GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Rok do RODO – sprawdzian gotowości

Przygotowany przez GIODO zestaw pytań pozwoli każdemu administratorowi danych ocenić stan swojej gotowości do reformy systemu ochrony danych osobowych.

Dokładnie na rok przed rozpoczęciem stosowania ogólnego rozporządzenia o ochronie danych osobowych Generalny Inspektor Ochrony Danych Osobowych (GIODO) przygotował zestaw pytań, który ma pomóc administratorom danych w ocenie stanu ich przygotowania do stosowania nowego prawa.

Trzeba bowiem pamiętać, że rozporządzenie znacząco zmieni dotychczasowe podejście do ochrony danych, administratorów danych w większym niż dotąd stopniu czyniąc podmiotami odpowiedzialnymi za zgodne z prawem przetwarzanie danych osobowych.
Oznacza to, iż muszą oni dokonać szczegółowej weryfikacji stosowanych dotychczas rozwiązań z zakresu ochrony danych osobowych i w wielu przypadkach je zmodyfikować.

Jednocześnie muszą być przygotowani na właściwą realizację zwiększonych praw osób, których dane dotyczą. Niestosowanie się do nowych zasad przetwarzania danych osobowych może m.in. skutkować odpowiedzialnością finansową – administracyjnymi karami pieniężnymi nawet do 20 milionów euro lub 4% całkowitego rocznego światowego obrotu albo odpowiedzialnością cywilną, gdyż osoby, których dane dotyczą, będą miały prawo dochodzić od administratora danych lub podmiotu przetwarzającego odszkodowania za szkodę majątkową lub niemajątkową spowodowaną naruszeniem przepisów rozporządzenia.

Zatem rok do rozpoczęcia stosowania nowych zasad przetwarzania danych osobowych to najwyższy czas, by sprawdzić stan swojej wiedzy w tym zakresie i przeanalizować, czy wszystkie stosowane rozwiązania, procedury czy formularze są z nimi zgodne.
Pomocny w dokonaniu takiego przeglądu może być przygotowany przez GIODO zestaw pytań, będący jednocześnie wskazaniem najważniejszych zagadnień i obszarów, w których następować będą znaczące zmiany.

Jednocześnie warto pamiętać, że materiał ten wskazuje jedynie na podstawowe kwestie, o których mowa w rozporządzeniu o ochronie danych osobowych. Tymczasem pod uwagę często trzeba będzie brać m.in. Wytyczne Grupy Roboczej Art. 29 (w przyszłości Europejskiej Rady Ochrony Danych), których polskie wersje językowe GIODO już teraz sukcesywnie zamieszcza na swojej stronie internetowej.

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Czy jesteś gotowy na RODO?

Generalny inspektor Ochrony Danych Osobowych

1. Reforma przepisów o ochronie danych osobowych

Czy wiesz, kiedy zacznie obowiązywać ogólne rozporządzenie o ochronie danych oraz jakie podstawowe zmiany wprowadza?

2. Nowe podejście do ochrony danych osobowych

Czy słyszałeś o zasadzie rozliczalności i wiesz, jak wykazać zgodność z przepisami rozporządzenia?

3. Zakres przetwarzanych informacji

Czy dokonałeś audytu przygotowawczego, odpowiadającego na pytania, jakie dane osobowe i na jakiej podstawie prawnej przetwarzasz?

4. Nowe obowiązki informacyjne

Czy wiesz, jakie zmiany nastąpią w dopełnianiu obowiązku informacyjnego?

5. Uprawnienia osób, których dane dotyczą

Czy znasz prawa osób, których dane dotyczą? Czy jesteś gotowy na realizacje wniosków z ich strony, dotyczących np. przeniesienia danych czy prawa do bycia zapomnianym?

6. Zgoda na przetwarzanie danych

Czy zadbałeś by pozyskiwane przez Ciebie zgody na przetwarzanie danych osobowych były dostosowane do wymogów rozporządzenia?

7. Zabezpieczenia

Czy zdecydowałeś, jakie środki techniczne i organizacyjne zastosujesz, by zapewnić bezpieczeństwo danych osobowych i zgodności z przepisami ogólnego rozporządzenia?

8. Dokumentacja przetwarzania danych.

Czy jesteś gotów do rejestracji czynności przetwarzania danych?

9. Privacy by design i Privacy by default

Czy znasz koncepcje ochrony danych w fazie projektowania oraz domyślnej ochrony danych i czy uwzględniłeś je w swoich działaniach?

10. Ocena skutków dla ochrony danych

Czy sprawdziłeś czy jesteś zobowiązany do dokonania oceny skutków w zakresie ochrony danych i wiesz, jak ja przeprowadzić?

11. Dane osobowe dzieci

Czy, świadcząc e-usługi, przetwarzasz dane osobowe dzieci i wiesz, jak pozyskiwać zgodę na przetwarzanie ich danych osobowych?

12. Automatyczne przetwarzanie danych oparte na profilowaniu

Czy dokonujesz profilowania osób? Jeśli tak, to czy wiesz, jakie warunki musisz spełnić, aby działanie to było legalne?

13. Naruszenia ochrony danych

Czy jesteś gotowy do wykrycia, analizy i zgłoszenia naruszenia ochrony danych? Czy wiesz, jakie działania musisz podjąć w przypadku wystąpienia takiego incydentu?

14. Inspektor ochrony danych (obecnie ABI)

Czy sprawdziłeś, czy jesteś zobowiązany do wyznaczenia inspektora ochrony danych?

15. Transgraniczne przetwarzanie danych

Jeśli Twoja firma prowadzi działalność w skali międzynarodowej, to czy wiesz, który organ będzie Twoim organem wiodącym?

16. Powierzenie danych

Czy dokonałeś analizy dotychczasowych urnów powierzenia, tak by podmioty przetwarzające (procesorzy) spełniały wszystkie wymagania wynikające z rozporządzenia?

17. Podnoszenie wiedzy na temat ogólnego rozporządzenia.

Czy rozpocząłeś już podnoszenie świadomości swoich pracowników co do nowych rozwiązani w zakresie ochrony danych osobowych?

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

1. Reforma przepisów o ochronie danych osobowych.

Ogólne rozporządzenie o ochronie danych weszło w życie w maju ubiegłego roku, będziemy je jednak stosować od 25 maja 2018 r.

Z uwagi na szczególny charakter prawny rozporządzenia, oznaczać to będzie, że wszystkie materialne przepisy tego dokumentu będą od tego dnia obowiązywać bezpośrednio i będą miały bezpośredni skutek. Zatem wszystkie obowiązki administratorów danych będą musiały być wykonywane już od 25 maja przyszłego roku. Wtedy tez osoby, których dane przetwarzamy będą mogły korzystać przysługujących im nowych uprawnień, takich jak prawo do przenoszenia danych, czy prawo do bycia zapomnianym.

Choć rozporządzenie będzie stosowane bezpośrednio to jednak pozostają obszary, które wymagają działań na poziomie krajowym, np. zmiany przepisów sektorowych – tak by wszystkie akty prawne regulujące przetwarzanie danych osobowych w Polsce były 25 maja 2018 r. zgodne z ogólnym rozporządzeniem o ochronie danych osobowych. Prace te koordynuje Ministerstwo Cyfryzacji.

Pakiet reformujący ramy prawne ochrony danych osobowych w UE obejmuje nie tylko ogólne rozporządzenie o ochronie danych, lecz również dyrektywę regulującą przetwarzanie danych osobowych przez wymiar sprawiedliwości i organy ścigania. Z tego względu właściwe wdrożenie nowych ram prawnych powinno uwzględniać oba akty prawne tak, aby przyszły system ochrony danych osobowych był spójny, co wymaga właściwej koordynacji tych działań w obrębie rządu.

Zapraszamy do odwiedzin dedykowanej zakładki na stronie Biura GIODO – „Reforma przepisów”. Będziemy tam umieszczać wszystkie stanowiska GIODO dotyczące wdrażania ogólnego rozporządzenia, jak również najnowsze wytyczne, opinie i wskazówki mające pomoc administratorom danych lepiej przygotować sie do stosowania nowych przepisów.

2. Nowe podejście do ochrony danych osobowych.

O ile podstawowe rozwiązania ogólnego rozporządzenia o ochronie danych osobowych trudno uznać za rewolucyjne, o tyle zaprezentowane w tym dokumencie podejście do ich praktycznego zastosowania jest już pewną rewolucja. Nie zmieniają się bowiem w sposób istotny podstawy prawne czy zasady przetwarzania danych osobowych. Jednak rewolucyjny charakter ma wprowadzenie nowych zasad, które zwiększają samodzielność, ale i odpowiedzialność administratorów danych.

W praktyce oznacza to np., ze obecne przepisy przewidujące ogólny obowiązek zawiadamiania GIODO o przetwarzaniu danych osobowych (obowiązek zgłaszania zbiorów do rejestracji) przestają obowiązywać. W ich miejsce ogólne rozporządzenie wprowadza skuteczne procedury i mechanizmy koncentrujące się na tych operacjach przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw lub wolnosci osób fizycznych. Wyrażone w rozporządzeniu podejście oparte na ryzyku (ang. risk based approach) okresla sposób, w jaki należy podchodzić do przetwarzania danych – w każdej sytuacji, kiedy zbieramy i korzystamy z danych osobowych, musimy przede wszystkim analizować ryzyko, jakie może to spowodować dla prywatności osób, których te dane dotyczą.

Zupełnie nowa zasada w systemie ochrony danych wprowadzona przez rozporządzenie jest zasada rozliczalności (ang. accountability). Zgodnie z nią, na każdym administratorze danych spoczywa obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających zgodność w wymogami rozporządzenia (np. wprowadzenie rozwiązań umożliwiających realizacje praw osób, których dane dotyczą). Rozporządzenie nie podaje jednak konkretnych przykładów najlepszych rozwiązań. Nie określa tez minimalnych standardów technicznych mających na celu zabezpieczenie danych (zachęca jedynie do skorzystania z narzędzi pseudonimizacja czy też szyfrowania danych). Co istotne, przestanie też obowiązywać rozporządzenie MSWiA określające warunki techniczne i organizacyjne, jakie musza spełniać urządzenia i systemy informatyczne wykorzystywane do przetwarzania danych osobowych. Od 25 maja 2018 r. każdy administrator - biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolnosci osób fizycznych -

będzie musiał samodzielnie zdecydować, jakie zabezpieczenia, dokumentacje i procedury przetwarzania danych wdrożyć.

Pomocne w podjęciu decyzji w tym zakresie mogą być wskazane w rozporządzeniu instrumenty, takie jak zatwierdzane przez GIODO tzw. kodeksy postępowania, a także mechanizm certyfikacji, wytyczne Europejskiej Rady Ochrony Danych lub sugestie inspektora ochrony danych. Ponadto źródłem praktycznej i sprawdzonej wiedzy w zakresie budowy i zarzadzania środkami bezpieczeństwa mogą być również np. normy ISO.

Innym aspektem zasady rozliczalności jest wykazanie przez administratora przestrzegania prawa, np. poprzez udokumentowane wdrożenie instrumentów prawnych określonych w rozporządzeniu, takich jak przeprowadzona ocena skutków dla ochrony danych, wdrożenie zasady privacy by design i privacy by default lub tez stosowanie przytoczonych wyżej zatwierdzonych kodeksów postępowania.

3. Zakres przetwarzanych informacji.

Przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już sie toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów.

Tak sformułowane zdanie motywu 171 ogólnego rozporządzenia o ochronie danych jest bardzo wyraźnym wskazaniem, że to właśnie teraz jest czas na dokonywanie przeglądu i weryfikacji stosowanych dotychczas rozwiązań z zakresu ochrony danych osobowych.

Zanim jeszcze będziemy stosować rozporządzenie, warto żebyś dokonał swego rodzaju audytu przygotowawczego i udokumentował, jakie dane osobowe przetwarzasz, skąd pochodzą i co cię uprawnia do ich wykorzystywania, czy i komu je udostępniasz oraz jak zabezpieczasz. Rzetelnie przeprowadzona analiza wszystkich operacji przetwarzania danych w organizacji będzie pierwszym krokiem do prowadzenia rejestru czynności przetwarzania, który od 25 maja 2018 r. będzie obowiązkowy dla wielu podmiotów (z cała pewnością dla tych zatrudniających więcej niż 250 pracowników oraz tych, którzy przetwarzają tzw. dane wrażliwe).

Na każdym administratorze danych ciąży obowiązek zapewnienia, ze przetwarzane przez niego dane są prawidłowe i aktualne. Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, musza zostać niezwłocznie usunięte lub sprostowane. Taki audyt przygotowawczy może pomóc w aktualizacji wszystkich przetwarzanych danych i uporządkować dokumentacje oraz procedury przetwarzania danych. Może również pomóc administratorowi danych w realizacji zasady rozliczalności, która wymaga, by każdy, kto przetwarza dane osobowe, był w stanie wykazać, ze robi to w zgodzie z zasadami przyjętymi w rozporządzeniu. Te zgodność można wykazać na przykład poprzez wdrożenie efektywnych polityk i procedur przetwarzania danych.

4. Nowe obowiązki informacyjne.

Informowanie osób, których dane dotyczą, o wykorzystywaniu ich danych osobowych (prowadzeniu operacji przetwarzania) i celach, dla których jest ono prowadzone, jest niezbędne dla zapewnienia rzetelności i przejrzystości przetwarzania danych osobowych.

Już obecnie obowiązujące przepisy zobowiązują podmioty pozyskujące dane osobowe do przekazywania osobom, których te dane dotyczą, takich informacji, jak: adres i siedziba administratora danych, cel zbierania danych czy źródło tych danych.

Ogólne rozporządzenie o ochronie danych podkreśla jeszcze bardziej konieczność realizacji obowiązku informacyjnego. Od wszystkich administratorów danych wymagać sie będzie, by wszelkie informacje kierowane do osób, których dane dotyczą, były formułowane jasnym i prostym jezykiem, by były zwięzłe i zrozumiałe. Szczególnie istotne będzie to zaś wówczas, gdy informacje i komunikaty będą kierowane do dzieci, które muszą móc je bez trudu zrozumieć.

Ważna zmiana, jaką wprowadzi rozporządzenie, jest zwiększenie zakresu informacji, które należy przekazać. Od 25 maja 2018 r. administratorzy danych będą musieli poinformować również m.in. o okresie, przez który dane osobowe będą przetwarzane (retencja danych), o ewentualnym fakcie profilowania i jego konsekwencjach czy też o danych kontaktowych inspektora ochrony danych, jeśli został on wyznaczony.

Już teraz zachęcamy więc do zapoznania sie z art. 13 i art. 14 rozporządzenia oraz do przeglądu stosowanych obecnie klauzul informacyjnych i analizy, jakie treści należy zmienić, a jakie uzupełnić – tak by odpowiednio wcześnie zaplanować wszelkie niezbędne zmiany w spełnianiu obowiązku informacyjnego zgodnie z wymogami rozporządzenia. Wobec szerszego katalogu informacji, które należy przekazać, z cała pewnością obecnie stosowane komunikaty będą musiały być zaktualizowane.

Przykładem rozwiązania już stosowanego w praktyce może być poinformowanie klientów o wprowadzeniu nowych klauzul informacyjnych (uwzględniających wymagania ogólnego rozporządzenia) z okresem obowiązywania od 25 maja 2018 r. Niewłaściwe jest jednak przekazywanie niektórych informacji już teraz, jak np. informacji o danych kontaktowych inspektora ochrony danych – obecnie w polskim systemie prawnym mamy jeszcze administratorów bezpieczeństwa informacji (ABI).

5. Uprawnienia osób, których dane dotyczą.

Każda osoba powinna mieć kontrole nad dotyczącymi jej danymi osobowymi, niezależnie od tego kto i w jakim celu te dane przetwarza. Ogólne rozporządzenie o ochronie danych przyznaje wiec szereg uprawnień podmiotom danych:

- prawo do bycia poinformowanym o operacjach przetwarzania,
- prawo dostępu,
- prawo do sprostowania/uzupełnienia danych,
- prawo do usunięcia danych (prawo do bycia zapomnianym),
- prawo do ograniczenia przetwarzania,
- prawo do przenoszenia danych,
- prawo do sprzeciwu,
- prawo do tego, by nie podlegać profilowaniu.

Z większości z wymienionych wyżej uprawnień możemy korzystać już teraz, bowiem przewiduje je ustawa o ochronie danych osobowych. Jeśli wdrożone przez Ciebie procedury przetwarzania danych już uwzględniają możliwość realizacji tych praw przez osoby, których dane przetwarzasz, dostosowanie się do ogólnego rozporządzenia powinno być stosunkowo łatwe. To jest jednak dobry moment by sprawdzić skuteczność zastosowanych procedur i wypracować sposób reakcji, np. w sytuacji, w której ktoś poprosi o usuniecie swoich danych osobowych. Należy w tym wypadku ustalić kto będzie podejmować decyzje o usunięciu danych i czy używany przez Ciebie system pomoże zlokalizować i usunąć te dane.

Zupełnie nowym prawem osób, których dane dotyczą jest natomiast prawo do przenoszenia danych, które ma zastosowanie, jeśli dane przetwarzane w sposób zautomatyzowany na podstawie zgody lub na podstawie umowy. Jest to prawo ścisłe związane z prawem dostępu, ale różni sie od niego pod wieloma względami.

Zapewnia ono osobom, których dane dotyczą, możliwość otrzymywania w ustrukturyzowanym, powszechnie używanym formacie nadającym sie do odczytu maszynowego danych osobowych, które dostarczyły administratorowi, oraz możliwość przesyłania tych danych

osobowych innemu administratorowi. Co więcej, prawo do przenoszenia danych pozwala również na bezpośrednie przekazywanie danych osobowych od jednego administratora do innego.

Warto wiec już teraz dokonać przeglądu procedur i systemów używanych do przetwarzania danych, tak by umożliwić praktyczna i bezpłatna realizacje przeniesienia danych w oczekiwanym formacie. Więcej informacji na temat prawa do przenoszenia danych znajdziesz w Wytycznych WP 242 przygotowanych przez Grupie Roboczej. Dokument dostępny jest w jeżyku polskim i angielskim na stronie internetowej GIODO w zakładce „Reforma przepisów

6. Zgoda na przetwarzanie danych.

Zgoda jest często mylnie traktowana jako podstawowa, najważniejsza przesłanka przetwarzania danych osobowych. Tymczasem jest jedna z kilku równoważnych podstaw prawnych – tak jak obowiązek wynikający z przepisu prawa, realizacja umowy czy też uzasadniony interes administratora danych. Pamiętaj by właściwie wskazać podstawę prawną przetwarzania danych i ich nie dublować. Złą praktyką jest chociażby pozyskiwanie zgody jako warunku zawarcia umowy o świadczenie usług.

Obowiązek uzyskania zgody na przetwarzanie danych osobowych zwiększa kontrole osób, których dane dotyczą, może jednak również budować zaufanie klienta
wobec administratora i zwiększać jego zaangażowanie. Ważne by każda osoba, która takiej zgody udziela mogła robić to dobrowolnie, świadomie i wobec konkretnie oznaczonego celu lub tych samych celów. Zgoda musi zatem zostać przedstawiona w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Każda osoba musi mieć pewność komu i na co wyraża zgodę – okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody.

Dobrowolność wyrażenia zgody zakłada możliwość swobodnego wyboru. Z tego powodu podmioty publiczne czy tez pracodawcy powinni szukać innych podstaw prawnych przetwarzania danych – z uwagi na oczywistą nierówność stron przekreślająca możliwość podjęcia dobrowolnej, nie przymuszonej zgody. Zasadniczym pytaniem, jakie pojawia sie wobec wejścia w życie ogólnego rozporządzenia jest to czy dotychczas pozyskane zgody na przetwarzanie danych będą nadal ważne po 25 maja 2018 r. Zasadniczo nie zmieniły sie warunki pozwalające uznać dane oświadczenie za prawnie wiążąca zgodę (jak wspomniany wymóg dobrowolności). Co więcej zmianie ulegnie charakter prawny zgody w porównaniu z obecnym stanem prawnym. Zwykła zgodę wyraźna w rozumieniu ustawy o ochronie danych osobowych zastąpi zgoda jednoznaczna – wyraźne oświadczenie woli zastąpi wiec jednoznaczne, nie pozostawiające wątpliwości przyzwolenie osoby w formie oświadczenia lub działania potwierdzającego. Nie będzie tez potrzeby udzielania zgody na piśmie w sytuacji gdy przetwarzamy dane wrażliwe, od maja 2018 r. w tych sytuacjach wystarczy już zgoda wyraźna.

Wobec tego „poluzowania” charakteru prawnego zgód, wydaje sie, ze większość otrzymanych dotychczas zgód zachowa ważność także pod rządami ogólnego rozporządzenia. Pod warunkiem, ze poinformowano osobę, której dane dotyczą o możliwości wycofania zgody w dowolnym momencie, a wycofanie zgody jest równie łatwe jak jej wyrażenie. Zachęcamy więc do przeglądu stosowanych klauzul i mechanizmów pozyskiwania zgody i upewnienia sie, że spełniają standardy określone w ogólnym rozporządzeniu i nie ma potrzeby zbierania zgód raz jeszcze.

Co więcej, pamiętając o zasadzie rozliczalności, warto dokumentować wszelkie czynności związane z pozyskiwaniem zgód – np. kiedy, w jakich okolicznościach i komu udzielona została zgoda oraz w jaki sposób spełniono obowiązek informacyjny. W przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem będzie przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Obecnie trwają w Ministerstwie Cyfryzacji prace nad obniżeniem tego wieku, co będzie oznaczało możliwość przetwarzania danych dzieci powyżej 13 roku życia bez konieczności pozyskiwania zgód ich rodziców czy opiekunów prawnych.

7. Zabezpieczenia.

Jednym z podstawowych celów ogólnego rozporządzenia o ochronie danych było dostosowanie zasad ochrony danych do wyzwań XXI wieku, takich jak internet rzeczy, czytniki RFID czy przetwarzanie danych w chmurze obliczeniowej. Prawo nigdy nie nadąży za rozwojem technologicznym, stad tez wiele przepisów rozporządzenia jest bardzo ogólnych i przede wszystkim technologicznie neutralnych (bez odniesień do konkretnych rozwiązań) – po to aby rozporządzenie zachowało aktualność także za 5 czy 10 lat. Efektem takiego myślenia jest przyjęta w rozporządzeniu koncepcja uwzględniania w każdym procesie przetwarzania danych ryzyka dla praw i wolnosci, jakie może nieść to przetwarzanie i każdorazowe dostosowywanie wykorzystywanych narzędzi zabezpieczających dane to tego ryzyka.

Każdy administrator danych zobowiązany jest do tego, by dane osobowe przetwarzał z poszanowaniem podstawowych zasad. W kontekście nadchodzących zmian szczególna uwagę warto zwrócić na zasadę integralności
i poufności. **Rozporządzenie definiuje je tak: „Dane osobowe musza być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych". Każdy, kto przetwarza dane osobowe, musi więc odpowiednio je zabezpieczyć, tak by uniemożliwić ich nieuprawnione udostępnienie.**

W ogólnym rozporządzeniu nie znajdziemy jednak szczegółowych wskazówek, jakie środki organizacyjne i techniczne wdrożyć. Rozporządzenie zachęca jedynie do skorzystania z narzędzi pseudonimizacji czy też szyfrowania danych. W przepisach nie znajdziemy również minimalnych standardów technicznych bezpieczeństwa danych, a w maju przyszłego roku przestanie w dodatku obowiązywać rozporządzenie techniczne MSWiA do ustawy o ochronie danych osobowych (gdzie mamy chociażby wskazówki dotyczące częstotliwości zmiany hasła). Zgodnie z zasadą rozliczalności, to administrator danych – uwzględniając aktualny stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania danych – samodzielnie będzie decydował, jakie środki bezpieczeństwa wdrożyć, by zapewnić zgodność przetwarzania danych z wymogami rozporządzenia. Może wiec uznać, ze od maja 2018 r. nadal aktualne pozostaną środki techniczne i organizacyjne wdrożone i udokumentowane w dotychczasowej polityce

bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, albo tez podjąć decyzje o wdrożeniu zupełnie nowych środków.

Ważne, by oceniając stopień bezpieczeństwa przetwarzanych danych osobowych, uwzględnić przede wszystkim ryzyko wiążące sie z przetwarzaniem – wynikające np. z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Ryzyko to może prowadzić do kradzieży tożsamości, straty majątkowej czy tez naruszenia dóbr osobistych osoby, których te dane dotyczą. W sytuacji, kiedy doszłoby to takiego naruszenia ochrony danych, każdy administrator będzie zobowiązany do zgłoszenia tego faktu do GIODO, a w szczególnych przypadkach także do osób, których dane zostały naruszone.

W tym aspekcie pomocne może być stosowanie zatwierdzonych przez GIODO po 25 maja 2018 r. kodeksów postępowania. W tych właśnie dokumentach możliwe będzie doprecyzowanie przepisów ogólnego rozporządzenia, także tych dotyczących bezpieczeństwa danych. Grupa administratorów danych – np. zrzeszonych w izbie czy związku branżowym – może w opracowanym kodeksie zaproponować modelowe rozwiązania techniczne mające na celu zapewnienie poufności i integralności danych, a które będą ponadto bardzo pomocne dla wszystkich administratorów, którzy zobowiążą sie do stosowania kodeksu.

Innym rozwiązaniem, dzięki któremu będzie można wykazać wywiązywanie się z obowiązku zabezpieczania danych, będzie stosowanie mechanizmu certyfikacji, czyli uzyskiwanie stosownych certyfikatów i znaków jakości potwierdzających właściwe zabezpieczenie danych osobowych.

Źródłem praktycznej i sprawdzonej wiedzy w zakresie budowy i zarządzania środkami bezpieczeństwa mogą być tez, krajowe, europejskie lub międzynarodowe normy, w tym normy ISO.

8. Dokumentacja przetwarzania danych.

Ogólne rozporządzenie o ochronie danych kładzie bardzo duży nacisk na dokumentowanie czynności przetwarzania danych. Jest to jeden z podstawowych sposobów wykazywania przez administratorów danych zgodności prowadzonych działań na danych osobowych z wymogami rozporządzenia. Warto więc pamiętać, żeby od 25 maja 2018 r. dokumentować czynności związane z przetwarzaniem danych osobowych, w tym w szczególności:

- jakie dane posiadasz i w jakich okolicznościach je pozyskałeś – wskaż podstawę prawna przetwarzania i w jaki sposób spełniłeś swoje obowiązki informacyjne,
- komu i kiedy udostępniasz dane, - jak raportujesz incydenty związane z naruszeniem ochrony danych,
- czy przeprowadziłeś analizę w zakresie obowiązku bądź braku obowiązku wyznaczenia inspektora ochrony danych i jakie wnioski z niej płyną, - który organ nadzorczy będzie wiodącym dla transgranicznych operacji przetwarzania, które prowadzisz.

Rozporządzenie zresztą wprost nakłada obowiązek prowadzenia wewnętrznego rejestru czynności przetwarzania danych osobowych, za które odpowiada administrator danych. Pamiętaj, że w praktyce często to inspektor ochrony danych będzie tworzył i prowadził powyższe rejestry na podstawie danych otrzymanych od pozostałych komórek organizacji.

Pojęcie „czynności przetwarzania” nie zostało doprecyzowane w przepisach rozporządzenia. Elementy tych rejestrów są jednak bardzo podobne do elementów zgłoszenia zbioru do rejestracji oraz lokalnego zbioru danych osobowych prowadzonego obecnie przez ABI na podstawie ustawy o ochronie danych osobowych. Stąd też, ze przez rejestrowanie czynności przetwarzania danych można rozumieć klasyfikowanie przetwarzanych danych ze względu m.in. na: zakres przetwarzanych danych, cele przetwarzania, kategorie osób, których dane dotyczą oraz - jeżeli jest to możliwe - środki bezpieczeństwa.

Ze względu na swoja zawartość rejestry mogą być rzeczywiście pomocnym narzędziem w stosowaniu zasady rozliczalności, zapewnianiu przestrzegania rozporządzenia oraz prowadzeniu prawidłowej polityki w zakresie ochrony danych. Dlatego rejestr powinien być prowadzony w formie pisemnej, najlepiej elektronicznej. Możliwe będzie prowadzenie również innych (np.

bardziej szczegółowych) ewidencji przetwarzanych danych, jeśli wynika to z analizy ryzyka oraz konkretnych potrzeb administratora danych.

Prowadzenie tych rejestrów nie zawsze będzie jednak obowiązkowe. W określonych w rozporządzeniu sytuacjach z tego obowiązku zwolnieni będą administratorzy, którzy zatrudniają mniej niż 250 pracowników. Więcej informacji na temat rejestrów czynności przetwarzania danych znajdziesz na zakładce ABI-Informator dostępnej na stronie internetowej GIODO.

9. Privacy by design i Privacy by default.

Zawsze, gdy decydujesz sie przetwarzać dane osobowe, dobra praktyka powinno być podejście oparte na poszanowaniu prywatności osób, których te dane dotyczą. Zakłada ono, że ochrona prywatności powinna być brana pod uwagę i stosowana w praktyce przy prowadzeniu wszelkich projektów i działań, tak w sferze publicznej, jak i prywatnej. Tak rozumiana koncepcja privacy by design jako cześć każdego podejmowanego projektu, niezależnie od jego charakteru i celu– została sformułowana wiele lat temu przez Ann Cavoukian – b. rzeczniczka ds. informacji i prywatności kanadyjskiej prowincji Ontario – jako wynik wieloletnich prac nad wprzęgnięciem zasad ochrony prywatności do nowych projektów infrastrukturalnych realizowanych w Kanadzie. Ogólne rozporządzenia o ochronie danych czyni te koncepcje prawnie wiążącym obowiązkiem, wprowadzając do porządku prawnego uwzględnianie ochrony danych w fazie projektowania oraz – jako pewnego rodzaju jeden z szerszych postulatów privacy by design – zasadę domyślnej ochrony danych.

Uwzględnianie ochrony danych w fazie projektowania ma z zasady umożliwić włączanie ochrony prywatności w samo tworzenie projektu, działanie jego składników oraz w zarządzanie technologiami informacyjnymi i systemami przez cały cykl życia informacji.

To proaktywne podejście wyrażone przez zasadę privacy by design zakłada, że ochrona prywatności powinna być wbudowana w każdy nowy projekt – co oznacza, ze prywatność będzie chroniona nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz jest wbudowana w jego konstrukcje tak, że jest po prostu składową projektu.

W przypadku systemów teleinformatycznych oznacza to wbudowanie ochrony prywatności zarówno w architekturę systemu, jak i w procesy biznesowe, które system obsługuje – np. poprzez jak najszybsza pseudonimizację danych czy tez umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych. Uwzględnianie ochrony danych w fazie projektowania może być dużym wyzwaniem w sektorze publicznym. Wskazane byłoby wbudowanie ochrony prywatności w konstrukcje instrukcji kancelaryjnych. Co więcej, rozporządzenie wprost wskazuje również, ze „zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy tez brać pod uwagę w przetargach publicznych”. Innym wyzwaniem będzie tez realizacja tej zasady w procesie legislacyjnym. Dobrym rozwiązaniem wydaje być wbudowanie privacy by design poprzez włączenie oceny skutków projektowanego aktu prawnego dla ochrony

danych do przygotowywanej w procesie legislacyjnym oceny skutków regulacji (OSR).

Zasadę domyślnej ochrony danych należy natomiast rozumieć jako postulat uwzględnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu. Domyślnie, czyli bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą – i to w kluczowym dla użytkownika momencie przyłączenia sie do danego systemu.

Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane (minimalizacja danych).Warto więc już teraz dokonać przeglądu używanych systemów i narzędzi przetwarzania danych pod kątem realizacji ww. zasad, by mieć pewność, ze 25 maja 2018 r. będziesz w stanie wykazać zgodność wszystkich działań na danych osobowych z wymogami ogólnego rozporządzenia.

10. Ocena skutków dla ochrony danych.

Nowa, przyjęta w ogólnym rozporządzeniu o ochronie danych, filozofia ochrony danych osobowych zakłada odejście od konieczności zgłaszania i rejestracji zbiorów. Zastępuje ją natomiast obowiązkiem przeprowadzenia oceny skutków dla ochrony danych. Ocena ta powinna obejmować przede wszystkim planowane operacje i cele przetwarzania, zabezpieczenia i mechanizmy mające minimalizować ryzyko. Ten istotny dla rozliczalności proces ma prowadzić do opisania przetwarzania danych, oceny jego niezbędności i proporcjonalności, a także pomóc we właściwym zarzadzaniu (przeciwdziałaniu) ryzykami wynikającymi z przetwarzania danych.

Przeprowadzenie takiej oceny będzie wymagane, jeśli operacje przetwarzania danych mogą powodować wysokie ryzyko naruszenia prywatności osób, których dane dotyczą, np. w sytuacji:

- kiedy działania na danych dokonywane są przy użyciu nowych technologii, - użycia zautomatyzowanych procesów przetwarzania danych, w tym profilowania,
- przetwarzania na duża skale szczególnych kategorii danych (danych wrażliwych, takich jak dane biometryczne czy dane na temat stanu zdrowia).

W przypadku gdy administrator danych nie może w wystarczającym stopniu zniwelować zidentyfikowanego ryzyka (znaleźć wystarczających środków) lub mimo zastosowania środków, ryzyko nadal jest wysokie, konieczna będzie konsultacja z GIODO. Jest więc oczywiste, że tego typu oceną musi pojawić sie na etapie projektowania – jej wynik prowadzi bowiem do decyzji, czy przetwarzanie danych w zakładany sposób wymagać będzie uprzedniej konsultacji z GIODO. Pamiętać jednak należy, ze ocena skutków jest procesem ciągłym, wymagającym aktualizacji.

Co ciekawe, rozporządzenie przewiduje, że w określonych przypadkach konieczne może być konsultowanie zamiaru przetwarzania danych osobowych z osobami, których dane dotyczą lub ich przedstawicielami – np. poprzez formalne pytanie do przedstawicieli pracowników czy tez badanie przesłane klientom.

A co z już prowadzonymi operacjami przetwarzania danych? Ocena skutków dla ochrony danych niezbędna będzie dopiero dla operacji rozpoczętych po 25 maja 2018 r. lub dotychczasowych operacji znacząco zmienionych po tej dacie - na przykład ponieważ została wprowadzona do użytku nowa technologia lub ponieważ dane osobowe są wykorzystywane w

innym celu. GIODO zdecydowanie zaleca jednak dokonanie oceny skutków dla wszystkich trwających już operacji przetwarzania danych spełniających kryteria wskazane w art. 35 rozporządzenia. Warto wiec już teraz zacząć analizować okoliczności, w których prowadzone przez Ciebie operacje będą wymagały dokonania takiej oceny. Zastanów sie, kto w twojej organizacji jej dokona oraz kto powinien być w ten proces zaangażowany (zasięganie opinii niezależnych ekspertów).

Rozporządzenie identyfikuje także problem oceny skutków dla ochrony danych dla operacji prowadzonych przez podmioty sektora publicznego, w sytuacji kiedy podstawa przetwarzania danych osobowych jest przepis prawa lub interes publiczny. W tej sytuacji ocena skutków powinna zostać przeprowadzona w ramach oceny skutków regulacji (OSR) dla aktu prawnego stanowiącego podstawę dla takiego przetwarzania.

Ocena skutków musi być realną ocena ryzyk, umożliwiającą administratorom podejmowanie działań mających na celu ich rozwiązanie. Ogólne rozporządzenie zapewnia administratorom danych elastyczność w wykorzystaniu różnych narzędzi służących do przeprowadzenia tej oceny. Więcej praktycznych informacji na ten temat znajdziesz w przygotowanych przez GIODO i Grupę Robocza Art. 29 Wytycznych WP 248 dotyczących oceny skutków dla ochrony danych (DPIA) dostępnych na stronie internetowej GIODO w zakładce „Reforma przepisów”.

11. Dane osobowe dzieci.

Ponieważ dzieci mogą być mniej świadome ryzyka i konsekwencji przetwarzania ich danych osobowych, a przede wszystkim praw przysługującym im w związku z tym przetwarzaniem, ogólne rozporządzenie o ochronie danych szczególny nacisk kładzie właśnie na ochronne danych osobowych dzieci.

Ochrona ta dotyczy przede wszystkim sytuacji, kiedy dzieci korzystają z usług społeczeństwa informacyjnego, takich jak portale społecznościowe czy poczta elektroniczna. Jeśli więc twoja firma czy organizacja świadczy usługi drogą elektroniczną oferowane bezpośrednio dzieciom, upewnij sie, że robisz to zgodnie z wymaganiami ogólnego rozporządzenia o ochronie danych.

Przede wszystkim pamiętaj, ze gdy podstawa przetwarzania danych jest zgoda, zgodne z prawem będzie przetwarzanie danych dziecka, które ukończyło 16 lat (ten wiek może być jeszcze obniżony do lat 13 w przepisach prawa krajowego). Będziesz zaś musiał uzyskać zgodę rodzica lub opiekuna prawnego dziecka, które nie osiągnęło jeszcze takiego wieku. Zacznij wiec już teraz analizować, w jaki sposób będziesz weryfikować wiek dziecka i to, czy rodzic lub opiekun prawny wyraził zgodę na takie przetwarzanie lub ja zaaprobował.

Szczególną ochroną dzieci powinna mieć również zastosowanie wówczas, kiedy dane dzieci są wykorzystywane do celów marketingowych i do tworzenia profili osobowych. Za każdym razem zwracaj szczególna uwagę, by wszelkie informacje i skierowane do nich komunikaty były formułowane jasnym i prostym jezykiem, tak by dziecko mogło je bez trudu zrozumieć.

12. Automatyczne przetwarzanie danych oparte na profilowaniu.

Przetwarzanie danych osobowych przy użyciu zautomatyzowanych narzędzi podejmowania decyzji – w tym profilowania, czyli oceny czynników osobowych osoby fizycznej – jest coraz powszechniejszym zjawiskiem. Marketing i branża reklamowa, bankowość, ubezpieczenia, ochrona zdrowia – to tylko niektóre z sektorów, gdzie korzysta sie już z operacji profilowania.

Ma to, oczywiście, związek z dynamicznym rozwojem technologicznym i praktycznie nieograniczonymi możliwościami gromadzenia i analizowania danych. Profilowanie skutecznie pomaga w analizie i wyciąganiu wniosków z zebranych danych. Problem jednak w tym, że osoby, których dane dotyczą, często nie są nawet świadome, ze tego typu operacje są dokonywane na ich danych osobowych – trudno im więc korzystać z przysługujących im praw związanych z przetwarzaniem ich danych i kwestionować dla przykładu trafność takich operacji. A jeśli konkretnej osobie zostaną przypisane nieprawidłowe atrybuty, może to w konsekwencji doprowadzić do sytuacji, w której przetwarzane dane są po prostu niepoprawne.

Dlatego ogólne rozporządzenie o ochronie danych szczególny nacisk kładzie na operacje przetwarzania przy użyciu technik profilowania, w sytuacji kiedy to przetwarzanie:

- jest zautomatyzowane,
- dokonywane jest na danych osobowych,
- ma na celu analizę lub prognozę aspektów dotyczących efektów pracy osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Co do zasady, każda osoba, której dane dotyczą, ma prawo, by nie podlegać decyzji opierających sie na przetwarzaniu zautomatyzowanym – w tym profilowaniu – i wywołującej dla niej określone skutki prawne (np. brak możliwości udzielenia kredytu). Rozporządzenie wyraźnie wskazuje wiec sytuacje, w których profilowanie będzie możliwe, tj.:

- kiedy jest to niezbędne do zawarcia lub wykonania umowy,
- przepis prawa na to zezwala,
- osoba, której dane dotyczą, udzieliła wyraźnej zgody.

W każdym z powyższych przypadków od administratora danych oczekuje się wdrożenia środków technicznych i organizacyjnych mających na celu właściwe i bezpieczne przetwarzanie danych przy użyciu technik profilowania. Szczególnie jeśli do profilowania używa sie szczególnych

kategorii danych osobowych (danych wrażliwych) lub danych osobowych dzieci. Wszystkie zasady przetwarzania danych (jak zasada adekwatności czy ograniczonego celu) również będą miały tu zastosowanie.

Przede wszystkim należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania – w szczególności o zasadach podejmowania decyzji, znaczeniu i konsekwencjach profilowania. Pamiętać należy także o możliwości złożenia – w dowolnym momencie i bezpłatnie – sprzeciwu wobec przetwarzania danych, szczególnie jeśli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego. Innym obowiązkiem będzie również dokonanie oceny skutków regulacji dla operacji przetwarzania wykorzystujących profilowanie.

Jeśli wykorzystujesz zautomatyzowane systemy do podejmowania decyzji. wobec osób, których dane dotyczą (w tym do ich profilowania), zwróć szczególna uwagę na obowiązki, z których wywiązywania będziesz sie musiał wykazać już 25 maja 2018 r. Szczególna uwagę poświeć analizie tego, jak spełnisz obowiązki informacyjne wobec osób, które profilujesz.

13. Naruszenia ochrony danych.

Zgłaszanie naruszeń ochrony danych będzie dla większości administratorów danych zupełnie nowym obowiązkiem. Od 2013 r. takie incydenty zgłaszają do Generalnego Inspektora Ochrony Danych Osobowych (GIODO) operatorzy telekomunikacyjni, którzy zdążyli już w tym czasie wypracować procedury wykrywania, analizy i zgłaszania naruszeń ochrony danych.

Począwszy od 25 maja 2018 r. obowiązek ten będzie jednak spoczywał na podmiotach ze wszystkich branż – upewnij sie więc, ze będziesz gotowy na wdrożenie tych procedur na czas. Szczególnie większe organizacje powinny wdrożyć odpowiednie polityki i procedury postępowania związane z przypadkami naruszenia ochrony danych. Naruszenie ochrony danych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych
osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Pamiętaj jednak, że nie każde naruszenie będzie wymagało poinformowania GIODO. Zgłosić taki incydent będziesz musiał jedynie wtedy, gdy może on skutkować ryzykiem naruszenia praw i wolnosci osób, np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy tez naruszenia tajemnic prawnie chronionych. W takim przypadku naruszenie należy zgłosić do GIODO nie później niż 72 godziny po stwierdzeniu (wykryciu) incydentu, gdyż brak odpowiedniej i szybkiej reakcji może mieć bardzo negatywne konsekwencje dla osób, których dane dotyczą.

Możliwość pojawienia sie takich ryzyk dla osób, których dane dotyczą, oznaczać również będzie konieczność ich zawiadomienia o naruszeniu. Jasnym i prostym jezykiem będziesz musiał opisać jego charakter, możliwe konsekwencje oraz możliwe do zastosowania środki zalecane w celu poradzenia sobie z incydentem i zminimalizowania jego negatywnych skutków. Warto potraktować ten obowiązek jako ważny element budowania przejrzystych relacji z klientami i zapewnienia osobom możliwości kontroli i pełnej wiedzy na temat ich danych osobowych.

Pamiętaj, ze niezgłoszenie naruszenia może skutkować nałożeniem przez GIODO dotkliwej kary pieniężnej. Oczywiście możliwe będzie także nałożenie tej kary już za samo naruszenie. Zatem, aby nie narazić sie ani na utratę dobrego imienia i zaufania klientów, ani na wysokie kary

finansowe, warto abyś z należyta troską podchodził do zagrożeń w sferze bezpieczeństwa danych, a na ochronę i bezpieczeństwo informacji przeznaczał odpowiednie środki.

14. Inspektor ochrony danych .

Ogólne rozporządzenie nakłada na administratorów danych wiele nowych obowiązków – na czele z zupełnie nowym podejściem do ochrony danych osobowych wyrażonym w zasadzie rozliczalności. Wdrożenie właściwych środków organizacyjnych i technicznych oraz wykazanie ich zgodności z ogólnym rozporządzeniem będzie sporym wyzwaniem. Żeby mu sprostać, warto rozważyć powołanie eksperta, jakim jest inspektor ochrony danych, który będzie cię wspierał w wykonywaniu zadań związanych z przetwarzaniem danych.

W świetle ogólnego rozporządzenia, inspektor ochrony danych ma kluczowe znaczenie w procesie administrowania danymi, w związku z czym dokładnie określono warunki jego wyznaczania, status oraz katalog zadań. Pamiętaj przede wszystkim, że ogólne rozporządzenie – inaczej niż jest obecnie – przewiduje sytuacje, kiedy wyznaczenie inspektora ochrony danych będzie obowiązkowe, np. kiedy administrator danych jest organem lub podmiotem publicznym lub gdy główna działalność administratora polega na przetwarzaniu na dużą skale danych wrażliwych. Sprawdź zatem, czy od 25 maja 2018 r. wręcz nie będziesz zobowiązany do wyznaczenia inspektora ochrony danych. W tej analizie pomocne będą ci wskazówki GIODO i Grupy Roboczej Art. 29 zawarte w Wytycznych WP 243, których polska wersja jest dostępna na naszej stronie internetowej. Niezależnie od tego GIODO zachęca do wyznaczenia inspektora ochrony danych, nawet jeśli nie będziesz miał takiego obowiązku.

Rozbudowany katalog zadań inspektora ochrony danych wymaga, by taka osoba posiadała fachową wiedze na temat prawa i praktyk w dziedzinie ochrony danych osobowych. Pamiętaj, by odpowiedzialnie wybierać osoby, którym powierzysz zadania inspektora ochrony danych, sprawdzając stopień ich przygotowania do pełnienia tej funkcji, posiadaną wiedzę, praktyczne umiejętności oraz doświadczenie. Nie zapomnij również o potrzebie zapewnienia takiemu inspektorowi właściwych gwarancji niezależności.

Wprowadzaj zatem rozwiązania (najlepiej poprzez odpowiednie postanowienia wewnętrznych regulaminów organizacyjnych czy statutów), które pozwolą na osiągniecie tego celu, pamiętając przede wszystkim o:

- odpowiednim usytuowaniu inspektora w strukturze organizacyjnej, tak, by był bezpośrednio podległy najwyższemu kierownictwu,
- zapewnieniu mu niezbędnych zasobów do wykonywania jego zadań,
- włączaniu inspektora we wszystkie procesy, gdzie przetwarzane są dane osobowe,
- nakładaniu na inspektora takich obowiązków, które nie powodują konfliktu interesów (zidentyfikuj stanowiska niekompatybilne z funkcją inspektora, np. członkowie zarządu spółki).

Otwarte pozostaje pytanie, co stanie sie z obecnymi administratorami bezpieczeństwa informacji (ABI). Czy staną sie z mocy prawa inspektorami ochrony danych? , jakie warunki trzeba będzie spełnić, by tak się stało?. Kwestia ta będzie uregulowana w nowej ustawie o ochronie danych, nad którą pracuje Ministerstwo Cyfryzacji. Więcej praktycznych informacji na temat inspektorów ochrony danych (m.in. w zakresie możliwości powołania jednego inspektora ochrony danych dla kilku podmiotów) znajdziesz w przywołanych już Wytycznych WP 243 oraz przygotowanym przez GIODO poradniku „Wykonywanie obowiązków ABI, przyszłego inspektora w świetle ogólnego rozporządzenia o ochronie danych” – oba dokumenty dostępne są na stronie internetowej GIODO w zakładce „Reforma przepisów”.

Cennym źródłem informacji będzie również serwis „ABI-Informator”, w którym utworzyliśmy specjalną zakładkę poświęcona inspektorowi ochrony danych. Znajdziesz tam wiele wyjaśnień dotyczących wyznaczania inspektora, wykonywania jego zadań i gwarancji jego niezależności.

15. Transgraniczne przetwarzanie danych.

Pozbawiony barier Internet, postępująca globalizacja, szybki rozwój nowoczesnych technologii - to te zjawiska powodują, że dane osobowe bardzo często przetwarzane są w kontekście transgranicznym, przez co aktywność coraz większej liczby przedsiębiorców wykracza poza granice jednego państwa. Jednym z założeń unijnej reformy ochrony danych osobowych było wprowadzenie ułatwień dla tych podmiotów - przede wszystkim jednolitych przepisów oraz mechanizmu określanego mianem „punktu kompleksowej współpracy".

Istotą tego mechanizmu jest ustanowienie jednego, konkretnego organu ochrony danych, który w pierwszym rzędzie odpowiada za nadzór nad przetwarzaniem danych przez danego administratora danych. Organu, który będzie także koordynował wszystkie postępowania, w które są zaangażowane organy nadzorcze innych krajów (tzw. organy, których sprawa dotyczy), zwłaszcza wówczas, kiedy jeden z organów rozpatruje skargę na administratora z innego kraju członkowskiego.

Wskazanie wiodącego organu nadzorczego będzie konieczne, jeśli przetwarzanie odbywa się w ramach działalności jednostek organizacyjnych danego przedsiębiorstwa w więcej niż jednym kraju (np. w przypadku operacji dokonywanych w międzynarodowych oddziałach danej spółki) lub też dany rodzaj przetwarzania znacznie wpływa na obywateli w więcej niż jednym kraju członkowskim (np. kiedy administrator z innego państwa nie ma w Polsce oddziału lub spółki zależnej, ale oferuje tu swoje usługi).

Organem wiodącym będzie organ nadzorczy głównej jednostki organizacyjnej danego administratora. W celu stwierdzenia, gdzie znajduje się główna jednostka organizacyjna, najpierw konieczne jest ustalenie, gdzie znajduje się centralna administracja administratora danych w UE, o ile taka istnieje. Według podejścia przyjętego w rozporządzeniu, centralna administracja w UE to miejsce, w którym zapadają decyzje co do celów i sposobów przetwarzania danych osobowych.

Pamiętaj więc, aby dokładnie określić, gdzie podejmowane są decyzje co do celów i sposobów przetwarzania. Właściwa identyfikacja głównej jednostki organizacyjnej leży w interesie administratorów i podmiotów przetwarzających, ponieważ zapewnia jasność co do tego, z którym organem nadzorczym będą musieli mieć do czynienia, jeżeli chodzi o różne obowiązki wynikające

z ogólnego rozporządzenia, takie jak informowanie o danych kontaktowych inspektora ochrony danych, konsultacje z organem w ramach oceny skutków dla ochrony danych lub zgłoszenie naruszenia danych.

Administrator danych sam określa, gdzie znajduje się jego główna jednostka organizacyjna i w związku z tym, który organ nadzorczy jest jego organem wiodącym. Co jednak kiedy nie ma centralnej administracji w Unii? Wtedy w ustalaniu lokalizacji głównej jednostki organizacyjnej administratora pomocne będą poniższe czynniki:

- gdzie są ostatecznie zatwierdzane decyzje co do celów i sposobów przetwarzania?
- gdzie są podejmowane decyzje dotyczące działań biznesowych obejmujących przetwarzanie danych?
- kto ma uprawnienie do podejmowania decyzji w tym zakresie?
- gdzie znajduje się dyrektor, do którego należy całkowita odpowiedzialność zarządcza za przetwarzanie transgraniczne?
- gdzie jest zarejestrowany administrator lub podmiot przetwarzający jako przedsiębiorstwo?

Więcej przydatnych informacji na ten temat znajdziesz w Wytycznych WP 244 Grupy Roboczej Art. 29, które dostępne są na stronie internetowej GIODO w zakładce „Reforma przepisów”.

16. Powierzenie danych.

Administratorzy danych coraz częściej decydują się na powierzanie przetwarzania danych osobowych innym podmiotom, które w ich imieniu wykonują część operacji na danych. Trudno w tym kontekście nie dostrzec np. coraz popularniejszych rozwiązań chmurowych. Administrator – chcąc wykorzystać możliwości obliczeniowe chmury – decyduje się na przetwarzanie danych przy użyciu tego właśnie instrumentu, powierzając tym samym proces przetwarzania danych usługodawcy świadczącemu tego rodzaju usługę.

W takich sytuacjach ważne jest, by podpisując umowę powierzenia, nie stracić kontroli nad danymi osobowymi, czyli nie dopuścić do sytuacji, w której powierzone dane będą wykorzystywane w innym celu niż ten określony przez samego administratora. Pamiętaj więc, aby powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać wyłącznie z usług podmiotów przetwarzających posiadających odpowiednią wiedzę fachową, wiarygodność i zasoby. W szczególności jeżeli chodzi o gwarancje wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom ogólnego rozporządzenia o ochronie danych osobowych, w tym wymogom bezpieczeństwa przetwarzania.

Mogą to być na przykład podmioty, które posiadać będą odpowiednie certyfikaty wydane na podstawie rozporządzenia. Powierzenie danych powinno być regulowane umową lub innym instrumentem prawnym, określającym przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą. Ta umowa lub inny instrument prawny powinny również uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą.

W stosunku do obecnych regulacji niezwykle ważną zmianą jest to, że na podmiocie przetwarzającym spoczywają bardzo podobne obowiązki jak na administratorze danych. Przede wszystkim musi on również wdrożyć środki techniczne i organizacyjne odpowiednie do ryzyk przetwarzania – tak by to przetwarzanie odpowiadało wymogom rozporządzenia. Wśród innych obowiązków podmiotu przetwarzającego można wskazać:

- prowadzenie rejestru czynności przetwarzania,

- zgłaszanie naruszeń ochrony danych do organu nadzorczego, czyli GIODO,
- wyznaczenie inspektora ochrony danych.

Zachęcamy więc do przeglądu zawartych przez ciebie umów powierzenia i upewnienia się, że podmiot, któremu powierzyłeś dane, będzie spełniał wszystkie określone w rozporządzeniu wymagania, zaś sama umowa zawiera wszelkie niezbędne elementy.

17. Podnoszenie wiedzy na temat ogólnego rozporządzenia.

Wobec skali zmian, jakie przynosi ogólne rozporządzenie o ochronie danych, przygotowanie sie do jego stosowania jest dużym wyzwaniem. Zarówno dla dużych przedsiębiorstw, w których w ten proces będzie musiało być zaangażowanych wiele osób, jak i dla małych i średnich firm – tu pracować należy przede wszystkim nad niezbędną wiedza dotycząca nowych instrumentów prawnych w zakresie przetwarzania danych osobowych.

Upewnij się więc, że osoby zarządzające i podejmujące kluczowe decyzje w twojej organizacji są świadome zmian, jakie nastąpią od 25 maja 2018 r. Muszą one zrozumieć skalę wyzwań, jakie niesie wykazanie zgodności z ogólnym rozporządzeniem i zidentyfikować obszary, które koniecznie wymagają zmian.

Jeśli w twojej organizacji został powołany administrator bezpieczeństwa informacji (ABI), powinien on już teraz podnosić wiedzę wszystkich osób uczestniczących w procesach przetwarzania danych, przygotowując ich tym samym do stosowania nowego prawa. Dodatkowo udział w zewnętrznych szkoleniach czy pomoc profesjonalnych firm w zakresie wdrożenia rozporządzenia może być pomocnym rozwiązaniem.

Najważniejsze, byś nie zostawiał przygotowania Twojej organizacji do stosowania rozporządzenia na ostatnia chwile. Wykorzystaj czas, który pozostał do momentu stosowania rozporządzenia na rzetelny przegląd wszystkich prowadzonych czynności przetwarzania danych, tak by 25 maja 2018 r. móc już wykazać zgodność z nowymi przepisami. Pomocne w tym zakresie będą wytyczne przygotowywane przez GIODO i Grupę Robocza Art. 29, które znajdziesz na naszej stronie w zakładce „Reforma przepisów”.