25.3.2025

Esencja z webinaru

Czy prawidłowo zidentyfikowałeś operacje przetwarzania danych? Lekcje z decyzji UODO dotyczącej Toyota Banku.

Dziękuję za udział w webinarze

Jeśli uważasz, że przekazałem wiedzę w sposób rzetelny
to dodaj proszę swoją opinię na wizytówce ODO 24 w Google.

Z góry dziękuję 😊

Jeśli potrzebujesz dodatkowego wsparcia merytorycznego – zachęcam do skorzystania z bezpłatnych porad prawnych i IT.

Justyna Pergałowska
Specjalista ds. ochrony danych

Linki do źródeł wiedzy, inspiracji i nie tylko

Linki
Nagranie webinaru • Czy prawidłowo zidentyfikowałeś operacje przetwarzania danych? Lekcje z decyzji UODO dotyczącej Toyota Banku.
Polecamy: • Rejestr czynności przetwarzania i RODO – wszystko, co musisz wiedzieć • Jak przeprowadzić analizę ryzyka zgodnie z RODO • Jak stworzyć użyteczną dokumentację • Ochrona danych osobowych w szkołach i placówkach oświatowych – poradnik UODO • RODO znosi obowiązek rejestracji zbiorów danych osobowych
W czym możemy pomóc? • Outsourcing IOD • Analiza ryzyka i DPIA - zgodnie z RODO • Bezpłatne porady prawne i informatyczne z zakresu ochrony danych.
Bezpłatne konsultacje • Porozmawiaj z naszymi doradcami:  Marcin Kuźniak umów spotkanie  Cezary Lutyński umów spotkanie

Pytania i odpowiedzi

Szanowni Państwo,
dziękuję za udział w webinarium i przesyłam odpowiedzi na zadane za pomocą czatu pytania. Jednocześnie uczulam, że odpowiedzi tych nie należy traktować jako „prawdy objawionej", gdyż – z uwagi na formę zadawania pytań – są to raczej wskazówki, sformułowane w oparciu o skromne informacje na temat stanu faktycznego.

Czy do rejestru powinno się dołączyć Standardy Ochrony Małoletnich?

Moim zdaniem kwestie związane z przetwarzaniem danych wynikających ze Standardów Ochrony Małoletnich powinny być uwzględnione zarówno w procesie rekrutacji i/lub zatrudnienia, jak i włączone do każdego procesu obejmującego współpracę z dziećmi, np. prowadzenia zajęć dodatkowych. Szczególną uwagę należy zwrócić na kwestie związane z podejmowaniem interwencji, identyfikacją małoletnich oraz budowaniem relacji z nimi, np. w kontekście realizacji usług hotelowych.

Mam może nieco nietypowe pytanie, ale czy w swojej dokumentacji ochrony danych nadal posiadacie wykaz zbiorów danych? Czy w sytuacji, gdy prowadzimy rejestr czynności przetwarzania danych, ten wykaz zbiorów staje się pewnego rodzaju powtórzeniem i jest już zbędny

Nie prowadzimy wykazu zbiorów danych, ponieważ zostały one zastąpione przez procesy przetwarzania danych ujęte w Rejestrze Czynności Przetwarzania. Aktualnie zbiory danych nie są już prowadzone. Warto również zauważyć, że Urząd (działający wówczas jako GIODO) na swojej archiwalnej stronie internetowej wskazał, iż „z dniem 25 maja 2018 r. wygasa obowiązek zgłaszania do rejestracji zbiorów danych osobowych, a także zgłaszania zmian w zbiorach oraz wniosków o ich wykreślenie z rejestru". Można zatem uznać, że prowadzenie wykazu zbiorów danych nie jest już wymagane.

Czy dla każdej operacji robimy analizę ryzyka i jak często ja robić?

Analiza ryzyka, o której mowa w art. 32 RODO, powinna być przeprowadzona przed rozpoczęciem przetwarzania danych lub wdrożeniem nowego zasobu uczestniczącego w operacjach przetwarzania. Jest to kluczowy element zasady ochrony danych w fazie projektowania (data protection by design).

Nasza metodologia opiera się na identyfikacji zasobów, a następnie przypisaniu do nich potencjalnych zagrożeń, zabezpieczeń technicznych i organizacyjnych oraz podatności. W przypadku wprowadzenia zmian w infrastrukturze lub wdrożenia nowego systemu biznesowego, konieczne jest dokonanie przeglądu analizy ryzyka i jej aktualizacja w celu uwzględnienia nowych elementów.

Aby analiza ryzyka odzwierciedlała aktualne zagrożenia i zmieniające się warunki przetwarzania danych, powinna być systematycznie aktualizowana. Zaleca się jej przegląd co najmniej raz w roku lub w innych cyklach zgodnych z polityką organizacji. Dodatkowo każdorazowo po wystąpieniu naruszenia ochrony danych osobowych należy przeprowadzić ponowną ocenę, aby zweryfikować skuteczność zastosowanych środków zabezpieczających.

Jakie dokumenty będą wystarczające, aby realizować podstawowe obowiązki wynikające z ustawy o ochronie danych i RODO, jeśli organizacja nie musi powoływać inspektora i jest zwolniona z prowadzenia rejestru czynności przetwarzania? Obecnie posiadamy upoważnienia do przetwarzania danych (w tym w systemach informatycznych), a dodatkowo, w ramach konkretnych umów z klientami, upoważnione są określone osoby do przetwarzania danych niezbędnych do realizacji danej umowy, wraz z klauzulami poufności i ochrony tajemnicy przedsiębiorstwa.

RODO nie określa szczegółowo, jak prowadzić dokumentację dotyczącą przetwarzania danych osobowych ani jakie powinna ona mieć elementy. Jednak, aby wykazać zgodność z przepisami, organizacja powinna udokumentować swoje działania w czterech kluczowych obszarach:

- Wdrożenie polityk i procedur – obejmuje to m.in. politykę ochrony danych i procedury związane z przetwarzaniem danych osobowych.
- Prowadzenie rejestrów i ewidencji – takich jak Rejestr Czynności Przetwarzania Danych (RCPD), Rejestr Kategorii Czynności Przetwarzania oraz Rejestr Naruszeń.
- Regularne analizy zgodności – w tym ocena skutków dla ochrony danych (DPIA) i analiza ryzyka, które pomagają monitorować i minimalizować zagrożenia związane z przetwarzaniem danych.
- Stosowanie odpowiednich klauzul i postanowień – we wszystkich dokumentach, w których zbierane są dane osobowe, takich jak umowy, formularze, polityki prywatności na stronie internetowej czy zgody na przetwarzanie danych.

Proszę się zastanowić, czy Państwa organizacja na pewno nie ma obowiązku prowadzenia Rejestru Czynności Przetwarzania. Zgodnie z art. 30 ust. 1 RODO każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. Wyjątek stanowi, że obowiązek ten nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że:

- przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- przetwarzanie nie ma charakteru sporadycznego,
- przetwarzanie obejmuje szczególne kategorie danych osobowych lub dane dotyczące wyroków skazujących i czynów zabronionych.

W praktyce niemal każdy podmiot przetwarzający dane ma do czynienia z przetwarzaniem opartym na ryzyku, a jeśli zatrudnia pracowników (niezależnie od ich liczby), będzie przetwarzał dane szczególnych kategorii (np. dane dot. zwolnień lekarskich).

Czy Microsoft należy uwzględnić jako podmiot przetwarzający w rejestrze czynności przetwarzania? Jeżeli tak, proszę o wskazówki dotyczące prawidłowego ujęcia tego podmiotu w rejestrze, biorąc pod uwagę, że dane mogą być przetwarzane poza obszarem EOG. Szczególnie interesują mnie kwestie związane z zastosowanymi zabezpieczeniami oraz ewentualnym dalszym powierzeniem przetwarzania (podpowierzeniem).

Zasadniczo, Microsoft, jako podmiot przetwarzający dane, powinien być uwzględniony w Rejestrze Czynności Przetwarzania, szczególnie że świadczy usługi związane z przetwarzaniem danych, które wiążą się z takim obowiązkiem. Ponadto istotnym jest, aby usługi Microsoft, takie jak M365 i Azure, zostały uwzględnione w analizie ryzyka.

Czy IOD jest przedstawicielem ADO i można na niego scedować prowadzenie RCP? Kogo mamy na myśli mówiąc, że administrator prowadzi ten rejestr? czy tu chodzi o inspektora ochrony danych, czy jakiś inny podmiot?

Prowadzenie Rejestru Czynności Przetwarzania (RCP) jest obowiązkiem administratora danych. Zgodnie z wytycznymi UODO, zadanie to nie powinno być powierzone inspektorowi ochrony danych. Jego rolą jest nadzór nad zgodnością rejestru z przepisami, a samodzielne prowadzenie RCP oznaczałoby konieczność oceniania własnej pracy, co mogłoby prowadzić do konfliktu interesów.

Choć to administrator ponosi ostateczną odpowiedzialność za prawidłowe prowadzenie i treść Rejestru, może on w codziennym utrzymywaniu jego rzetelności i aktualności korzystać ze wsparcia innych osób. Warto w tym celu zaangażować właścicieli poszczególnych procesów, ponieważ:

- dysponują oni najpełniejszą wiedzą na temat przepływu danych osobowych w swoich obszarach,
- mają bezpośredni kontakt z osobami realizującymi te procesy, co ułatwia aktualizację informacji.

Wskazanie odpowiedzialnych za konkretne procesy nie tylko usprawnia prowadzenie Rejestru, ale również zwiększa jego dokładność i zgodność z rzeczywistymi działaniami organizacji.

Jak wykazać, że rejestr został zaakceptowany przez Administratora? Czy prowadzenie rejestru w formie arkusza Excel jest wystarczające dla UODO? Czy powinniśmy posiadać potwierdzenie mailowe lub inny dokument świadczący o tym, że rejestr został zaakceptowany przez Administratora? Czy w takiej sytuacji cały Zarząd powinien podpisać i zaakceptować ten rejestr?

Prezes UODO wskazuje, że Rejestr Czynności Przetwarzania powinien być prowadzony w formie pisemnej, przy czym może to być zarówno forma papierowa, jak i elektroniczna. W praktyce oznacza to, że narzędzia takie jak arkusz Excel są w pełni wystarczające, o ile umożliwiają bieżącą aktualizację oraz czytelne przedstawienie procesów przetwarzania danych.

Zarówno przepisy RODO, jak i interpretacje doktryny nie wymagają formalnego zatwierdzenia RCP przez administratora. Jednak zgodnie z zasadą rozliczalności, osoby zajmujące najwyższe stanowiska w organizacji – zwłaszcza z kadry kierowniczej – powinny być świadome treści rejestru.

Taka wiedza nie tylko ułatwia monitorowanie zgodności z przepisami o ochronie danych osobowych, ale także pozwala na podejmowanie świadomych decyzji dotyczących zarządzania ryzykiem i ochrony danych w organizacji.

Czy Administrator wyznacza dodatkową osobę do prowadzenia dokumentacji?

Jak już wcześniej wskazywałam, administratorem danych osobowych jest zazwyczaj organizacja, np. spółka. W praktyce oznacza to, że sporządzanie i aktualizowanie dokumentacji może zostać powierzone wyznaczonemu pracownikowi, np. właścicielowi konkretnego procesu biznesowego, lub podmiotowi zewnętrznemu, takiemu jak firma ODO24.

Rolą inspektora ochrony danych jest natomiast nadzór i kontrola, aby dokumentacja była zgodna z RODO oraz innymi przepisami dotyczącymi ochrony danych osobowych.

Gdy Administrator jest podmiotem prawnym - firmą/organizacją - kto w takiej strukturze fizycznie prowadzi rejestr i jest odpowiedzialny za nadzorowanie procesów związanych z ochroną danych (upoważnienia, klauzule, zgody itp.)? Czy jest to prezes spółki, czy może osoba specjalnie do tego zadania dedykowana?

Proszę zwrócić uwagę na odpowiedź na pytanie nr 6. Za monitorowanie przestrzegania przepisów o ochronie danych osobowych odpowiada inspektor ochrony danych, o ile został powołany. Jego zadaniem jest nadzorowanie zgodności działań organizacji z RODO, identyfikowanie potencjalnych zagrożeń oraz rekomendowanie działań naprawczych.

Odpowiedzialność za podejmowanie decyzji i realizację konkretnych działań związanych z ochroną danych osobowych – takich jak prowadzenie Rejestru Czynności Przetwarzania, nadawanie upoważnień czy zapewnienie prawidłowych klauzul informacyjnych – spoczywa jednak na administratorze danych. Oznacza to, że odpowiedzialność ponoszą osoby działające w jego imieniu, np. członkowie zarządu lub inne osoby upoważnione do wykonywania tych obowiązków.

W praktyce:

- Inspektor ochrony danych pełni rolę doradczą i kontrolną – monitoruje zgodność z RODO, wskazuje zagrożenia i sugeruje działania naprawcze.
- Osoby zarządzające lub upoważnione do realizacji zadań odpowiadają za wdrożenie i egzekwowanie konkretnych procedur w ramach organizacji.

Taki podział obowiązków umożliwia skuteczne wdrażanie i przestrzeganie przepisów, jednocześnie jasno określając zakresy odpowiedzialności i kompetencji.

W przypadku stwierdzenia uchybień w rejestrze, odpowiedzialność ponosi Administrator Danych Osobowych (ADO), ale czy Inspektor Ochrony Danych (IOD) może zostać zwolniony z powodu niewywiązania się ze swoich obowiązków w tym zakresie?

Jak słusznie zauważono w pytaniu, za prowadzenie Rejestru Czynności Przetwarzania danych odpowiada administrator danych. Inspektor ochrony danych) może monitorować zgodność rejestru z RODO oraz przepisami o ochronie danych, jednak nie jest odpowiedzialny za jego prowadzenie.

W kontekście samego RODO nie ma przepisów, które wskazywałyby na odpowiedzialność inspektora za działania związane z wykonywaniem jego obowiązków – IOD nie ponosi osobistej odpowiedzialności za naruszenia przepisów RODO. Jednakże, jeśli inspektor jest pracownikiem organizacji, może zostać pociągnięty do odpowiedzialności na zasadach ogólnych (odpowiedzialność pracownika za wyrządzoną pracodawcy szkodę). W przypadku innej formy współpracy, inspektor może odpowiadać cywilnie za ewentualną szkodę, którą wyrządził.

Czy w przypadku, gdy firma promuje swoją działalność na Facebooku, można uznać, że przetwarza dane osobowe poza obszarem EOG?

Nie, w przypadku, gdy firma promuje swoją działalność na Facebooku, nie można uznać, że przetwarza dane osobowe poza obszarem EOG. Facebook, jako platforma społecznościowa, jest odrębnym administratorem danych osobowych użytkowników. Oznacza to, że to Facebook ponosi odpowiedzialność za przetwarzanie danych osób korzystających z tej platformy, niezależnie od ich lokalizacji. Firma, która korzysta z narzędzi reklamowych Facebooka, nie dokonuje transferu danych użytkowników ani nie przetwarza ich danych w sposób, który wymagałby spełnienia wymogów dotyczących transferów danych poza EOG.

Jak szczegółowy powinien być rejestr czynności przetwarzania w przedszkolach? Czy mogliby Państwo podać konkretne przykłady dotyczące zakresu danych i czynności przetwarzania w odniesieniu do wychowanka przedszkola?

Szczegółowość prowadzenia Rejestru Czynności Przetwarzania danych zależy od Administratora. Kluczowe jest, aby Rejestr zawierał elementy wskazane w art. 30 ust. 1 RODO, w tym:

- Dane kontaktowe administratora oraz, jeśli ma to zastosowanie, współadministratorów, przedstawiciela administratora i inspektora ochrony danych;
- Cele przetwarzania danych;
- Opis kategorii osób, których dane dotyczą, oraz kategorii przetwarzanych danych osobowych;
- Kategorie odbiorców danych, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
- W przypadku przekazywania danych do państw trzecich lub organizacji międzynarodowych – wskazanie kraju lub organizacji oraz dokumentacja dotycząca zastosowanych zabezpieczeń;
- Planowane terminy usunięcia danych, jeżeli jest to możliwe, dla poszczególnych kategorii danych;
- Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, jeśli jest to możliwe.

Administrator decyduje o zakresie zbieranych danych, ponieważ to on ustala cele oraz sposoby ich przetwarzania. Ponadto zakres i specyfika działań mogą być uzależnione od przepisów sektorowych, takich jak prawo oświatowe. Zachęcam do zapoznania się z „Poradnikiem Ochrona danych osobowych w szkołach i placówkach oświatowych", opracowanym przez UODO i MEN, który może stanowić pomoc w tym zakresie.

Czy oznacza to, że z czynności obsługi pracownika powinna być wydzielona odrębna czynność dotycząca obsługi byłego pracownika? Czy przetwarzanie danych w ramach umowy o pracę i do końca zatrudnienia, a następnie przechowywanie dokumentów pracowniczych przez okres 10/50 lat, powinno być traktowane jako odrębne czynności ze względu na inny cel i inny termin przetwarzania?

Jak słusznie zauważono, są to odrębne cele przetwarzania danych, które należy traktować jako niezależne czynności w ramach całego procesu zatrudnienia. Pierwsza z nich dotyczy przetwarzania danych w trakcie trwania umowy o pracę i ma na celu zarządzanie bieżącymi obowiązkami pracowniczymi, natomiast druga odnosi się do przechowywania dokumentacji po zakończeniu zatrudnienia, w związku z obowiązkiem archiwizacji danych przez określony czas, zgodnie z przepisami prawa. Różnice w celach oraz okresach przechowywania danych uzasadniają ich traktowanie jako odrębne czynności, co umożliwia odpowiednie dostosowanie środków bezpieczeństwa i zarządzania danymi do specyfiki każdego z tych etapów.

Jak szczegółowe powinny być operacje opisane w rejestrze? Czy wystarczy wpisać ogólne kategorie, takie jak "obsługa zatrudnienia pracowników", czy należy podzielić je na bardziej szczegółowe operacje, jak na przykład "ewidencja czasu pracy", "rozliczenia z pracownikami - wypłaty wynagrodzeń itd."? Jak to wygląda w Państwa organizacji?

Nie ma jednolitych wytycznych dotyczących szczegółowości Rejestru ani sposobu opisywania operacji przetwarzania danych, dlatego jego forma powinna być dostosowana do potrzeb organizacji. Rejestr może być bardziej ogólny, z podziałem na główne procesy przetwarzania danych, a następnie cele, w których dane są wykorzystywane, lub bardziej szczegółowy, z rozbiciem na poszczególne procesy i operacje. Ostateczny kształt Rejestru zależy od wielkości organizacji, rodzaju przetwarzanych danych oraz wymagań prawnych, które mogą się różnić w zależności od branży.

Uważam, że przy tworzeniu Rejestru warto szczególną uwagę zwrócić na specyficzne operacje przetwarzania, takie jak profilowanie, które mogą wiązać się z istotnym ryzykiem naruszenia praw osób, których dane są przetwarzane. Przykładem może być kara nałożona przez UODO na Toyota Bank. Takie operacje powinny być dokładnie opisane i szczegółowo analizowane, aby zapewnić zgodność z wymaganiami RODO oraz właściwą ochronę danych osobowych. Niemniej jednak, nie widzę potrzeby szczegółowego opisywania każdej pojedynczej operacji przetwarzania, zwłaszcza gdy nie wiąże się to z istotnym ryzykiem. W przeciwnym razie Rejestr stanie się zbyt rozbudowany i trudny do utrzymania, co może prowadzić do zbędnych komplikacji administracyjnych.

Rejestr powinien być narzędziem umożliwiającym efektywne zarządzanie i kontrolowanie operacji przetwarzania danych, a nie obciążeniem administracyjnym. Kluczowe jest znalezienie równowagi między dokładnością a przejrzystością, aby Rejestr był skutecznym dokumentem w kontekście zapewnienia zgodności z przepisami ochrony danych osobowych, a jednocześnie łatwym do utrzymania i aktualizacji.

Mam pytanie dotyczące analizy ryzyka w kontekście ochrony danych osobowych. Jeżeli organizacja przeprowadza analizę ryzyka według zasobów, czy jest zobowiązana do przeprowadzenia dodatkowo odrębnej analizy według procesów przetwarzania danych osobowych?

Nie ma takiej konieczności. Organizacja ma swobodę w doborze metodologii przeprowadzania analizy ryzyka, o ile wyniki analizy pozwalają wykazać, jakie środki techniczne oraz organizacyjne zostały wdrożone w celu zapewnienia ochrony danych osobowych. Najważniejsze jest, aby przeprowadzona analiza była skuteczna i dostosowana do specyfiki działalności organizacji oraz rodzaju przetwarzanych danych.

Z perspektywy praktycznej, nie ma obowiązku przeprowadzania oddzielnej analizy ryzyka według procesów przetwarzania danych osobowych, jeśli organizacja stosuje podejście oparte na analizie zasobów. Jednakże, bardzo istotne jest, aby w ramach analizy ryzyka uwzględnić wszystkie istotne elementy, które mogą wpływać na bezpieczeństwo przetwarzanych danych. Podejście oparte na zasobach pozwala na zidentyfikowanie elementów infrastruktury, aplikacji, systemów i osób, które mają kluczowe znaczenie dla ochrony danych, a następnie przypisanie im odpowiednich zagrożeń, zabezpieczeń oraz identyfikację podatności.

Jedną z najlepszych praktyk w tym zakresie jest wykorzystanie metodyki bazującej na normie ISO 27005, która koncentruje się na identyfikacji zasobów oraz ocenie ryzyka związanych z ich użytkowaniem. Norma ta pozwala na kompleksowe podejście do analizy ryzyka, obejmujące zarówno zagrożenia, jak i zabezpieczenia techniczne i organizacyjne, a także określenie ewentualnych podatności, które mogą stanowić ryzyko dla danych osobowych. Podejście to jest elastyczne i może być dostosowane do różnorodnych potrzeb organizacji.

Organizacja nie prowadzi rejestru, natomiast prowadzi sprzedaż licencji i sprzętu IT dla klientów. Przetwarzamy dane kontaktowe i dane wysyłkowe na potrzeby realizacji konkretnych zamówień. W przypadkach, gdy przekazywane są inne dane, podpisujemy osobne umowy (czasem także upoważnienia dla konkretnych pracowników). Zarówno dane kontaktowe, jak i wysyłkowe przekazujemy dalej - do firm zajmujących się dystrybucją licencji/sprzętu (firmy z kapitałem polskim i zagranicznym, dane czasem wysyłane poza EOG). Przekazujemy klientom klauzule informacyjne na formularzach zamówień, gdzie również zawarte są informacje o przetwarzaniu danych. Ponadto, na naszej stronie internetowej znajduje się polityka RODO. Czy wypełniamy wszystkie obowiązki, czy jednak prowadzenie rejestru oraz zbiory danych są jednak konieczne?

Niestety, nie jestem w stanie jednoznacznie odpowiedzieć na to pytanie, ponieważ nie znam Państwa organizacji. W celu uzyskania precyzyjnej odpowiedzi, wskazany byłby audyt oraz przegląd dokumentacji, którą Państwo posiadają. Warto również pamiętać, że poza działalnością sprzedażową zatrudniacie Państwo pracowników, a tym samym ich dane osobowe powinny być przetwarzane zgodnie z RODO i obowiązującymi przepisami o ochronie danych osobowych. Należy również pamiętać, że upoważnienia do przetwarzania danych powinny być nadawane wszystkim pracownikom i współpracownikom, którzy mają do nich dostęp – niezależnie od tego, czy dotyczą one danych klientów, kontrahentów, czy innych pracowników. Jeśli zaś dane są przekazywane do państw trzecich, należy zapewnić, że transfery te odbywają się zgodnie z warunkami określonymi w art. 44-49 RODO.

Proszę się zastanowić, czy Państwa organizacja na pewno nie ma obowiązku prowadzenia Rejestru Czynności Przetwarzania. Zgodnie z art. 30 ust. 1 RODO każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. Wyjątek stanowi, że obowiązek ten nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że:

- przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- przetwarzanie nie ma charakteru sporadycznego,
- przetwarzanie obejmuje szczególne kategorie danych osobowych lub dane dotyczące wyroków skazujących i czynów zabronionych.

W praktyce niemal każdy podmiot przetwarzający dane ma do czynienia z przetwarzaniem opartym na ryzyku, a jeśli zatrudnia pracowników (niezależnie od ich liczby), będzie przetwarzał dane szczególnych kategorii (np. dane dot. zwolnień lekarskich).

W przypadku firmy międzynarodowej, gdzie dane osobowe są regularnie udostępniane innym krajom ze względu na charakter świadczonych usług, w jaki sposób należy prawidłowo określić "nazwę państwa trzeciego" w dokumentacji dotyczącej ochrony danych?

Określenie „nazwy państwa trzeciego” w dokumentacji dotyczącej ochrony danych powinno być uzależnione od konkretnego transferu oraz miejsca, do którego dane są faktycznie przesyłane. Każdy transfer danych osobowych do państw trzecich musi być starannie udokumentowany, z uwzględnieniem kluczowych informacji, takich jak kraj docelowy, cel transferu oraz środki zapewniające ochronę danych zarówno w trakcie, jak i po transferze. W dokumentacji należy precyzyjnie wskazać nazwę państwa, do którego dane są przekazywane, a także metodologię transferu, w tym zastosowane środki ochrony, takie jak standardowe klauzule umowne, decyzje o odpowiednim poziomie ochrony danych w państwie trzecim, lub inne mechanizmy zgodne z wymaganiami RODO.

Czy w przypadku prowadzenia bardzo szczegółowego rejestru czynności przetwarzania, podczas przeprowadzania analizy ryzyka, można pogrupować bardziej szczegółowe operacje w jednorodne kategorie i stworzyć analizę ryzyka dla tych podobnych grup, zamiast dla poszczególnych operacji?

Tak, w przypadku prowadzenia bardzo szczegółowego Rejestru Czynności Przetwarzania, podczas przeprowadzania analizy ryzyka, można pogrupować bardziej szczegółowe operacje w jednorodne kategorie i stworzyć analizę ryzyka dla tych podobnych grup, zamiast dla każdej z osobna. Takie podejście może ułatwić zarządzanie analizą ryzyka, zwłaszcza gdy w grę wchodzi duża liczba operacji, które mają podobny charakter i niosą podobne ryzyko.

Należy jednak pamiętać, że takie grupowanie operacji w kategorie nie zwalnia z obowiązku dokładnej oceny ryzyka, szczególnie gdy w ramach danej grupy mogą występować istotne różnice w zakresie potencjalnych zagrożeń. Ważne jest, aby analiza ryzyka była wystarczająco szczegółowa, aby uwzględniała wszystkie istotne aspekty przetwarzania danych, niezależnie od tego, czy są one oceniane indywidualnie, czy w ramach grupy.

Dodatkowo, jeżeli dla jakiegoś procesu będzie konieczne przeprowadzenie oceny skutków dla ochrony danych (DPIA – Data Protection Impact Assessment), to należy pamiętać, aby taki proces został uwzględniony w analizie ryzyka.

Gdzie znajdziemy informacje nt. operacji przetwarzania?

Jak wspomniałam podczas webinaru, brak precyzyjnej definicji prowadzi do „rozproszenia informacyjnego". Niemniej jednak poniższe źródła pomogą nam zdefiniować operacje oraz określić, w jaki sposób należy je charakteryzować:

- RODO (art. 4 ust. 2, art. 30 ust. 1, 35)
- Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony;
- Wytyczne nr 4/2019 dotyczące artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych
- Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679
- Wytyczne Dotyczące Wykonania Wyroku Trybunału Sprawiedliwości Unii Europejskiej W Sprawie „Google Spain Sl I Google Inc. Przeciwko Agencia Española De Protección De Datos (Aepd) I Mario Costeja González" C-131/12 .

Wartość ODO 24 tkwi w merytoryce zespołu ekspertów

Ochrona danych osobowych

Bezpieczeństwo informacji

Szkolenia RODO

Sprawdź nas

Tomasz Ochocki
Koordynator
zespołu merytorycznego

ZAPYTAJ O OFERTĘ