RODO - informacje

Ogólne

W roku 2016 przestała obowiązywać po 20 latach przestarzała dyrektywa 95/46/WE Parlamentu Europejskiego i Rady i została zastąpiona Rozporządzeniem Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie uchylenia dyrektywy 95/46/WE.

Jakie dane są osobowe?

To wszelkie dane, które umożliwiają identyfikację danej **osoby fizycznej** (ale bez nadmiernych kosztów, czasu i działań). Może to być IP, rejestracja samochodu, numer telefonu, Pesel, adres e-mail (bo może zawierać nazwisko, imię lub jednoznaczną ksywkę), GPS, cechy fizyczne / psychiczne / ekonomiczne / kulturowe (art. 4, pkt. 1).

Jakie dane są wrażliwe?

Lista danych wrażliwych jest zamknięta (art. 9, ust. 1 RODO):

- pochodzenie rasowe lub etniczne;
- poglądy polityczne;
- przekonania religijne i światopoglądowe;
- przynależność do związków zawodowych;
- dane genetyczne;
- dane biometryczne;
- dane dotyczące zdrowia;
- orientacja seksualna.

Administrator Danych Osobowych (ADO)

Administratorem danych osobowych jest z reguły dyrektor / właściciel firmy lub instytucji. Ustala on cele i sposoby przetwarzania danych osobowych (art. 4, pkt. 7 RODO) i jest odpowiedzialny za ich przetwarzanie (musi wykazać, że wprowadził właściwe procedury, środki techniczne i utworzył dokumentację). Jest także odpowiedzialny za wdrożenie zasad ochrony danych (np. minimalizacja, pseudonimizacja, szyfrowanie, monitorowanie, audyt, kontrola dostępu do pomieszczeń i stanowisk, polityka czystego biurka i ekranu [foldery nie powinny znajdować się na Pulpicie], szafy pancerne, upoważnienia do przetwarzania danych, zabezpieczenia IT, UPS, itp.).

Do obowiązków administratora należy opublikowanie danych kontaktowych IOD (jeśli go posiada), a także zgłoszenie go do Prezesa Urzędu Ochrony Danych Osobowych w terminie do 14 dni. Powinien także w ten sam sposób informować o wszelkich zmianach dotyczących osoby IOD.

Administrator powinien prowadzić rejestr przetwarzania danych (ale nie danych wrażliwych!), aby móc w każdej chwili udostępnić go organom nadzorczym (nie ma takiego obowiązku, jeśli firma zatrudnia mniej niż 250 osób, ale warto go prowadzić).

Do obowiązków Administratora należy także wydawanie upoważnień do przetwarzania danych (tego nie może robić IOD; dobrze jest zrobić rejestr takich upoważnień).

Do obowiązków administratora należy również zgłaszanie jednoznacznych naruszeń ochrony danych do organu nadzorczego, jakim jest Prezes Urzędu Danych Osobowych (bez zbędnej zwłoki, do 72 godzin) oraz powiadomienie o tym fakcie osób, których dane dotyczą (przy dużej

ilości klientów, można to zrobić w postaci komunikatu publicznego). Administrator w takim przypadku powinien utworzyć dokumentację zawierającą: okoliczności naruszenia; przybliżoną liczbę osób, których dane dotyczą; skutki naruszenia, podjęte działania zaradcze, dane kontaktowe IOD.

Inspektor Ochrony Danych (IOD, dawny ABI)

Jest to osoba fizyczna (nie firma!) posiadająca fachową wiedzę dotyczącą ochrony danych osobowych (brak sprecyzowanych wymagań). Podległa jest wyłącznie ADO, i jest niezależna (nie można jej wydawać instrukcji działań). Jest do dyspozycji klientów. IOD nie może być osoba, która jednocześnie przetwarza dane (konflikt interesów, musiałaby monitorować samą siebie).

Organy administracji publicznej i finansowej są zobowiązane do posiadania IOD. Firmy muszą posiadać IOD, gdy przetwarzają dane na **dużą skalę** (np. telekomunikacja) lub przetwarzają **dane wrażliwe** (np. ośrodki zdrowia, ubezpieczenia) lub zatrudniają więcej niż **250 pracowników**.

Zadaniem IOD jest:

- informowanie o obowiązkach wynikających z RODO;
- wydawanie zaleceń (opracowanie polityki bezpieczeństwa i mechanizmów zabezpieczeń → należy zachować je w tajemnicy, są tylko do wglądu GIODO i wybranych osób → nie publikujemy tego);
- szkolenia dla pracowników i ADO (mogą być zlecone komuś), które muszą być uwzględnione w planie działań (potwierdzenie obecności, testy, materiały do kursu);
- monitorowanie procedur (ale już nie bezpośrednie wdrażanie);
- współpraca z ADO;
- prowadzenie rejestru czynności;
- prowadzenie punktu kontaktowego dla klientów;

IOD jest odpowiedzialny karnie (do 2 lat więzienia) za ujawnienie tajemnicy służbowej (KK, art. 266) oraz jest odpowiedzialny **cywilnie** za naruszenie dóbr osobistych lub szkody wyrządzenie pracodawcy (kara pieniężna).

Procesor

Jest to osoba / firma, która zawarła z ADO umowę o przetwarzaniu i powierzeniu danych, za które on jest odpowiedzialny. Zasady takiej współpracy reguluje art. 28 RODO. W przypadku naruszeń, zarówno ADO jak i Procesor są odpowiedzialni. Przykład powierzenia: księgowość, zewnętrzny marketing.

Zasady przetwarzania danych

- **ograniczenie celu** (nie można zbierać ich „na zapas”; art. 5, ust. 1bc RODO);
- **ograniczenie okresu przechowywania** (art. 5, ust. 1e RODO; muszą istnieć powody lub przepisy prawne, które wymagają dłuższego przechowywania);
- **zagwarantowanie bezpieczeństwa danych** (art. 5, ust. 1f RODO; analiza zagrożeń i ich okresowa ewaluacja, co najmniej raz w roku; podejście oparte na ryzyku ludzkim, naturalnym, technicznym, proceduralnym);
- **minimalizacja danych** (nie można zbierać danych nadmiarowych);
- **rozliczalność** (za każde przetwarzanie danych lub ich wyciek musi być odpowiedzialna konkretna osoba; na przykład, do łączenia się z bazą danych, każdy pracownik powinien mieć swoje własne konto i hasło);
- **poufność**.

Uwaga: To administrator danych musi udowodnić, dlaczego jest tak duży zakres zbieranych danych, taki cel i tak długi okres przechowywania.

Sposobem na ochronę danych jest:

- **Pseudonimizacja** - gdy na przykład nazwisko zastępujemy poprzez ID (jest to proces odwracalny; art. 4, pkt 5 RODO).
- **Anonimizacja** - gdy trwale niszczymy część danych, co gwarantuje nam brak możliwości rozpoznania osoby (proces nieodwracalny).

Prawa klienta (art. 15 RODO)

- powinien otrzymać informację o przetwarzaniu jego danych (celu, kategoriach, źródle, okresie przechowywania) i swoich prawach w tym zakresie w jak najprostszej formie (można posiłkować się grafiką, i przygotować informację jak dla dziecka);
- prawo do modyfikacji swoich danych, ich usunięcia oraz prawo do „bycia zapomnianym" (art. 16, 17, 21 RODO; np. w przypadku „marketingu bezpośredniego");
- prawo do wniesienia skargi;
- prawo do otrzymania kopii swoich danych;
- prawo do przeniesienia swoich danych (art. 20 RODO);
- prawo do anulowania zgody na przetwarzanie danych lub niektórych ich składników (musi to być tak samo proste i łatwe, jak wyrażenie zgody);
- prawo do informacji o zautomatyzowaniu przetwarzania danych i ich profilowaniu (art. 22 RODO);
- prawo do informacji o zabezpieczeniach dotyczących swoich danych;
- prawo do otrzymania informacji o usunięciu danych (art. 19 RODO; jest to jednocześnie obowiązek administratora danych realizowany w każdej sytuacji usuwania danych osobowych).

Uwaga: Warunkiem niezbędnym przy realizacji tych praw jest udowodnienie swojej tożsamości przez osobę korzystającą z tych praw (np. klienta). Niektóre z tych praw w niektórych sytuacjach mogą być ograniczone wymogami prawa (interes publiczny, cele archiwalne, cele naukowe i statystyczne, cele kryminalne).

Kary

Osobą odpowiedzialną za wyciek danych jest zarówno ADO, jak i jego pracownik (jeśli udowodni mu się ewidentne zaniedbania w tym zakresie). Ciężar udowodnienia braku winy spoczywa na ADO.

Za naruszenie RODO grozi kara finansowa do 20 milionów euro (100000zł w Polsce), kara więzienia do lat 3.

Przykłady sytuacji

- Jeśli ktoś przysłał nam swoje CV, powinien być poinformowany do kiedy będzie ono przechowywane, kiedy może je otrzymać z powrotem lub kiedy zostanie zniszczone.
- W przypadku wdrożenia profilowania, pracownik musi być poinformowany o tym fakcie na 14 dni wcześniej lub w dniu podpisania umowy o pracę.
- Przed usunięciem jakichkolwiek danych osobowych, musimy o tym fakcie poinformować właściciela tych danych.
- W przypadku monitoringu (musi być bez dźwięku) należy poinformować o tym fakcie poprzez tabliczkę „*Obiekt monitorowany*" i odsyłacz do dodatkowych informacji z tym związanych (m. in. kto jest administratorem danych i kto jest IOD). Jeśli ktoś nie zgadza się na nagrywanie, nie powinien przebywać z takim budynku. W przypadku szkół publicznych, monitoring podpada pod „cel bezpieczeństwa", ale nie może obejmować szatni, WC, a obraz możemy przechowywać maksymalnie przez 3 miesiące, chyba że stanowi dowód w sprawie. Informacja o monitoringu w zakładzie pracy może być umieszczona w regulaminie pracy, który pracownik podpisuje.

- Pracodawca ma prawo przeglądać pocztę służbową pracowników i monitorować ich komputery, ale pod warunkiem, że wcześniej poinformuje ich o tym (muszą wyrazić zgodę).
- W przypadku osób poniżej 16 roku życia, zgodę na przetwarzanie danych muszą wyrazić rodzice.
- W przypadku publikowanych fotografii, należy zamazywać rejestracje samochodów, ale już nie numery domów i twarze pojedynczych osób (jeśli stanowią tło sytuacji).
- Prywatna książka adresowa w notesie (także adresy e-mail w kliencie pocztowym) nie podlegają RODO tak długo, jak nie zamierzamy tego nikomu udostępniać.
- Zdjęcia pracowników umieszczane przez firmę na FB lub blogu - także powinny być w rejestrze zbioru danych osobowych.
- Telefony służbowe pracowników a także służbowe laptopy również powinny podlegać pod RODO i politykę zabezpieczeń. W przypadku ich kradzieży, musimy zgłosić taki incydent do GIODO.
- Osoby przetwarzające dane powinny mieć osobną dedykowaną sieć Wi-Fi.
- Dopuszczalne jest ubezpieczenie się od wycieku danych.

Ostatnia aktualizacja: 31 maja 2020.