

Sieniawa, dnia 14 maja 2018 r.

Komunikat nr 3/2018
dla klientów Biura Rachunkowego „ATUT”
w sprawie ochrony danych osobowych - RODO

Już od 25 maja 2018 r. zaczną obowiązywać nowe przepisy dotyczące ochrony danych osobowych. RODO chroni szeroko pojęte dane osobowe od danych kontaktowych po dane biometryczne. Przepisy obejmują wszystkie podmioty, które przetwarzają dane dotyczące osób fizycznych. Przetwarzanie oznacza jakiegokolwiek operacje wykonywane na danych osobowych, takie jak ich zbieranie, przechowywanie, usuwanie, opracowywanie, udostępnianie. Przedsiębiorca może być administratorem danych osobowych lub jako podmiot przetwarzający dane osobowe. Administratorem danych osobowych można uznać np.:

- pracodawcę w stosunku do danych osobowych swoich pracowników,
- sprzedawcę w sklepie internetowym w stosunku do danych osobowych swoich klientów,
- pozostałych sprzedawców dysponujących danymi osobowymi osób fizycznych.

Podmiotem przetwarzającym dane osobowe będzie administrator, ale również biuro rachunkowe, które przetwarza pozyskane przez Państwa dane osobowe, przekazane do biura rachunkowego. Moje biuro rachunkowe na mocy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wprowadziło już w 2016 roku stosowne zapisy w umowach zawieranych pomiędzy mną, a Państwem (klientami biura) na podstawie których jestem upoważniony do przetwarzania danych osobowych. Po wejściu w życie nowej polskiej ustawy o ochronie danych osobowych, o ile zajdzie taka konieczność będą przygotowane stosowne aneksy do istniejących umów.

Nowe unijne przepisy wprowadzają szereg obowiązków, nowe rodzaje odpowiedzialności, ale też sankcje finansowe. Prognozowane kary to miliony euro lub setki tysięcy złotych w zależności od podmiotu, który zostanie ukarany. Ale są też inne zmiany:

- rozszerzające kategorie odpowiedzialności za naruszenie,
- wskazujące kierowników jednostek, jako osoby odpowiedzialne bezpośrednio za poprawność przetwarzania danych osobowych,
- powołujące nowych inspektorów danych osobowych (IOD),
- nakazujące przeprowadzanie audytów bezpieczeństwa, czy prowadzenie rejestrów ryzyka i naruszeń.

Metody zabezpieczania i przetwarzania danych osobowych każdy przedsiębiorca musi dostosować indywidualnie. Firmy zobowiązane są we własnym zakresie przeprowadzić wieloaspektową analizę, zawierającą ocenę ryzyk związanych z przetwarzaniem danych osobowych, a następnie na jej podstawie wdrożyć adekwatne rozwiązania.

Przetwarzanie danych osobowych będzie możliwe za wyraźną zgodą podmiotu, którego dotyczą. Osoba, której dane są faktycznie przetwarzane będzie miała prawo do uzyskania informacji:

- w jakim celu jej dane są przetwarzane,
- jakie kategorie danych są przetwarzane,

- u jakich odbiorców zostaną dane ujawnione.

Jednocześnie osoba będzie miała prawo żądania od administratora: sprostowania, usunięcia lub ograniczenia przetwarzania danych. Osobie, której dane są przetwarzane przysługuje również prawo uzyskania do nich bezpośredniego dostępu. Zgodnie z wymaganiami RODO uprawnienie uzyskania dostępu do danych osobowych realizowane będzie poprzez dostarczenie przez administratora kopii przetwarzanych danych.

Zadaniem administratora danych osobowych jest dostosowanie systemów informatycznych tak, aby na każde żądanie osoby, której dane dotyczą, można było między innymi je całkowicie i trwale usunąć. Prawo do bycia zapomnianym przysługuje podmiotowi w sytuacji między innymi gdy podmiot danych nie wyraża dłuższej zgody na przetwarzanie danych osobowych, podmiot danych sprzeciwia się przetwarzaniu jego danych osobowych na potrzeby i w zakresie marketingu bezpośredniego (w tym profilowania), dane osobowe zostały zebrane w nawiązaniu do oferowania bezpośrednio osobom poniżej 16 lat usług społeczeństwa informatycznego (np. e-handel czy portale społecznościowe).

Osoba, której dane dotyczą, ma prawo o ile to jest technicznie możliwe zażądać by jej dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi (przykładowo będzie można zażądać, aby każdy urząd lub bank, który ma nasze dane, przekazał je innemu urzędowi lub bankowi).

Unijne przepisy nakładają także obowiązek powiadomienia o wycieku danych osobowych. Obowiązek notyfikacji naruszenia ochrony danych osobowych będzie spoczywał na każdym administratorze danych osobowych. Zgodnie z RODO, naruszenie ochrony danych osobowych, należy bezwzględnie zgłosić w ciągu 72 godzin od stwierdzenia naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

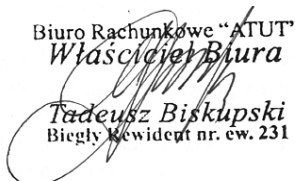
Więcej informacji na temat RODO znajdziecie Państwo w przewodniku po RODO dla małych i średnich przedsiębiorstw, które przygotowało Ministerstwo Przedsiębiorczości i Technologii.

Przewodnik ten został opublikowany na stronie MPiT:

https://www.mpit.gov.pl/media/50521/PrzewodnikMSP_RODO_2018.pdf

Równocześnie podaję akty prawne regulujące prawo o ochronie danych osobowych:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Jako rozporządzenie UE akt ten nie wymaga implementacji do prawa polskiego. Oznacza to, że 25 maja 2018 r. będzie obowiązywał i musi być stosowany w kwestii ochrony danych osobowych.
- Uzupełnieniem do europejskiego rozporządzenia RODO jest projekt polskiej ustawy z 13.09.2017 r. o ochronie danych osobowych – nadal na ścieżce legislacyjnej.

Biuro Rachunkowe "ATUT"
Właściciel Biura

Tadeusz Biskupski
Biegły Rewident nr. ew. 231