



RODO w firmie transportowej

RADCA PRAWNY PAWEŁ JUDEK

Co to jest RODO?

- ▶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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)
- ▶ Wejdzie w życie w dniu 25.05.2018 r.

Co obowiązuje obecnie?

- ▶ Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych
- ▶ Rozporządzenie MSWiA z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące przetwarzaniu danych osobowych

Co jest tworzone?

- ▶ Nowy projekt ustawy o ochronie danych osobowych wpłynął do sejmu w dniu 05.04.2018 r. (druk nr 2410)
- ▶ Wbrew pierwotnym zapowiedziom w projekcie brak jest wyłączeń w stosowaniu niektórych postanowień RODO w odniesieniu do przedsiębiorców z sektora MŚP
- ▶ Planowano wyłączenie obowiązku informacyjnego lub obowiązku informowania o naruszeniach, ale na razie zniknęło to z projektu do czasu zakończenia negocjacji z Komisją Europejską.

Zakres zastosowania RODO

- ▶ automatyczne lub częściowo automatyczne przetwarzanie danych osobowych
- ▶ ręczne przetwarzanie danych osobowych będących częścią lub mających być częścią zbioru danych

Co to są dane osobowe?

- ▶ Zarówno ustawa jak i RODO definiują to podobnie: informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
- ▶ RODO precyzuje, że chodzi wyłącznie o dane osób żyjących.
- ▶ Wskazane w przepisach przykłady danych:
 - imię i nazwisko
 - numer identyfikacyjny
 - dane o lokalizacji
 - identyfikator internetowy

Dane zwykłe a dane wrażliwe

- ▶ Dane wrażliwe wg RODO – ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby
- ▶ Szczególną podkategorią danych wrażliwych są dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.
- ▶ W przypadku danych wrażliwych odrębne podstawy przetwarzania danych oraz nakaz mocniejszego zabezpieczenia danych wrażliwych

Przetwarzanie danych osobowych

- ▶ RODO – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych
 - zbieranie
 - utrwalanie
 - organizowanie
 - porządkowanie
 - przechowywanie
 - adaptowanie
 - modyfikowanie
 - pobieranie
 - przeglądanie
 - wykorzystywanie
 - ujawnianie poprzez przesłanie
 - rozpowszechnianie
 - udostępnianie
 - dopasowywanie lub łączenie
 - ograniczanie
 - usuwanie lub niszczenie

Zasady przetwarzania danych

- ▶ zgodne z prawem (zasada legalności)
- ▶ zbierane w konkretnym celu (zasada celowości)
- ▶ adekwatne do celu (zasada adekwatności)
- ▶ prawidłowe i uaktualniane (zasada merytorycznej poprawności)
- ▶ przechowywane przez okres nie dłuższy niż niezbędny (zasada czasowości) - nowa
- ▶ przechowywane w sposób zapewniający bezpieczeństwo (zasada integralności i poufności) – nowe podejście do wymogów
- ▶ z domniemaniami „winy” administratora (zasada rozliczalności) - nowa

Podstawy przetwarzania danych osobowych

- ▶ RODO określa sytuacje, w których dopuszczalne jest przetwarzanie danych osobowych
 - osoba, której dotyczą dane, wyraziła zgodę na przetwarzanie swoich danych
 - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego administratora
 - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą
 - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osoby trzeciej, chyba że nadrzędny charakter mają interesy, prawa i wolności osoby, której dane dotyczą

Jakie podstawy przetwarzania w firmie transportowej

- ▶ zgoda osoby np. w celach marketingowych
- ▶ realizacja obowiązków wynikających z przepisów prawa np. przekazywanie danych do ZUS
- ▶ niezbędność w celu realizacji umowy – dane ze zleceń transportowych dotyczące osoby będącej stroną umowy
- ▶ prawnie usprawiedliwione cele administratora danych – dochodzenie roszczeń, cesja wierzytelności

Problem aktualności zgód

- ▶ Nie jest do końca jasne, czy zgody na przetwarzanie danych osobowych uzyskane wcześniej.
- ▶ RODO nakazuje poinformowanie osoby dającej zgodę o możliwości jej wycofania. Ustawa o ochronie danych osobowych nie miała takiego wymogu i większość zgód nie ma takiego zastrzeżenia.
- ▶ GIODO skłania się ku stanowisku, że zgody zachowują aktualność, jeśli były dobrowolne, konkretne, świadome i jednoznaczne. Spełnienie tych warunków musi wykazać administrator

Powierzenie przetwarzania danych osobowych

- ▶ Powierzenie w ramach danego podmiotu np. pracownikom na podstawie upoważnień do przetwarzania danych osobowych
- ▶ Przekazanie do podmiotu trzeciego (w tym organu) na podstawie przepisu nakładającego taki obowiązek lub na podstawie zgody osoby, której dane dotyczą
- ▶ Zawarcie umowy o powierzenie przetwarzania danych osobowych

Umowa o powierzenie przetwarzania danych osobowych

- ▶ Umowa o powierzenie przetwarzania musi być zawarta na piśmie.
- ▶ Wymogi co do treści umowy:
 - przewiduje przetwarzanie wyłącznie na udokumentowane polecenie administratora
 - nakazuje zachowanie tajemnicy przez osoby, którym powierzono dane
 - nakazuje przestrzeganie zasad bezpieczeństwa
 - po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa lub zwraca dane
 - udostępnia administratorowi wszelkie niezbędne informacje

Wybór podmiotu do przetwarzania danych

- ▶ Konieczne jest udokumentowanie, że przy wyborze podmiotu przetwarzającego administrator zadbał, aby był to podmiot, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia.

Przetwarzanie danych w firmie transportowej

- ▶ Umowy z podmiotami rozliczającymi czas pracy kierowców
- ▶ Umowy z podmiotami rozliczającymi płace minimalne
- ▶ Umowy z biurami rachunkowymi
- ▶ Umowy z podmiotami zapewniającymi geolokalizację
- ▶ Umowy dotyczące obsługi informatycznej

Istotne zmiany w stosunku do obecnej ustawy

- ▶ likwidacja obowiązku zgłaszania zbiorów danych osobowych
- ▶ wprowadzenie prawa do bycia zapomnianym (chyba że zachodzi inna niż zgoda podstawa do dalszego przetwarzania danych)
- ▶ prawo do przenoszenia danych (administrator ma obowiązek przekazać wszystkie posiadane dane dotyczące danej osoby)
- ▶ dane osobowe osób fizycznych prowadzących działalność gospodarczą podlegają ochronie

Obowiązek prowadzenia rejestru

- ▶ Każdy administrator danych osobowych będzie miał obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych
- ▶ Rejestr zawiera:
 - dane administratora
 - cele przetwarzania
 - kategorie osób, których dane dotyczą oraz kategorie danych osobowych
 - kategorie odbiorców, którym przekazano dane
 - planowane terminy usunięcia danych (jeśli możliwe)
 - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeśli możliwe)

Obowiązki informacyjne

- ▶ Administrator danych osobowych ma obowiązek informować osobę, której dane przetwarza o tym fakcie.
- ▶ Różnice w treści i sposobie przekazania informacji w zależności od tego, czy dane pozyskujemy od osoby, której dotyczą, czy od innego podmiotu, w szczególności:
 - swoje dane
 - cel przetwarzania
 - prawa osoby, której dane dotyczą
- ▶ Przewidziano wyłączenia w stosowaniu obowiązku informacyjnego.

Obowiązek autodenuncjacji

- ▶ Jeśli u administratora nastąpiło naruszenie ochrony danych osobowych, administrator niezwłocznie (max 72 h) zgłasza naruszenie organowi nadzorczemu, chyba że niewielkie prawdopodobieństwo, że naruszenie spowoduje ryzyko naruszenia praw lub wolności osoby fizycznej
- ▶ Administrator dokumentuje wszystkie naruszenia, okoliczności, skutki oraz podjęte środki zaradcze
- ▶ Jeśli naruszenie powoduje wysokie ryzyko naruszenia praw lub wolności osoby fizycznej, administrator musi powiadomić tę osobę

Polityka bezpieczeństwa

- ▶ Administrator może stworzyć dokument w postaci polityki bezpieczeństwa, która dokumentuje zasady przetwarzania danych osobowych w danej firmie.
- ▶ Nie jest to dokument obowiązkowy, ale z uwagi na zasadę rozliczalności kluczowy dla udokumentowania przestrzegania zasad wynikających z RODO

Zasady zabezpieczania danych

- ▶ Obecnie kwestie techniczne dotyczące zabezpieczenia danych reguluje ustawa i rozporządzenie, wskazując konkretne rozwiązania i wymogi, jakie powinny być spełnione.
- ▶ RODO nie wskazuje konkretnych rozwiązań technicznych, nakazując jedynie, by poziom zabezpieczeń był odpowiedni i adekwatny do ryzyka i charakteru danych
- ▶ W początkowym okresie będzie się kształtować praktyka, jakie rozwiązania techniczne uważane są za odpowiednie.

Obowiązek powołania IOD

- ▶ Niektóre kategorie podmiotów (publiczne, przetwarzające dane szczególnie na dużą skalę lub gdzie przetwarzanie jest podstawową działalnością) mają obowiązek powołać Inspektorów Ochrony Danych
- ▶ Podmiot niezależny podległy ścisłemu kierownictwu, którego zadaniami są m.in.:
 - informowanie podmiotu o obowiązkach w zakresie o.d.o.
 - monitorowanie przestrzegania regulacji o.d.o.
 - współpraca z organami nadzorczymi

Sankcje cywilne

- ▶ Podmioty, których prawa w zakresie ochrony danych osobowych naruszono, mogą dochodzić roszczeń od administratorów i domagać się zarówno naprawienia szkody jak i zapłaty zadośćuczynienia.

Sankcje administracyjne

- ▶ Kary do 20.000.000 EUR lub 4 % rocznego obrotu w zależności od tego, która kwota jest wyższa
- ▶ Przy obliczaniu wysokości kary bierze się pod uwagę szereg czynników takich jak:
 - charakter, wagę, ilość i czas trwania naruszeń
 - charakter winy
 - działania podjęte w celu zminimalizowania szkody
 - stopień odpowiedzialności
 - wcześniejsze naruszenia

Sankcje administracyjne

- stopień współpracy z organem nadzorczym
- kategorie danych osobowych
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu
- stosowanie zatwierdzonych kodeksów postępowania
- inne okoliczności łagodzące czy obciążające

Dziękuję za uwagę

Działyński i Judek Spółka Partnerska Radców
Prawnych

ul. Czartoria 1/16, 61-102 Poznań

Tel. / Fax +48 61 855 22 79, + 48 61 851 85 33

E-mail: kancelaria@dzialynski.pl

www.dzialynski.pl

www.transportoweprawo.pl