**RODO po wdrożeniu – czy faktycznie działa?**

**Choć Rozporządzenie o Ochronie Danych Osobowych (RODO) weszło w życie w maju 2018 roku, wiele firm i instytucji nadal w niewystarczającym stopniu dostosowało swoje zasady do nowych przepisów. Paradoksalnie, świadczą o tym także absurdalne sytuacje, w których brak znajomości prawa zasłaniany bywa przezorną nadgorliwością, czasem sprzeczną ze zdrowym rozsądkiem.**

Zgodnie z analizami firmy doradczej PwC, nawet 50% przedsiębiorców w Polsce nie poradziło sobie z wdrożeniem przepisów wynikających z RODO. Nie wiadomo także, jaka część przedsiębiorców spośród tych, którzy deklarują, że dostosowali swoje firmy do nowych przepisów, faktycznie dokonała tego prawidłowo. Firmy audytorskie w wielu publikacjach wyrażały swoje wątpliwości co do jakości przeprowadzonych wdrożeń. Problemem może być także niedobór odpowiednio przygotowanych inspektorów ochrony danych osobowych w Polsce – specjalistów w tym zakresie jest obecnie za mało.

Z drugiej strony, media co i raz donoszą o kolejnych absurdach wynikających z nadgorliwości tych, którzy jak sądzą, usiłują przestrzegać zasad RODO. Jak np. w Poznaniu, gdzie rodzina nie mogła dowiedzieć się, czy zmarłym jest członek rodziny, ponieważ szpital nie udzielał informacji, zasłaniając się właśnie ochroną danych osobowych.

– Absurdalne sytuacje można by mnożyć w nieskończoność, zaczynając od zamkniętych cmentarzy, poprzez pseudonimy zamiast imion i nazwisk w dzienniku nauczycielskim, a kończąc na zdjętych z drzwi plakietkach z imieniem i nazwiskiem lekarza w przychodni – mówi Gabriela Rychły-Stucke, trenerka w firmie szkoleniowej Effect Group wyspecjalizowana w tematyce ochrony danych osobowych. – Moim zdaniem takie sytuacje to nie wynik RODO, ale niewiedzy a może przede wszystkim strachu przed ogromnymi karami. Można mieć wątpliwości, czy osoby doprowadzające do wyżej wymienionych sytuacji faktycznie zapoznały się z przepisami – podkreśla ekspertka.

**Więcej praw – więcej obowiązków**

Przepisy RODO oraz ustaw dostosowujących polskie prawo do europejskiego powinien znać właściwie każdy przedsiębiorca i prawie każdy pracownik. Dlaczego? Ponieważ do przetwarzania danych osobowych dochodzi praktycznie wszędzie, a konsumenci wraz z RODO otrzymali dodatkowe prawa, o które należy odpowiednio zadbać.

Każdy konsument, którego dane są przetwarzane, musi mieć zapewnione m.in.: prawo do informacji, prawo dostępu do danych osobowych, prawo do sprostowania danych osobowych, prawo do usunięcia danych osobowych, prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych, czy też prawo do sprzeciwu. Przestrzeganie tych obowiązków dotyczy nie tylko banków czy operatorów telekomunikacyjnych, ale choćby i niewielkich sklepów internetowych.

– Poza dostępem, prawem do sprostowania, usunięcia czy ograniczenia celu przetwarzania warto zwrócić uwagę na prawo do przenoszenia danych. O ile jest to technicznie możliwe, osoba której dane dotyczą, powinna mieć prawo do spowodowania, by dane osobowe zostały przesłane przez jednego administratora bezpośrednio innemu administratorowi. Ma to zastosowanie np. w bankowości czy ubezpieczeniach – mówi Gabriela Rychły-Stucke.

Poza tym niektóre podmioty mają obowiązek wyznaczenia inspektora ochrony danych osobowych. Będzie tak m.in. wówczas, gdy główna działalność firmy lub innej organizacji polega na regularnym przetwarzaniu danych osobowych na dużą skalę.

Unijna Grupa Robocza art. 29, jako przykład przetwarzania danych na dużą skalę wymieniła:

przetwarzanie w czasie rzeczywistym danych o lokalizacji klientów sieci fast foodów przez dostawcę takiej usługi;

przetwarzanie danych osobowych osób korzystających ze środków transportu publicznego;

przetwarzanie danych osobowych dla reklamy behawioralnej przez wyszukiwarki internetowe;

przetwarzanie danych osobowych (takich jako treść, ruch, lokalizacja) przez dostawcę usług internetowych i operatora usług telefonicznych;

przetwarzanie danych osobowych pacjenta przez szpital;

przetwarzanie danych osobowych przez banki i ubezpieczycieli.

– W wielu przypadkach wyznaczenie inspektora jest fakultatywne. Jednak nawet w sytuacji, gdy z przepisów nie wynika obowiązek wyznaczenia inspektora, Grupa Robocza art. 29 zaleca udokumentowanie wewnętrznej procedury, która została przeprowadzona w celu ustalenia i uwzględnienia poszczególnych przesłanek istnienia lub braku tego obowiązku – mówi ekspertka Effect Group.

Przepisy najwięcej obowiązków nakładają na firmy i instytucje, które przetwarzają dane wrażliwe. Według polskich przepisów do tego typu danych zalicza się informacje, które ujawniają poglądy polityczne, przynależność wyznaniową czy partyjną. Dane wrażliwe dotyczą także stanu zdrowia, życia seksualnego, przekonań religijnych, nałogów, karalności czy mandatów. Zapisy RODO poszerzyły katalog danych wrażliwych o dane biometryczne i genetyczne. W przypadku danych biometrycznych mowa m.in. o odręcznym podpisie, liniach papilarnych, czy sposobie chodzenia. Wyjątkowa ochrona tych danych polega m.in. na zakazie ich zbierania i przetwarzania bez pisemnej zgody osoby zainteresowanej.

RODO wprowadziło także pojęcie „pseudonimizacji”, podczas gdy we wcześniejszych przepisach o ochronie danych występowało jedynie określenie „anonimizacja”. Anonimizacja danych polega na przekształceniu danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej. Inaczej mówiąc, anonimizacja oznacza, że w efekcie naszych działań nie jest możliwe ustalenie, jakiej osoby fizycznej dotyczy dana informacja. Sposobem anonimizacji danych występujących w wersji papierowej może być np. zakreślanie danych czarnym markerem. Należy pamiętać o tym, że anonimizacja jest procesem nieodwracalnym. Czym jest natomiast pseudonimizacja?

– Pojęcie to oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie bez użycia dodatkowego „klucza”. Obrazowo – zamiast imienia i nazwiska używamy np. liczb. Ważne jest, aby klucz do odszyfrowania był przekazany innym kanałem niż zaszyfrowana wiadomość. Czyli, jeśli wysyłamy jakieś zaszyfrowane zestawienie w formie załącznika poczta elektroniczną, to klucz do otwarcia tego załącznika przesyłamy innym kanałem np. sms-em. Pseudonimizacja w odróżnieniu od anonimizacji jest procesem odwracalnym – wyjaśnia Gabriela Rychły-Stucke.

**Przedsiębiorcom i pracownikom brakuje wiedzy**

Największym problemem związanym z RODO wydaje się brak wiedzy. Zanim przepisy weszły w życie, w mediach pojawiło się wiele materiałów na temat zakresu zmian, a także wysokich kar grożących za niewłaściwą ochronę danych osobowych. Jednak wielu przedsiębiorców poprzestało na zapoznaniu się z doniesieniami medialnymi – bez lektury samego Rozporządzenia, a tym bardziej, bez przeprowadzenia odpowiedniego audytu, czy wprowadzenia nowych procedur, co pozwoliłoby na działanie w zgodzie z nowymi przepisami.

Przedsiębiorcy często nie mają świadomości, że organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych i to wytyczne właśnie tego organu powinni stosować w swoich firmach. Nie wiedzą, jak przeprowadzić analizę ryzyka, jak dostosować działy IT, a często nie wiedzą również jak prawidłowo przygotować klauzulę informacyjną, czy też jak powinny być sformułowane upoważnienia do przetwarzania danych i kto powinien je otrzymać.

– Podnośmy świadomość ludzi – apeluje Gabriela Rychły-Stucke. – Bardzo ważne są szkolenia dla pracowników, aby zauważyli, że istnieje ścisły związek pomiędzy ich zachowaniem, a naruszeniami prywatności. Ważne, żeby mieli świadomość zagrożeń, jakie mogą wystąpić przy udostępnianiu danych i żeby potrafili te zagrożenia minimalizować – dodaje.

Bardzo ważne jest, aby zrozumieć założenia RODO i to, w jak istotny sposób zmienia ono podejście do ochrony danych osobowych. Podstawowe zasady powinien znać praktycznie każdy pracownik, tym bardziej, że Rozporządzenie jest jednakowe dla każdej branży.

W pracy biurowej stosowanie właściwej ochrony danych osobowych może wymagać choćby stosowania polityki czystego biurka. W większości firm nie da się uniknąć sytuacji, w której do danego pokoju wchodzi personel sprzątający, a często także inne osoby. Pracownik, który ma świadomość, jak wrażliwą kwestią są dane osobowe, powinien zawsze blokować komputer, gdy się od niego oddala, a także nie może pozostawiać na biurku dokumentów, które mogą zawierać dane osobowe.

– Nie ma innego rozporządzenia dla działu kadr, innego dla księgowych a jeszcze innego dla brygadzistów na hali produkcyjnej. Każda osoba, która pracuje z danymi osobowymi powinna zainteresować się szkoleniami z zakresu RODO – podkreśla ekspertka Effect Group.

Ważne przy tym, aby szkolenia były prowadzone przez osoby kompetentne, które przekażą uczestnikom wiedzę w sposób przystępny i dostosowany do określonego stanowiska. Celem takiego szkolenia nie powinno być straszenie karami, ale przekazanie jak najbardziej praktycznych informacji, przydatnych podczas codziennej pracy.

Źródło: [Effect Group](https://effectgroup.pl/)