Jak jest naprawdę z ochroną danych osobowych w 2021 roku w Polsce?

Czy ochrona danych osobowych w Polsce obowiązuje ? Większość z Was odpowie, że tak. Przecież wiadomo, że RODO. Niektórzy z Was nawet wiedzą na ten temat całkiem sporo, innym wydaje się, że wiedzą wszystko. Większość przedsiębiorców w Polsce jednak ma przekonanie, że RODO ich nie dotyczy, a poza tym są ważniejsze problemy, bo Covid … Jak jest naprawdę z ochroną danych osobowych w 2021 roku w Polsce? Postaramy się w prosty sposób przekazać, czym naprawdę jest RODO, przystępnie wyjaśnić definicje i pojęcia, które wynikają z przepisów prawa. Będziemy Wam też na bieżąco przedstawiać informacje dotyczące nakładanych kar na firmy, w których stwierdzono naruszenie ochrony danych osobowych. Będziemy sygnalizować zagrożenia, o których przedsiębiorcy najczęściej nie mają pojęcia, aż do momentu… kiedy problem nagle wybuchnie.

Zaczynając od początku. Czym tak naprawdę jest powszechnie używane RODO? To popularnie używany w Polsce skrót na określenie Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Co należy o tym rozporządzeniu powiedzieć z rzeczy najważniejszych – to, że obowiązuje od 25 maja 2018 r. we wszystkich krajach Unii Europejskiej. W takim samym zakresie stosowania i wymogów, bez różnicy. A jednak jeżeli ktoś miał, przez ostatnie parę lat, okazję pobytu w którymś z krajów Unii, to niewątpliwie zauważył różnice w zakresie stosowania zasad ochrony danych osobowych w poszczególnych krajach. I nic w tym dziwnego, podobnie jak w większości przepisów unijnych, w niektórych krajach ich stosowanie jest dość liberalne, w innych realizowane w niezbędnym minimum, a w innych … trzeba się mieć mocno na baczności, bo egzekwowane są wręcz w nadmiarze. I chyba każdy jest w stanie wskazać , który kraj do której grupy przyporządkować.

Na dzisiaj dwa z najważniejszych pojęć dotyczących kto jest kim w RODO . A także co to są dane osobowe.

Administrator danych (osobowych) – to podmiot, który odpowiada za prawidłowe przestrzeganie ochrony danych osobowych. Decyduje o wszystkim – jak te dane chronić, w jaki sposób i jakimi środkami. Pomimo, że można by się tak zasugerować, wcale nie musi być osobą fizyczną – może to być spółka z o.o., szkoła, teatr, fundacja, ale w przypadku prowadzenia działalności gospodarczej na swoje imię i nazwisko, administratorem będzie osoba fizyczna czyli właściciel. Co ważne – administrator danych odpowiada bezpośrednio za ochronę danych osobowych i tej odpowiedzialności nie może się pozbyć, scedować jej na kogoś innego. W związku z tym, wyznaczając u siebie osoby mające się zająć RODO w waszej firmie , musicie mieć tego świadomość, że muszą to być osoby odpowiedzialne i nieprzypadkowe. Muszą znać i rozumieć przepisy RODO. Bo i tak za ich błędy w działaniu, odpowie w pierwszej kolejności Administrator danych. A ta odpowiedzialność może być różnoraka. Od kar finansowych nakładanych przez organ nadzoru, przez sankcje finansowe nakładane przez sądy powszechne, aż po zakaz dalszego przetwarzania danych osobowych, co wiadomo jak się ma w niektórych podmiotach do dalszego prowadzenia działalności. O pierwszym odszkodowaniu zasądzonym przez polski sąd cywilny jeszcze trochę napiszemy. Teraz drugie ważne pojęcie.

Urząd ochrony danych osobowych (UODO) a właściwie **Prezes urzędu ochrony danych osobowych (PUODO).** Każdy kraj unijny ma wyznaczony tzw. Organ nadzoru nad prawidłowym przestrzeganiem ochrony danych osobowych. W Polsce takim organem jest właśnie PUODO. To organ uprawniony do kontroli , także w firmach prywatnych, wydawania decyzji skutkujących nakazami lub zakazami skierowanymi do **Administratorów danych,** a także nakładania na nich kar finansowych. PUODO może

nałożyć karę finansową nie tylko w wyniku kontroli czy prowadzonego postępowania. W ostatnich miesiącach na paru przedsiębiorców nałożone zostały kary „dyscyplinujące" (kilku i kilkunastotysięczne) za brak współpracy w trakcie kontroli czy postępowania, a także za „niechęć" do okazania PUODO wszystkich żądanych od przedsiębiorcy dokumentów.

Co to są, te wszechobecne już w naszym życiu, **dane osobowe**? Najprościej, to wszystkie dane , które pozwalają na jednoznaczne określenie, że dotyczą one konkretnej osoby fizycznej. RODO chroni bowiem tylko prawa i wolności osób fizycznych , i to tych żyjących. Dlatego pytając się w Administracji cmentarza o miejsce, w którym pochowana jest konkretna osoba powinniśmy tę informację uzyskać bez problemu, ale na pytanie, kto się tym grobem opiekuje, odmowa odpowiedzi będzie uzasadniana ochroną danych osobowych. Ale sprawa z danymi wcale taka prosta i niejednoznaczna nie jest. Zgodnie z RODO dane osobowe to **informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.** Ta identyfikacja jest możliwa bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. I już wiadomo, że sprawa nie jest taka prosta. Czy imię i nazwisko samo w sobie to dane osobowe? W praktyce mało prawdopodobne, żeby wystarczyły na zidentyfikowanie osoby fizycznej, no chyba że ma się imię i nazwisko jedyne w Polsce. Jednak z reguły, żeby zidentyfikować po imieniu i nazwisku potrzebne są dodatkowe dane, na przykład adres zamieszkania. Ale czy zawsze jest to wystarczające do jednoznacznej identyfikacji? Jeżeli pod tym samym adresem mieszkają ojciec i syn o tym samym imieniu i nazwisku to potrzebne jest dodatkowe dookreślenie, dodatkowy identyfikator. Do kwestii co to są dane osobowe będziemy jeszcze nie raz wracać przy okazji opisywania różnych przypadków stosowania RODO.

Teraz dwa przykłady naruszeń przepisów RODO, z ostatnich miesięcy, a właściwie dni. Te sprawy dotyczą sytuacji, które mogą zdarzyć się u każdego przedsiębiorcy i spowodować podobne konsekwencje. W tych przypadkach związane też z sankcjami finansowymi.

Przypadek pierwszy – Towarzystwo Ubezpieczeń i Reasekuracji Warta S.A. otrzymało karę w wysokości 85 588 zł za niezgłoszenie Prezesowi Urzędu Ochrony Danych Osobowych naruszenia ochrony danych osobowych. Do Urzędu wpłynęła informacja od osoby postronnej, którą okazał się nieuprawniony odbiorca, o naruszeniu ochrony danych osobowych, które polegało na wysłaniu pocztą elektroniczną, przez agenta ubezpieczeniowego (będącego podmiotem przetwarzającym dla Towarzystwa Ubezpieczeń i Reasekuracji Warta S.A.) polisy ubezpieczeniowej do nieuprawnionego adresata. Dokument elektroniczny zawierał dane osobowe m.in. imiona, nazwiska, adresy zamieszkania, numery PESEL oraz informacje dotyczące przedmiotu ubezpieczenia (samochód osobowy). Sytuacja zdarzyła się w firmie WARTA S.A., ale może zdarzyć się w każdej przedsiębiorstwie – w większości firm codziennie pracownicy, ale też sami właściciele wysyłają dziesiątki, setki maili w których treści często zawarte są dane osobowe. Pomyłka w adresie odbiorcy bądź wysłanie pod adres błędny może się zdarzyć w każdej chwili. W tym konkretnym przypadku sprawa jest jeszcze bardziej skomplikowana, ponieważ poczta elektroniczna przesłana została na adres, który agent otrzymał od klienta, tyle że adres był błędny. W uzasadnieniu swojej decyzji PUODO podniósł dwie kwestie: spółka nie zgłosiła naruszenia ochrony danych osobowych oraz nie powiadomiła o incydencie osób, których dotyczyło naruszenie. Organ nadzoru wszczął więc postępowanie administracyjne. Dopiero w wyniku wszczęcia postępowania spółka zgłosiła naruszenie ochrony danych osobowych oraz zawiadomiła dwie osoby, których dotyczy naruszenie. TUiR Warta S.A. uzasadniało, że naruszenie powstało na skutek wysłania dokumentu polisy ubezpieczeniowej **na błędny adres poczty elektronicznej, który wskazał sam klient**. Ponadto nieuprawniony odbiorca zwrócił się do spółki, a ta poprosiła o trwałe usunięcie wiadomości

wraz z prośbą o informację zwrotną potwierdzającą jej usunięcie. Jednak PUODO stwierdził, że: "Administrator dopuszczając możliwość wykorzystania do komunikacji z klientem poczty elektronicznej powinien mieć świadomość ryzyk związanych np. z nieprawidłowym podaniem przez klienta adresu e-mail. W związku z tym w celu minimalizacji tych ryzyk administrator powinien **wprowadzić odpowiednie środki organizacyjne i techniczne, jak np. weryfikacja podanego adresu, czy też szyfrowanie przesyłanych w ten sposób dokumentów**".

Przypadek drugi – początek roku 2021 przyniósł informację o pierwszym w Polsce wyroku Sądu cywilnego przyznającym odszkodowanie dla osoby fizycznej za naruszenie przepisów RODO. Wiedzieliście, że RODO przewiduje nie tylko sankcje finansowe nakładane przez Prezesa UODO, ale też prawo do dochodzenia odszkodowania, zarówno za szkodę majątkową, jak i niemajątkową w trybie powództwa cywilnego ? Właśnie takie odszkodowanie za szkodę niemajątkową miało miejsce w tym przypadku. Czego konkretnie dotyczyło? Czegoś co w Waszych firmach też może mieć miejsce, a z czego albo sobie nie zdajecie, albo nie chcecie zdawać sobie sprawy. Czyli z przetwarzania danych osobowych Waszych klientów, kontrahentów, pracowników w zakresie zbyt szerokim od tego, czego wymaga załatwienie sprawy. Czyli po prostu zbieraniu zbyt dużej (nadmiarowej) ilości danych osobowych. Cała sprawa opisywanego wyroku zaczęła się od kolizji drogowej. Pozew do sądu skierowała właścicielka pojazdu, której pojazd brał udział w kolizji, ale która nie prowadziła auta w chwili zdarzenia. Natomiast polisa ubezpieczeniowa OC na nią była wystawiona.
Ubezpieczyciel, w trakcie prowadzonej likwidacji szkody, przekazał poszkodowanemu w stłuczce wszystkie jej dane, w tym również PESEL i numer telefonu. Kobieta uznała, że w tym przypadku jej dane osobowe przekazane zostały z naruszeniem przepisów RODO i kierując sprawę do Sądu zażądała 10.000 zł odszkodowania za nadmierne przetwarzanie danych osobowych.
Sąd uznał jej argumenty i odwołując się do RODO, które nakazuje ograniczać zakres danych do tego, co jest niezbędne dla celów, w jakich są przetwarzane stwierdził, że numer telefonu czy PESEL nie są konieczne do dochodzenia roszczeń związanych z kolizją. I przyznał jej 1.500 zł odszkodowania.
Ten wyrok pokazuje , że jest możliwość skutecznej, alternatywnej wobec skargi do UODO, drogi dochodzenia sprawiedliwości. Przy wyciekach danych z firmy, koszty dla przedsiębiorcy z tytułu odszkodowania mogą okazać się dotkliwsze, niż kary nakładane przez PUODO. Informacja szybko się rozchodzi i szybko znajdą się chętni żeby spróbować wydostać od firm i instytucji pieniądze za nieprawidłowe przetwarzanie ich danych osobowych.

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i wsprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - Dziennik Urzędowy Unii Europejskiej L 119/1
- Artykuł 4 RODO Definicje: 1) „dane osobowe” ,
- Artykuł 4 RODO Definicje: 7) „administrator” ,
- Artykuł 51 RODO: Organ nadzorczy,
- Decyzja w sprawie TUiR WARTA S.A. - https://uodo.gov.pl/decyzje/DKN.5131.5.2020 https://uodo.gov.pl/decyzje/DKN.5131.5.2020
- Wyrok Sądu Okręgowego w Warszawie - XXV Wydział Cywilny z dnia 6 sierpnia 2020 r. XXV C 2596/19

Janusz Dębowski
Ochrona Danych Osobowych
tel. 502 434 909
biuro@etaxar.pl

Magdalena Piekuś
OCHRONA DANYCH OSOBOWYCH