Istota regulacji RODO, czyli przepisów o ochronie danych osobowych

Biura rachunkowe, kancelarie podatkowe są jednostkami działającymi na podstawie m.in. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wraz z późniejszymi zmianami.

Z dniem 25 maja 2018 r. w życie weszło swoistego rodzaju novum, **RODO** - czyli unijne Rozporządzenie Ogólne o Ochronie Danych Osobowych, jeszcze szerzej regulujące kwestie danych osobowych.

W definicji **danych osobowych**, kryją się informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, zwłaszcza na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, adres IP, identyfikator plików cookies, bądź też jeden ze szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Zakres zastosowania RODO dotyczy szerokiej grupy osób, to:

- osoby fizyczne prowadzące działalność gospodarczą

- osoby fizyczne – wspólnicy spółek cywilnych

- osoby fizyczne – wspólnicy spółek jawnych

- dane kontaktowe osób prawnych.

Rozporządzenie reguluje kwestie przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz w sposób inny niż zautomatyzowany danych osobowych będących częścią zbioru danych lub mających stanowić część zbioru danych.

Pod pojęciem **przetwarzania** rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. W praktyce przez przetwarzanie danych należy rozumieć każdą operację albo zestaw operacji, które są dokonywane na danych osobowych za pośrednictwem środków zautomatyzowanych, a więc mogą to być m.in. takie czynności jak: rejestracja, porządkowanie, przechowywanie, gromadzenie, adaptacja, modyfikacja, odzyskiwanie, ujawniania, transmisja, blokowanie, a nawet ich niszczenie.

Głównymi zasadami przetwarzania danych osobowych są :

- zasada legalności,
- zasada celowości,
- zasada adekwatności,
- zasada merytorycznej poprawności,
- zasada czasowości,
- zasada integralności i poufności danych,
- zasada rozliczalności,
- zasada przejrzystości.

W procesie przetwarzania wyróżnia się dwie strony, **administratora** – właściciela danych, osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który ustala cele i sposoby przetwarzania oraz **procesora**, tj. podmiot przetwarzający dane w imieniu administratora. Obowiązkiem administratora jest korzystanie wyłącznie z usług podmiotów przetwarzających, zapewniających wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych dla spełnienia wymogów rozporządzenia i ochrony praw osób.

Relacje administrator-procesor są unormowane w **umowie powierzenia**, za której sporządzenie odpowiada Administrator i który udziela wyraźnej zgody na przetwarzanie danych, art. 28 RODO, określa podstawowy katalog obligatoryjnych zapisów umowy powierzenia. **Zgoda** oznacza w tym przypadku dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w postaci oświadczenia czy wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Ważnym jest aby przetwarzanie zawsze było oparte na przepisie prawnym i przesłance usprawiedliwionego celu (realizacji umowy, obowiązku prawnego, prawnie uzasadnionego interesu). Jako zakres przetwarzanych danych rozumie się poszczególne kategorie danych (np. imię, nazwisko, stanowisko, adres e mail, adres zamieszkania, płeć, dane do faktury, PESEL, nr tel.) lub zbiory danych (np. Pracownicy, Klienci, Odwiedzający). Cel to albo wskazanie konkretnych operacji, jakie może wykonać na powierzonych danych albo powołanie się na umowę, w związku, z którą następuje powierzenie.
Biura rachunkowe, kancelarie podatkowe itp. jako podmioty przetwarzające muszą mieć na uwadze także :

• zapewnienie bezpieczeństwa danych osobowych zgodnie z art.32RODO,

• pomaganie administratorowi w wywiązywaniu się z jego obowiązków związanych z realizacją praw osób, których dane dotyczą, czy też zabezpieczaniem danych,

• umożliwienie administratorowi przeprowadzanie kontroli/audytów,

• po zakończeniu umowy na żądanie administratora usuwanie lub zwracanie wszelkich danych bądź ich kopii.

Ponadto każdemu powierzającemu dane przysługuje szereg praw:

- **prawo dostępu do danych osobowych**: do informacji na temat przetwarzanych danych i do kopii danych,
- **prawo do sprostowania swoich danych**, poprawiania błędnych danych osobowych, nieaktualnych, zmienionych;
- **prawo do bycia zapomnianym**, usunięcia danych bez uzasadnionych podstaw prawnych;
- **prawo do ograniczonego przetwarzania**, polegające na przechowywaniu danych, czasowym przeniesieniu danych do innego systemu przetwarzania, czasowym usunięciu opublikowanych danych;
- **prawo do przenoszenia danych**, prawo do otrzymania danych w odpowiednim formacie, prawo do żądania od administratora przesłania danych innemu administratorowi;
- **prawo do niepodlegania profilowaniu,** zautomatyzowanemu przetwarzaniu;

- **prawo do wycofania zgody**, w każdej chwili bez podawania przyczyny, czynności wykonane do tej chwili nie tracą mocy;
- **prawo do sprzeciwu** wobec przetwarzania danych,
- **zasada przejrzystości,** zwięzła i zrozumiała, spełniana przy obowiązku informacyjnym względem podmiotów danych.

W rozporządzeniu pojawia się zagadnienie **profilowania,** uregulowane także w rekomendacji Rady Europy (2010)/13 z dnia 23 listopada 2010 r. w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych. Profilowanie to inaczej dobrowolna forma zautomatyzowanego przetwarzania danych osobowych, do oceny niektórych czynników osobowych osoby fizycznej, do analizy lub prognozy aspektów związanych z efektami pracy tej osoby fizycznej, sytuacją ekonomiczną, zdrowiem, preferencjami, zainteresowaniami, wiarygodnością, zrachowaniami, lokalizacją czy przemieszczaniem się.

Wśród obowiązków, z którymi można spotkać RODO przewidziało:
- obowiązek stosowania szczególnych środków technicznych i organizacyjnych, **pseudonimizacja i szyfrowanie danych** (prowadzenie ewidencji, rejestrów przetwarzania, wydawania upoważnień, ale i polityki czystego biurka, zamykania szaf na klucze, zakazu wstępu do pokoju osobom trzecim itd.) art. 32 RODO,
- obowiązek dokonywania oceny skutków przetwarzania dla ochrony danych, art. 35 RODO,
- obowiązek powiadomień w przypadku naruszeń ochrony danych osobowych, art. 33-34 RODO,
- obowiązek wyznaczania Administratora, IOD, art. 37-39 RODO,
- prywatność na etapie projektowania aplikacji, systemu przetwarzania danych, art. 25 RODO.

Ochrona danych osobowych wykracza poza proces przetwarzania, z uwagi na dalej idące możliwości prawne. W przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych RODO przewiduje **sankcje administracyjne i cywilnoprawne,** natomiast prawo krajowe dodatkowo **sankcje karne**. Środkami ochrony są więc na gruncie RODO, skarga do organu nadzorczego lub powództwo sądowe. GIODO(UODO) dysponuje także uprawnieniami naprawczymi (ostrzeżenia i upomnienia). Istnieje możliwość wprowadzenia czasowego lub całkowitego ograniczenia przetwarzania, czy też obciążenia karą pieniężną. Niemniej każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia posiada prawo uzyskania od administratora lub podmiotu przetwarzającego **odszkodowanie za poniesioną szkodę**.

Każda osoba wyrażająca chęć zapoznania się z szczegółowym opisem działania, procedurami z zakresu ochrony danych osobowych powinna zaznajomić się z **Polityką bezpieczeństwa** oraz **Instrukcjami**, wymaganymi przez powszechnie obowiązujące przepisy prawa, których posiadaczami są wszystkie podmioty władające danymi osobowymi.