Vademecum ochrony danych – co warto wiedzieć?

Jak korzystać z praw gwarantowanych przez RODO?

Ogólne rozporządzenie o ochronie danych osobowych (RODO) to akt, który bezpośrednio obowiązuje we wszystkich państwach członkowskich Unii Europejskiej, w sposób jednolity regulując prawa obywateli i obowiązki administratorów.

Dane osobowe to informacje, które pozwalają na ustalenie Twojej tożsamości. To Twoje imię, nazwisko, miejsce zamieszkania, numer telefonu czy Twój adres e-mail lub dane o lokalizacji.

Przetwarzanie danych to z kolei wszystkie działania, które wykorzystują dane osobowe, jak np. ich zbieranie, utrwalanie, porządkowanie, przechowywanie, przeglądanie, wykorzystywanie czy udostępnianie.

RODO przyznaje osobom fizycznym wiele praw, które pozwalają na większą kontrolę nad danymi osobowymi.

UODO przygotował wskazówki, jak korzystać z praw gwarantowanych przez RODO.

Masz prawo wiedzieć, co będzie się działo z Twoimi danymi
Powinieneś wiedzieć, kto, na jakiej podstawie i po co przetwarza Twoje dane osobowe. Firma bądź instytucja, która nimi dysponuje, powinna Cię o tym poinformować. Ma też obowiązek wskazać, jakie prawa daje Ci RODO. A masz prawo m.in. do: dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu czy do tego, by być poinformowanym o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu. Realizując obowiązek informacyjny, administrator musi też wskazać, jak długo będzie przechowywał Twoje dane, oraz podać dane kontaktowe inspektora ochrony danych (IOD), jeśli go wyznaczył.

Masz prawo w każdej chwili wycofać zgodę
Jeśli podstawą przetwarzania Twoich danych jest wyrażona przez Ciebie – świadomie i dobrowolnie – zgoda, masz prawo w dowolnym momencie ją wycofać i nie może to rodzić dla Ciebie żadnych negatywnych konsekwencji (np. podwyższenia opłaty za usługi powyżej jej standardowej wysokości). Pamiętaj, że cofnięcie zgody powinno być równie łatwe, jak jej udzielenie.

Powinieneś być informowany w sposób dla Ciebie zrozumiały

Wszelkie przekazywane Ci informacje związane z przetwarzaniem Twoich danych powinny być sformułowane jasnym i prostym, zrozumiałym dla Ciebie językiem. Dotyczy to również komunikatów informacyjnych związanych z korzystaniem z usług internetowych czy aplikacji mobilnych. Jeśli ich nie rozumiesz lub nie są dla Ciebie wystarczająco zrozumiałe, zwracaj się do administratora o przekazanie dodatkowych wyjaśnień. W Polsce językiem urzędowym jest język polski. Wszystkie komunikaty muszą być w tym języku, ale mogą być dodatkowo tłumaczone także w innych językach.

Masz prawo do bycia zapomnianym, ale nie zawsze

Wprawdzie RODO przyznało Ci prawo do bycia zapomnianym (usunięcia danych), ale pamiętaj, że nie jest ono bezwzględne. Możesz żądać jego realizacji np. wówczas, gdy: dane stały się zbędne do realizacji zakładanych celów, dane były przetwarzane niezgodnie z prawem albo wycofałeś swoją zgodę i nie ma innej przesłanki legalizującej ich wykorzystywanie. Pamiętaj jednak, że nie w każdej sytuacji masz prawo do bycia zapomnianym. Tak jest choćby wtedy, gdy dany podmiot (np. szkoła, gmina czy przychodnia) musi wykorzystywać Twoje dane, by zrealizować nałożony na niego obowiązek prawny.

Masz prawo do informacji o naruszeniu Twoich danych

Wyciek danych, ich zagubienie czy udostępnienie osobom niepowołanym – to się zdarza. I jeżeli rodzi to dla Ciebie poważne zagrożenie, to nie dziw się, że administrator Cię o tym informuje – taki ma obowiązek. Zastosuj się więc do jego wskazówek, dzięki którym możesz zminimalizować zagrożenie. Czasami np. zmiana hasła w systemie internetowym czy zastrzeżenie dokumentów pozwoli Ci zabezpieczyć swoje dane i uniknąć np. kradzieży tożsamości i związanych z tym konsekwencji, jak np. zaciągnięcie w Twoim imieniu pożyczki. W razie wątpliwości kontaktuj się z administratorem lub z wyznaczonym przez niego inspektorem ochrony danych (IOD), który ma Ci w takiej sytuacji pomóc.

Jeśli wniesiesz sprzeciw – marketing nie może być prowadzony

Jeżeli Twoje dane są wykorzystywane w celach marketingowych, a więc do przedstawiania Ci oferty towarów czy usług, w dowolnym momencie możesz się temu sprzeciwić. Jeżeli to zrobisz, Twoich danych nie wolno już wykorzystywać do takich celów.

Chroń dzieci przed nieuczciwymi praktykami

Jeśli jesteś rodzicem lub opiekunem prawnym osoby poniżej 16. roku życia, pamiętaj, że gdy korzysta ona z tzw. usług społeczeństwa informacyjnego (świadczonych drogą elektroniczną), a więc portali społecznościowych, aplikacji czy gier, to Ty decydujesz o udzieleniu zgody na przetwarzanie jej danych osobowych. To ważne, bo dzieci często są mniej świadome ryzyka i konsekwencji przetwarzania ich danych osobowych. RODO wskazuje, że należy im zapewnić szczególną ochronę, gdy ich dane są wykorzystywane do celów marketingowych czy tworzenia profili osobowych. Zwracaj uwagę, czy komunikaty kierowane do nich przez administratora są sformułowane językiem, który są one w stanie zrozumieć.

Realizacji swoich praw żądaj najpierw od administratora

Jeżeli uważasz, że ktoś nieprawidłowo postępuje z Twoimi danymi, to z nim (lub z wyznaczonym przez niego IOD) skontaktuj się w pierwszej kolejności i zażądaj wyjaśnień lub spełnienia Twojego żądania, np. sprostowania danych, odnotowania sprzeciwu, usunięcia danych.

Możesz dochodzić odszkodowania przed sądem

Pamiętaj! Jeśli podmiot, który dysponuje Twoimi danymi, wykorzystuje je niezgodnie z RODO, a Ty poniosłeś przez to szkodę majątkową lub niemajątkową, możesz dochodzić od niego odszkodowania, wszczynając postępowanie przed sądem. Masz do tego prawo niezależnie od tego, czy zamierzasz złożyć skargę do Prezesa UODO.

Jak złożyć skargę do Prezesa UODO?

Każdy, kto uważa, że jego prawa w zakresie ochrony danych osobowych nie są respektowane, może złożyć na administratora skargę do Prezesa Urzędu Ochrony Danych Osobowych. Skargi mogą być kierowane w formie pisemnej lub elektronicznej. Kierowanie skargi następuje przez Elektroniczną Skrzynkę Podawczą Prezesa Urzędu, po wypełnieniu formularza, wykorzystując w tym celu dokument pn. „Pismo ogólne do podmiotu publicznego" dostępny na portalu ePUAP2.

Pamiętaj, aby każda skarga zawierała:

- Twoje imię i nazwisko oraz adres zamieszkania;
- wskazanie podmiotu, na który składasz skargę (nazwę/imię i nazwisko oraz adres siedziby/zamieszkania);
- dokładny opis naruszenia;
- Twoje żądanie – jakich działań oczekujesz od UODO (np. usunięcia danych, wypełnienia obowiązku informacyjnego, sprostowania danych, ograniczenia przetwarzania danych itd.);
- własnoręczny podpis;

Pamiętaj, by dołączyć dowody potwierdzające nieprawidłowe działanie administratora (np. korespondencję z administratorem, umowy, zaświadczenia). Ułatwi to pracownikom Urzędu ocenę.

Skargi niezawierające Twojego imienia i nazwiska (nazwy) oraz adresu pozostawiamy bez rozpoznania z uwagi na brak możliwości kontaktu.

Jak chronić dane osobowe?

Dane osobowe, są bardzo cenne, bo dzięki nim można uzyskać dostęp do wielu dóbr. Mogą one też być wykorzystywane w celach marketingowych i sprzedażowych czy także, niestety, w celach przestępczych. Aby lepiej chronić dane osobowe każdej osoby i bezpiecznie je przetwarzać w Unii Europejskiej obowiązują specjalne przepisy, które temu służą. To ogólne rozporządzenie o ochronie danych (RODO).

UODO przedstawia kilka najważniejszych porad, w jaki sposób zadbać o swoje dane osobowe.

Uważaj, co i komu udostępnisz o sobie w Internecie

Zdarza się, że nadmiernie dzielisz się informacjami na swój temat, a w mediach społecznościowych dzielisz się informacjami o Tobie, o Twoim stanie majątkowym, miejscu pracy, wydarzeniach z Twojego codziennego życia, udostępniasz swoją lokalizację, wrzucasz zdjęcia. Przez to Internet jest źródłem wiedzy także o Twoich poglądach, zachowaniach konsumenckich, zainteresowaniach. Dane te pozwalają, np. działom marketingowym różnych firm, dostosować ofertę kierowaną do Ciebie. Ale też z takich informacji mogą skorzystać oszuści w celach przestępczych. Szczególnie gdy profil, który Ciebie dotyczy jest w pełni publiczny, możesz być narażony na użycie Twoich danych bez Twojej wiedzy i przyzwolenia niezgodnie z celami, dla których dane udostępniłeś.

Nie zostawiaj dokumentów w zastaw

Zgodnie z prawem zatrzymywanie dowodu osobistego czy paszportu bez podstawy prawnej jest karane. Utrata kontroli nad dowodem osobistym czy paszportem naraża Cię na posłużenie się tym dokumentem bez Twojej wiedzy i woli, co z kolei stwarza niebezpieczeństwo kradzieży tożsamości.

Nie pozwól robić kopii

Co do zasady nie powinieneś się godzić na kopiowanie Twojego dokumentu tożsamości. Tylko w niektórych sytuacjach jest to wyjątkowo dopuszczalne, gdy pozwalają na to przepisy prawa. Gdy administrator domaga się kopii np. Twojego dowodu osobistego, poproś, aby wskazał Ci podstawę prawną, która nakłada na niego obowiązek takiego działania.

W innych wypadkach, jak np. wypożyczenie sprzętu, w dalszym ciągu taka praktyka naraża nas na te same niebezpieczeństwa. Dlatego nie gódźmy się na to.

Nie podawaj danych przez telefon

Unikaj przekazywania danych telefonicznie – szczególnie, gdy to nie Ty inicjujesz rozmowę, ale ktoś dzwoni do Ciebie. Udostępnianie danych na odległość obarczone jest ryzykiem, brakiem pewności co do tego komu faktycznie dane są przekazane.

Upewnij się, komu faktycznie udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt, np. oddzwaniając i sprawdzając, czy dany numer i osoba faktycznie reprezentuje podmiot, na który się powołała.

Uważaj na różne formularze, poprzez które udostępniasz dane

Zachowaj rozwagę przy wypełnianiu i podpisywaniu różnego rodzaju ankiet, formularzy czy umów. Zastanów się, czy faktycznie chcesz założyć kartę lojalnościową w sklepie, by mieć rabaty lub dodatkowe promocje. W takich sytuacjach podajesz sklepom imię, nazwisko, adres zamieszkania, datę urodzenia, adres e-mail, numer telefonu, a w zamian otrzymujesz promocje, bony rabatowe, dodatkowe upominki przy zakupach.

Należy pamiętać, że administrator musi spełnić wobec Ciebie obowiązek informacyjny, czyli przekazać Ci niezbędne informacje na swój temat, podając m.in. swoją tożsamość, dane kontaktowe oraz dane kontaktowe swojego inspektora danych osobowych (o ile go wyznaczył), po co, czyli w jakim celu i na jakiej podstawie prawnej przetwarzają dane.

Unikaj podawania nadmiarowych danych

Nie podawaj wszelkich danych (danych nadmiarowych), które pozwalają na pełną identyfikację, jeżeli w danej sytuacji nie jest to konieczne. Jeśli musisz skorzystać z danej usługi, to podaj tylko dane niezbędne do jej wykonania – dobrze przemyśl przekazanie tych, których przekazanie oznaczone jest jako opcjonalne.

Wyrażam zgodę na…

Zanim zaznaczysz wszystkie zgody pozwalające na przetwarzania Twoich danych osobowych, upewnij się czego dotyczą. Zwróć uwagę, czy w formularzu zgody nie są zaznaczone one w sposób domyślny.

Dokładnie też czytaj, czego dotyczą klauzule zgód. W przypadku wątpliwości, zadawaj pytania administratorom. Powinni Cię poinformować o okresie przez jaki dane będą przetwarzane oraz o przysługujących Ci prawach, w tym dostępu do danych, ich sprostowania, usunięcia czy wniesienia sprzeciwu wobec przetwarzania, a także, czy Twoje dane będą komuś innemu (innym odbiorcom) przekazywane.

Pamiętaj, że często udzielasz zgód na wykorzystywanie danych w celach marketingowych nie tylko administratora, ale i jego partnerów biznesowych. O ile możesz, zweryfikuj, kim oni są, jakie to są firmy. Zgody na marketing „cudzy" powinny być nieobowiązkowe, powinna być Ci pozostawiona możliwość wyboru co do tego, czy taką zgodę wyrazisz.

Administrator powinien Ci zapewnić, by możliwość wycofania zgody była równie łatwa, jak jej udzielenie oraz powinieneś być poinformowany o prawie do cofnięcia zgody nim ją wyrazisz.

Nie wyrzucaj danych do śmieci, dopóki ich nie zniszczysz

Wszelkie dokumenty z Twoimi danymi, to kolejne źródło wiedzy o Tobie, zwłaszcza gdy zawierają one wiele różnych informacji umożliwiających wyciągania wniosków na Twój temat. Dlatego też - zanim wyrzucisz dokumenty do kosza – należy je zniszczyć (np. faktury, rachunki), zapiski, naklejki na opakowaniach od korespondencji czy po dostarczonych towarach, w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych.

Usuwaj trwale dane z nośników

Ogrom danych o Tobie może znajdować się na Twoich starych dyskach twardych, kartach pamięci, pendrive'ach czy innych nośnikach. Zwróć uwagę, że coraz więcej informacji na Twój temat jest zapisanych w komputerach, smartfonach, aparatach fotograficznych czy tabletach. Zanim się pozbędziesz takich urządzeń lub nośników, trwale usuń z nich dane. Jednak zwykłe ich skasowanie nie będzie wystarczające, gdyż wiele danych da się odzyskać. Dlatego zanim wyrzucisz nośnik albo go sprzedasz, usuń z niego dane, korzystając przy tym z odpowiedniego do tego oprogramowania. Warto też przywrócić ustawienia fabryczne urządzenia, aby nie było w nim zapamiętanych loginów i haseł do różnych usług i aplikacji, z jakich korzystałeś, a zwłaszcza z takich, z których nadal korzystasz.

Używaj programów chroniących urządzenia mobilne

Używaj oprogramowania chroniącego urządzenia mobilne, np. smartfon czy komputer, przed niepożądanymi działaniami z zewnątrz, np. złośliwego oprogramowania. Oprócz popularnych programów antywirusowych przydatne mogą być również te, które zabezpieczą przed ingerencją z zewnątrz tzw. firewall. Ważna jest bieżąca aktualizacje. Złośliwe oprogramowanie, przed którym chronią nas takie narzędzia, powstaje codziennie. Dlatego bez aktualnej bazy wirusów i bazy złośliwych aplikacji program antywirusowy nie będzie w pełni spełniał swojej roli.

Unikaj publicznych hotspotów

Należy unikać „otwartych" hotspotów dostępnych dla wszystkich w zatłoczonych miejscach. W przypadku korzystania z sieci w hotelu lub kawiarni należy upewnić się czy punkt dostępu, do którego się logujemy, na pewno należy do miejsca, w którym właśnie przebywamy. Jeśli nie mamy pewności, ograniczmy się do wyszukiwania informacji i nie korzystajmy z usług, które wymagają podania hasła. Należy ograniczyć się do korzystania wyłącznie ze stron internetowych obsługujących protokół HTTPS lub używając tunelu VPN.

Zadbaj o hasła

Dobrze jest, aby nie miały one nic wspólnego z Twoimi życiem osobistym, miejscem zamieszkania, Twoim imieniem i nazwiskiem, datą urodzin, imionami Twoich bliskich czy Twoich zwierząt itp., tj. informacjami, które łatwo można skojarzyć z Tobą obserwując Twoje zachowania w sieci, czy połączyć z innymi informacjami o Tobie.

Nie powinno się też zapisywać ich na kartce papieru czy w notesie. Najlepiej jest je zapamiętywać, co jest dużą sztuką, gdy musimy logować się do wielu serwisów. Pomocne w tym zakresie mogą być np. darmowe menadżery haseł, które umożliwiają nie tylko generowanie odpowiednio trudnych do złamania haseł, ale i zapamiętują je za nas. Tym samym łatwiejsza jest częstsza zmiana haseł, a ryzyko, że ktoś je pozna maleje.

Na bieżąco zmieniaj hasła dostępu do swojego komputera, do poczty elektronicznej, systemów bankowości elektronicznej, ale nawet sklepów internetowych, w których masz konto użytkownika. Staraj się przy tym korzystać z różnych haseł.

Wprowadź uwierzytelnianie wieloskładnikowe

Uwierzytelnianie wieloskładnikowe jest niezbędne, gdyż zapewnia dodatkową ochronę podczas logowania. Podczas uzyskiwania dostępu, oprócz wpisania hasła, użytkownicy muszą przejść dodatkową weryfikację tożsamości, np. poprzez wprowadzenie kodu otrzymanego na numer telefonu.

Uważaj na ogłoszenia

Przykładem sytuacji, gdy jesteśmy narażeni na utratę danych jest poszukiwanie pracy. Niestety, wśród prawdziwych ogłoszeń są i takie, których celem jest pozyskanie jak najdokładniejszych informacji na nasz temat. Warto więc bardzo dokładnie analizować takie treści i szczególną ostrożność zachować, gdy potencjalny pracodawca chce byśmy oprócz podstawowych danych na swój temat i wskazania danych do kontaktu, także np. udostępnili skany naszych dokumentów tożsamości, co nie jest niezbędne w procesie rekrutacji. Warto korzystać z oficjalnych serwisów pośrednictwa pracy.

Bądź czujny

Zachowaj ostrożność, która może uchronić Twoje dane osobowe przed dostaniem się w ręce nieupoważnionych podmiotów lub osób, gdyż wśród nich mogą znaleźć się takie (np. grupy przestępcze, złodzieje, porywacze), które pozyskane w ten sposób informacje wykorzystają niezgodnie z prawem.

- Nie odpowiadaj na maile od osób, których nie znasz, zwłaszcza gdy domagają się podania jakichś informacji o Tobie czy namawiają do kliknięcia w przesłany link lub otwarcia przesłanego załącznika, sugerują zmianę identyfikatora i hasła.
- Zachowaj ostrożność także przy korzystaniu z usług bankowości elektronicznej i dokonywaniu zakupów przez Internet.
- Zwracaj uwagę czy aby na pewno logujesz się do serwisu bankowości internetowej ze strony banku, która ma certyfikat SSL (widoczny w pasku adresu przeglądarki).
- Weryfikuj sklepy, w których chcesz coś kupić: czy w ogóle istnieją, czy i jakie mają opinie, czy są to podmioty zidentyfikowane, gdzie mają siedzibę, czy podany jest kontakt z ich właścicielem i czy kontakt ten nie jest ograniczony tylko do elektronicznego. Jeśli masz wątpliwości co do bezpieczeństwa Twoich danych zastanów się, czy koniecznie musisz dokonać zakupów u tego sprzedawcy.
- Weryfikuj regulaminy i polityki prywatności – unikaj sprzedawców nieprzedstawiających takich dokumentów czy też prezentujących w nich postanowienia zbyt ogólne, niejasno czy nieprecyzyjnie brzmiące, sformułowane niepoprawnie gramatycznie czy językowo, może to bowiem oznaczać, że są to podmioty niepodlegające polskiemu czy europejskiemu prawu.

Ochrona danych osobowych jest bardzo ważna. Odpowiednio chroniąc swoje dane osobowe, możemy ograniczyć ryzyko ich wykorzystania przez osoby do tego nieuprawnione.