techniczne i organizacyjne (np. minimalizacja danych czy odpowiednie zabezpieczenia).

PRIVACY BY DEFAULT:

Obowiązkiem jest wdrożenie takich środków technicznych i organizacyjnych, które zapewnią, aby domyślnie zbierane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu.

Stosowanie tego obowiązku ograniczyć ma ilość zbieranych danych, zakres ich przetwarzania, okres przechowywania oraz ich dostępność.



Istotną nowością jest również rezygnacja z wymogu prowadzenia wykazu zbiorów danych jako elementu polityki bezpieczeństwa oraz obowiązku zgłaszania zbiorów danych do rejestracji GIODO.

Na gruncie RODO zostały one zastąpione obowiązkiem rejestrowania czynności przetwarzania danych.



W rejestrze czynności przetwarzania muszą znaleźć się m.in. następujące informacje:

INFORMACJE ZAMIESZCZANE W REJESTRZE CZYNNOSCI PRZETWARZANIA:

- Imię i nazwisko lub nazwę oraz dane kontaktowe administratora (oraz współadministratorów, przedstawiciela administratora oraz inspektora ochrony danych).
- Cele przetwarzania danych.
- Opis kategorii osób, których dane dotyczą, oraz kategorii danych ich dotyczących.
- Kategorie odbiorców, którym dane zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych.



INFORMACJE ZAMIESZCZANE W REJESTRZE CZYNNOSCI PRZETWARZANIA:

- Gdy ma to zastosowanie, informacje o transferach danych osobowych do państw trzecich lub organizacji międzynarodowej, ze wskazaniem tych państw lub organizacji (wraz z udokumentowaniem odpowiednich środków bezpieczeństwa).
- Planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe.
- Ogólny opis stosowanych technicznych i organizacyjnych środków bezpieczeństwa zapewniających bezpieczeństwo danych osobowych – jeżeli jest to możliwe.
- Forma prowadzenia rejestru czynności przetwarzania:
Pisemna, w tym elektroniczna.



INFORMACJE ZAMIESZCZANE W REJESTRZE CZYNNOSCI PRZETWARZANIA:

- Kto jeszcze jest zobowiązanych do prowadzenia rejestru:
Przedstawiciel administratora Podmiot przetwarzający (procesor)
- Podmioty wyłączone z obowiązku: Przedsiębiorca lub podmiot zatrudniający mniej niż 250 osób.
- Wyłączenie to nie dotyczy jednak trzech przypadków:
 - gdy dokonywane przez te podmioty przetwarzanie danych może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą;
 - przetwarzanie danych nie ma charakteru sporadycznego;
 - przetwarzanie dotyczy szczególnych kategorii danych (danych wrażliwych) lub danych dotyczących wyroków skazujących za przestępstwa i naruszeń prawa.



Kto będzie mógł pełnić funkcję inspektora ochrony danych i jakie będzie miał zadania?



Od 25 maja 2018 roku trzy kategorie administratorów oraz podmiotów przetwarzających w imieniu administratora będą musiały powoływać inspektorów ochrony danych. Powołanie inspektora będzie obligatoryjne dla:

1. Organów i podmiotów publicznych z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2. Podmiotów, których główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę;
3. Administratorzy, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych dotyczących wyroków skazujących i naruszeń prawa.



Inspektor ochronnych danych osobowych wyznaczany jest zgodnie z RODO na podstawie kwalifikacji zawodowych i wiedzy, nie tylko na temat prawa, ale i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania powierzonych mu zadań. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego, ale może też wykonywać swoje zadania na podstawie umowy o świadczenie usług.



Artykuł 38 rozporządzenia ogólnego wskazuje, jaki jest status inspektora ochrony danych. Inspektor nie może otrzymywać instrukcji dotyczących wykonywanych przez niego zadań.

Nie może być też odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor musi też podlegać bezpośrednio najwyższemu kierownictwu.

Warto zwrócić uwagę na fakt, że przepisy rozporządzenia wymagają też tego, by administrator oraz podmiot przetwarzający wspierali inspektora ochrony danych w wypełnianiu przez niego zadań.

To wsparcie oznaczać ma zapewnienie zasobów niezbędnych do wykonania zadań inspektora, dostęp do danych i operacji przetwarzania oraz, co bardzo ważne, zasoby niezbędne do utrzymania wiedzy fachowej inspektora.



Zgodnie z RODO, zadania inspektora ochrony danych obejmują:

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia ogólnego oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie
2. Monitorowanie przestrzegania RODO oraz innych przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty
3. Udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania tej oceny
4. Współpraca z organem nadzorczym
5. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami.



Jak krajowe prawo postrzega nowych Inspektorów a starych ABI?

W ocenie projektodawcy najwłaściwszym rozwiązaniem, jest przesądzenie wprost, że osoby wykonujące w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, pełnią funkcję inspektora ochrony danych do dnia 1 września 2018 r.

Do tego czasu, każdy z inspektorów ochrony danych ma czas na podjęcie decyzji o dalszym pełnieniu takiej funkcji (i dokonaniu stosowanego zawiadomienia do Prezesa Urzędu).

W razie braku do tego czasu jakiegokolwiek aktywności z ich strony, w dniu 1 września 2018 r. z mocy prawa przestaną pełnić funkcję inspektorów ochrony danych.



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 1. Rozpoznaj obecną sytuację

Zanim skupisz się na konkretnych wymogach Rozporządzenia, dobrze będzie rzucić okiem na obecnie funkcjonujące w Twojej firmie zasady ochrony prywatności i [danych osobowych](#).

Przeprowadź analizę dokonanych sprawdzeń, posiadanej dokumentacji. Zdobywaj wiedzę w zakresie nowych regulacji, interpretacji przepisów. Śledź pojawiające się poradniki w zakresie realizacji RODO.



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 2. Przyjrzyj się również samym danym, które twoja jednostka przetwarza

Zadaj sobie cztery proste pytania:

1. Czy dane, które przetwarzam są nadal potrzebne?
2. Czy nie archiwizujecie danych dłużej niż jest to wymagane?
3. Czy dysponujecie zgodami udzielonymi przez Klientów?
4. Czy przechowujecie dane w sposób bezpieczny?

Jeśli nie potrzebujesz już jakichś danych – nie zatrzymuj ich! Tutaj mniej oznacza więcej. Warto też zidentyfikować osobę lub osoby w Twojej organizacji, które będą odpowiadać za zgodność w zakresie ochrony danych.



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 3. Pozyskaj wymagane zgody

Na obecnym etapie warto skupić się na pozyskaniu zgód na przetwarzanie ich danych, jeżeli to zgoda jest stosowaną w danym procesie przesłanką legalności. Oczywiście mowa jest o pozyskaniu zgód w formie wskazanej w RODO. Oznacza to m.in., jak wyjaśnił brytyjski organ ds. ochrony danych, że „Ważne jest, aby zgoda na zbieranie danych i ich użycie w określonym celu była widoczna, a nie ukryta w umowie z użytkownikiem”.

Dlatego bardzo ważne jest dokonanie już teraz oceny, w jaki sposób zgody są pozyskiwane, a także w jaki sposób spełniany jest obowiązek informacyjny wobec osób, których dane dotyczą.



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 4. Privacy by Design, czyli bezpieczeństwo uwzględnione w fazie projektowania

Jeśli już teraz uwzględniysz kwestie prywatności w planowanych działaniach i projektach, to w 2018 roku będziesz w stanie zapewnić, że są one zgodne z europejskimi standardami RODO.

Planując działania weź pod uwagę:

konieczność przechowywania danych, środki zabezpieczające [dane osobowe](#), anonimizacje danych, itp.



Materiały z którymi warto się zapoznać:

[Wytyczne GIODO Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych](#)

[Wytyczne Grupy Roboczej art. 29 dotyczące inspektorów ochrony danych \(WP 243\)](#)

Baza wiedzy portalu GDPR.pl



Dziękuję za uwagę.

e-mail: wspolpraca-regiony@csioz.gov.pl

