**RODO – najważniejsze zmiany dla firm**

**Unijne rozporządzenie o ochronie danych osobowych to nie ewolucja, ale rewolucja w europejskich przepisach związanych z przetwarzaniem danych. Zmiany te będą dotyczyły wszystkich firm, które gromadzą informacje na temat osób fizycznych. A za zaniedbania w tym zakresie przewidziane zostały dotkliwe kary.**

25 maja 2018 r. w krajach członkowskich Unii Europejskiej zacznie obowiązywać „Rozporządzenie o ochronie danych osobowych” (RODO). Firmy, które do tego czasu nie przygotują swoich systemów i nie przeszkolą pracowników, mogą mieć poważne problemy. Za niedostosowanie się do wymaganych procedur lub uchybienia w ochronie danych nowe prawo przewiduje kary w wysokości do 2% światowego obrotu danej organizacji, a w sytuacjach szczególnie poważnych naruszeń prawa, nawet do 4%.

- W wielu przypadkach, szczególnie jeżeli mówimy o dużych organizacjach przetwarzających ogromne ilości danych osobowych, już dziś może być już za późno, by na czas zdążyć ze wszystkimi zmianami. Najlepszym rozwiązaniem jest lektura rozporządzenia połączona z merytorycznym szkoleniem lub warsztatem – mówi Krzysztof Stucke, autor szkoleń z zakresu ochrony danych osobowych w firmie szkoleniowej Effect Group.

Zmiany, które rozpoczną obowiązywać pod koniec maja dotyczą każdego administratora danych osobowych, a pod tym pojęciem kryją się wszystkie podmioty gromadzące i przetwarzające informacje o osobach fizycznych, a więc także firmy. Nowe przepisy przygotowane zostały głównie z myślą o dużych przedsiębiorstwach, których główna działalność wiąże się z operacjami przetwarzania danych na dużą skalę. Nie oznacza to jednak, że najmniejsze firmy nie mają czym się przejmować.

- Co do zasady, każda firma, bez względu na formę prawną prowadzenia działalności, jest zobowiązana do wdrożenia procedur i podlega pod przepisy RODO. Przepisy europejskiego rozporządzenia nie dzielą podmiotów na małe i duże, a więc dotyczą zarówno wielkich korporacji, jak i firm jednoosobowych – podkreśla Krzysztof Stucke.

**Rejestr czynności przetwarzania danych osobowych**

Zgodnie z obowiązującymi obecnie przepisami, każda baza danych osobowych powinna zostać zgłoszona do Generalnego Inspektora Danych Osobowych (GIODO). W momencie wejścia w życie nowych przepisów, obowiązek ten zniknie. Bazy nie będzie już trzeba zgłaszać, jednak w większości sytuacji administrator danych będzie musiał prowadzić wewnętrzny rejestr czynności przetwarzania danych osobowych.

- Rejestr ma pokazywać w szczególności, w jakich procesach w organizacji są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jakie zabezpieczenia zastosował administrator. Ponadto dokument ten będzie musiał zostać udostępniony na każde wezwanie GIODO – mówi trener Effect Group.

Rejestr będą zobowiązane prowadzić m.in. przedsiębiorstwa zatrudniające powyżej 250 pracowników. Większość mniejszych firm nie będzie miała takiego obowiązku, chyba że przetwarzają dane w sposób ciągły (np. agencje marketingowe świadczące usługi mailingów reklamowych czy firmy medyczne). Rejestr obligatoryjnie prowadzić muszą także te organizacje, które przetwarzają dane wrażliwe (np. wyroki skazujące).

**Inspektor ochrony danych osobowych**

Rozporządzenie ustanawia obowiązek powołania inspektora ochrony danych osobowych, przy czym dotyczy to sytuacji analogicznych do przedstawionych powyżej – głównie firm zatrudniających powyżej 250 pracowników lub mniejszych organizacji, jeśli zajmują się one monitorowaniem osób fizycznych na dużą skalę (bądź przetwarzają dane wrażliwe).

Inspektor ochrony danych powinien czuwać nad przestrzeganiem przepisów rozporządzenia przez administratora danych i jego pracowników, kontaktować się z organem nadzoru w celu zgłaszania naruszeń wynikających z nieprzestrzegania rozporządzenia, czy też wydawać zalecenia dotyczące ochrony danych osobowych.

- Administrator włącza inspektora we wszystkie bieżące sprawy dotyczące ochrony danych osobowych na każdym etapie procesu gromadzenia i przetwarzania danych oraz w sprawy związane z ryzykiem naruszenia praw lub wolności. Nowością przewidzianą w rozporządzeniu jest możliwość wyznaczenia jednego inspektora danych przez grupę przedsiębiorców. A także to, że inspektor będzie punktem kontaktowym dla osób, których dane przetwarza administrator – wyjaśnia Krzysztof Stucke.

**Obowiązek zgłaszania naruszeń**

Zgodnie z RODO, jeśli w danej organizacji wystąpi jakikolwiek incydent w zakresie naruszenia bezpieczeństwa danych osobowych, administrator musi taki przypadek zgłosić do instytucji nadzorującej w przeciągu 72 godzin od stwierdzenia naruszenia. Oznacza to, że np. firma będzie musiała „donieść” sama na siebie, jeśli bezpieczeństwo danych osobowych zostało zagrożone.

**Uaktualnione klauzule i regulaminy**

Przed wejściem w życie nowych przepisów, firmy powinny dostosować do nich treści umów, regulaminów czy choćby formularzy zawierających opcję wyrażenia zgody na przetwarzanie danych osobowych.

Osoby, których dane będą zbierane, muszą otrzymać m.in. dane kontaktowe do administratora danych, a także wyjaśnienie, z czego wynika prośba o podanie danych oraz celu w jakim dane są zbierane. Przedsiębiorstwo, prosząc o podanie danych, będzie musiało poinformować także o zakresie i czasie przetwarzania takich informacji. A to oznacza, że umowy, regulaminy czy też klauzule dotyczące ochrony danych osobowych będą jeszcze obszerniejsze niż dotychczas.

**Informacja, przenoszenie i usuwanie danych**

Osoba, której dane są przetwarzane, uzyska prawo do otrzymania informacji na temat danych, jakie posiada na jej temat dowolna organizacja. Informację taką należy przekazać na prośbę zainteresowanego w ciągu miesiąca od jej złożenia i musi być ona podana w sposób zrozumiały i w dostępnej formie. Uzyskanie takich danych będzie bezpłatne.

Mechanizm ten powiązany został z prawem do przenoszenia danych. Można więc będzie poprosić o przeniesienie danych osobowych od jednego do drugiego usługodawcy (np. przy zmianie operatora telefonicznego). Będzie to oznaczało, że firma przekazująca utraci prawo do dalszego korzystania z danych, które zostały przeniesione.

Jeszcze innym aspektem tego prawa będzie „prawo do zapomnienia”. Osoba, której dane są przetwarzane, może wnioskować do administratora danych o usunięcie wszelkich informacji na jej temat, z wyłączeniem tych, których przetwarzanie wynika z wymogów prawa.

**Profilowanie klientów**

Obecnie powszechne jest w internecie kierowanie reklam do określonych klientów na podstawie wcześniej dokonywanych zakupów lub ich zainteresowań, ustalanych na podstawie plików „cookies”. W efekcie osobie, która np. przegląda w sklepie internetowym laptopy, sklep może później wyświetlać reklamy podobnych urządzeń. To właśnie jeden z możliwych rodzajów profilowania klientów.

Gdy rozporządzenie wejście w życie, osoby profilowane będą musiały zostać poinformowane o stosowaniu takiego mechanizmu i jego konsekwencjach. Poza tym, na gruncie nowych przepisów osoba fizyczna zyska prawo do sprzeciwienia się profilowaniu. Oznacza to, że firma stosująca tego typu metody marketingowe, musi zapewnić takie mechanizmy, które będą umożliwiały wyłączenie z profilowania tych klientów, którzy sobie tego nie życzą.

**„Ludzki” język – obowiązkowy**

Rozporządzenie wymusza na wszystkich administratorach danych, aby informacje takie jak np. zgody marketingowe lub regulaminy były formułowane jasnym i prostym językiem, a także, by były zwięzłe i zrozumiałe. Gdy informacje i komunikaty są kierowane do dzieci, wtedy język powinien być w sposób szczególny dopasowany do takiej grupy odbiorców.

- To, czy administratorzy będą się stosować do tych nakazów i jaki w praktyce będzie język komunikacji, pokaże przyszłość. Trudno ustalić jeden wzór poprawnego komunikatu, tak jak trudno ustalić wzorzec odbiorcy informacji. W praktyce, wymóg ten może okazać się punktem zapalnym w relacjach pomiędzy administratorem danych osobowych oraz nowym GIODO – uważa trener Effect Group.

**Warto uaktualnić wiedzę pracowników**

Powyżej wymienione zmiany nie wyczerpują tematu. Dodatkowo, trzeba wziąć pod uwagę, że w życie będą wchodziły również przepisy krajowe, uszczegóławiające stosowanie ochrony danych osobowych w rozmaitych aspektach, np. w odniesieniu do ochrony pracowników.

- Kodeks pracy również będzie wymagał zmian ze względu na wejście w życie przepisów RODO. Najważniejsze dotyczą nowego zakresu danych osoby ubiegającej się o zatrudnienie, możliwości korzystania przez pracodawcę z danych biometrycznych, czy też stosowania monitoringu – zwraca uwagę Krzysztof Stucke. - Zmiany pojawią się w ustawie o zakładowym funduszu świadczeń socjalnych i prawie bankowym. W tej ostatniej ustawie pracodawca uzyska prawo żądania danych biometrycznych oraz przedłożenia informacji dotyczącej karalności – dodaje.

W związku z tym, że zmiany, jakie wprowadza RODO są bardzo poważne i dotyczą wielu aspektów funkcjonowania przedsiębiorstw, niezwykle istotne jest poinformowanie pracowników o nowych wymogach prawnych oraz o konsekwencjach nienależytej ochrony danych osobowych.

Same zmiany w systemach organizacyjnych, czy też wprowadzenie funkcji inspektora danych osobowych nie wystarczy, jeśli pozostali pracownicy nie będą mieli wiedzy na temat podstawowych zasad oraz świadomości, jak starannie należy strzec osobistych danych na temat klientów czy też współpracowników. Na pewno warto wziąć pod uwagę możliwość przeszkolenia pracowników w tym zakresie – i to nie tylko tych, którzy będą bezpośrednio odpowiedzialni za ochronę danych.

Źródło: [Effectgroup](https://effectgroup.pl/)