Szanowni Państwo,

w ostatnim czasie gorącym tematem stało się wejście w życie RODO, czyli unijnego rozporządzenia o ochronie danych osobowych a konkretnie Rozporządzenia 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) (Dz.U.UE.L.2016.119.1).

Im bliżej rozpoczęcia stosowania RODO, co nastąpi 25 maja 2018 r., tym więcej szkoleń, artykułów, dyskusji. Wiele firm szkoleniowych postanowiło zarobić na chaosie związanym z wprowadzaniem RODO w tym na przedsiębiorcach - szczególnie tak jak członkowie naszego Cechu - małych lub średnich przedsiębiorcach (odpowiednio zatrudniających do 50 i do 250 pracowników z wysokim limitem obrotu do 10 i 50 milionów Euro), którzy czują się zagubieni pośród wielu docierających do nich z różnych źródeł informacji. Jesteśmy straszeni milionowymi karami, powstaniem nowych i dotkliwych obowiązków oraz koniecznością skrupulatnego przygotowania się na stosowanie RODO z dniem 25 maja 2018 r. Tematem RODO zajęli się teraz nawet ci mali przedsiębiorcy, którzy kiedyś w ogóle nie myśleli o danych osobowych w swoim przedsiębiorstwie (i źle robili, bo obowiązki w tym zakresie istniały także wcześniej po rządami obowiązującej obecnie ustawy o ochronie danych osobowych).

Znając ogólnie specyfikę prowadzonej przez Państwa działalności gospodarczej, jako radca prawny Cechu Rzemiosł Spożywczych w Krakowie, **pragnę uspokoić Państwa, że dla większości z Państwa wprowadzenie RODO nie będzie stanowiło rewolucji w podejściu do ochrony danych osobowych**. Nie twierdzę bynajmniej, że RODO zupełnie nic nie zmienia i można przejść obok niego obojętnie. Uważam jednak, że w stosunku do obowiązków z zakresu ochrony danych osobowych jakie obciążały przedsiębiorców na podstawie obowiązującej obecnie polskiej ustawy o ochronie danych osobowych (która przestanie obowiązywać właśnie 25 maja 2018 r.) - RODO tak naprawdę **ułatwi** życie wielu firmom, odformalizowując ochronę danych osobowych (np. zniesienie obowiązku zgłaszania zbioru danych osobowych do GIODO). Niestety do tej pory obowiązek ten był różnie traktowany przez osoby, które powinny zgłaszać zbiory danych do GIODO. Wielu przedsiębiorców nawet nie wiedziało, że taki zbiór należy zgłaszać do GIODO. W RODO stawia się na dopasowanie stosowanego rodzaju ochrony danych do rzeczywistego charakteru prowadzonej działalności oraz do skali jej prowadzenia. Wprowadzenie RODO będzie jednak stanowiło okazję aby ci z Państwa, którzy w ogóle nie zajmowali się problematyką ochrony danych osobowych w przedsiębiorstwie i przez to czynili (tak jak większość małych przedsiębiorców na rynku) niezgodnie z dotychczas obowiązującym prawem - uporządkowali ten stan i doprowadzili do sytuacji zgodnej z przepisami (już nowymi). Jest to szczególnie rekomendowane ze względu na fakt, że dawna ustawa w praktyce nie przewidywała realnych sankcji finansowych za naruszenia przepisów ochrony danych osobowych. Teraz RODO już takie sankcje przewiduje (uspokajam, że w Państwa przypadku nie będą to kary milionowe czy wielotysięczne).

**Dla chętnych, którzy chcą zapoznać się bliżej z zasadami RODO przesyłam w załączeniu przewodnik dla małych i średnich przedsiębiorców autorstwa Ministerstwa Przedsiębiorczości i Technologii, w którym dostępnym językiem zostało przedstawione na czym polega RODO.**

**Dla tych, którzy nie planują wybrania się na szkolenie i nie mają czasu czytać przewodnika - poniżej wyjaśnię w kilku punktach (pytaniach i odpowiedziach) - do kogo w ogóle stosuje się RODO i czego dotyczy.** Proszę mieć przy tym na uwadze, że choć unijne przepisy RODO wchodzą w życie dnia 25 maja 2018 r., bo rozporządzenie UE obowiązuje w całej Unii bezpośrednio (bez konieczności wprowadzania do tego polskiej ustawy), to i tak polski ustawodawca dopiero wprowadzi kompatybilne z RODO rozwiązania krajowe w postaci nowej ustawy o ochronie danych osobowych oraz przepisów wykonawczych (np. co do dokumentacji kadrowej czy uściślenia obowiązków małych i średnich przedsiębiorców). Ministerstwo Cyfryzacji wyraża obecnie stanowisko, że w stosunku do małych i średnich przedsiębiorców nastąpi pewno ograniczenie stosowania RODO, które ma przede wszystkim ułatwić im prowadzenie biznesu. Nie oznacza to jednak, że małe i średnie przedsiębiorstwa zostaną całkowicie wyłączone z obowiązków informowania konsumentów o tym, że przetwarzają ich dane. Na razie RODO obowiązuje wszystkich jednakowo.

**1. Kto podlega RODO? Kto powinien wdrożyć RODO?**

RODO podlega każdy przedsiębiorca, który prowadzi działalność w Unii Europejskiej. Może to być działalność w jakiejkolwiek formie prawnej: spółka, jednoosobowa działalność gospodarcza, czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią. Nie ma znaczenia narodowość osób, których dane osobowe są przetwarzane. Nie ma znaczenia to, gdzie są przetwarzane dane osobowe (gdzie znajdują się serwery). RODO nie znajduje zastosowania do działalności osobistej lub domowej. To oznacza, że osoba fizyczna prowadząca działalność gospodarczą musi stosować RODO do danych osobowych swoich klientów, czy pracowników, ale nie stosuje RODO do danych przetwarzanych w celach czysto prywatnych, np. do danych adresatów wysyłanych corocznie kartek świątecznych.

2. **Jakie czynności podlegają RODO?**

   RODO stosuje się do przetwarzania danych osobowych. Dane osobowe to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą zidentyfikowaną jest taka osoba, której tożsamość znamy, którą możemy wskazać spośród innych osób. Osobą możliwą do zidentyfikowania jest taka osoba, której tożsamości nie znamy, ale możemy poznać, korzystając z tych środków, które mamy.

   Przykłady:

   • osoba zidentyfikowana: pracownik, którego dane osobowe przetwarza pracodawca; klient sklepu internetowego, który podał swoje dane osobowe do wysyłki zamówienia; osoba, która w formularzu kontaktowym podaje swoje imię, nazwisko i adres e-mail,

   • osoba możliwa do zidentyfikowania: potencjalny kontrahent, którego posiadamy tylko numer ewidencyjny w CEIDG; nadawca listu poleconego na podstawie numeru przesyłki;

   Dane osobowe to informacje o osobach fizycznych – osoby prawne nie mają danych osobowych.

   Przetwarzaniem danych osobowych są jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

   • zbieranie danych,

   • przechowywanie danych,

• usuwanie danych,
• opracowywanie danych,
• udostępnianie danych.
Co bardzo ważne, RODO obejmuje wszelkie czynności, które mają za przedmiot dane osobowe – czyli nie tylko np. usługę archiwizowania dokumentów, ale wszelkie usługi, w których dochodzi do zbierania danych osobowych.
**RODO powinni więc stosować** nie tylko przedsiębiorcy zajmujący się przetwarzaniem danych – np. usługi kurierskie itp., ale **także przedsiębiorcy, którzy przetwarzają dane osobowe przy okazji świadczenia innych usług, np. zamówienia osób fizycznych na torty komunijne, weselne.** Co do zasady nie ma związku z przetwarzaniem danych realizowanie usług dla kontrahentów będących przedsiębiorcami czy obsługa anonimowych osób kupujących w sklepie, kiedy nie podają oni swoich danych.

**3. Kto może przetwarzać dane osobowe?**

Jeżeli jakiś przedsiębiorca przetwarza dane osobowe (zbiera, przechowuje, usuwa, opracowuje, udostępnia) to może to robić jako jeden z dwóch kategorii podmiotów:
• administrator danych,
• podmiot przetwarzający dane.
Administrator danych to taki podmiot, który decyduje o celach i sposobach przetwarzania danych. Innymi słowy, decyduje o tym, po co (cele) i jak (sposoby) wykorzystać dane osobowe.
Przykłady:
• pracodawca w stosunku do danych osobowych swoich pracowników - w tym przypadku większość z Państwa będzie właśnie administratorami danych osobowych;
• sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów,
• właściciel strony internetowej w stosunku do danych osobowych osób, które zaprenumerowały newsletter.

Administratorem danych jest zawsze określony podmiot – np. spółka, a nie jego pracownik.
Przykłady:
• administratorem danych jest spółka z o.o., a nie jej prezes zarządu, czy dyrektor marketingu,
• administratorem danych jest Jan Kowalski prowadzący jednoosobową działalność gospodarczą.

Podmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego. Przykłady:
• biuro rachunkowe przetwarza na zlecenie dane osobowe przekazane mu w tym celu przez klientów lub biuro zajmujące się zewnętrznie kadrami - przetwarza przekazane mu dane osobowe pracowników administratora,
• podmiot utrzymujący na zlecenie swoich klientów konta poczty elektronicznej przetwarza na zlecenie dane osobowe,

• podmiot zajmujący się profesjonalnie niszczeniem danych osobowych przetwarza w tym zakresie dane osobowe na zlecenie swoich klientów.

Podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych odpowiednią umowę, tzw. umowę powierzenia, w której określone zostaną zasady przetwarzania danych.
W danej organizacji, dane osobowe faktycznie przetwarzają konkretne osoby fizyczne – pracownicy lub współpracownicy administratora lub podmiotu przetwarzającego dane. Takie osoby powinny posiadać upoważnienie do przetwarzania danych osobowych.

**4. Jak wiele danych osobowych można zbierać zgodnie z RODO?**

RODO wprowadza tzw. zasadę minimalizacji danych osobowych. Zgodnie z nią, można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych. Przetwarzanie danych powinno więc zostać ograniczone do takich danych, bez których nie można osiągnąć celu przetwarzania danych.

Przykład – jeżeli celem przetwarzania danych jest realizacja zamówienia w sklepie internetowym, przetwarzanie danych o sytuacji rodzinnej, czy finansowej klienta, nie będzie dopuszczalne.

**5. Co to oznacza w praktyce?**

Gdy przedsiębiorca pozyskuje dane osobowe pracowników czy kontrahentów, gromadzi je, utrwala, przechowuje i przetwarza – oznacza to, że w myśl przepisów staje się ich administratorem. A co za tym idzie musi je chronić – przed udostępnieniem osobom nieupoważnionym, przed utratą, zniszczeniem, uszkodzeniem a także przetwarzaniem z naruszeniem przepisów.

Podstawowe, przykładowe błędy skutkujące naruszeniem przepisów RODO:
1. przesyłanie drogą mailową dokumentów z poufnymi danymi, które nie są zaszyfrowane. Takie zachowanie jest niebezpieczne z dwóch powodów – ktoś może otworzyć skrzynkę adresata lub nadawca pomyli się, wysyłając wiadomość, i dane trafią nie tam, gdzie trzeba;
2. wysyłanie maili do wielu odbiorców bez ukrycia adresów innych osób. To nie tylko naruszenie prawa do prywatności, ale także złamanie ustawy o ochronie danych. Adres mailowy bowiem też podlega takiej ochronie;
3. udostępnianie firmowej skrzynki osobom trzecim;
4. umożliwienie osobom trzecim dostępu do skrzynki e-mail przez pozostawienie w widocznym miejscu hasła;
5. umożliwienie osobom trzecim dostępu do danych osobowych poprzez zwykłe wyrzucanie dokumentów z informacjami o kontrahentach czy pracownikach do kosza – zamiast do niszczarki;
6. wynoszenie informacji z firmy bez szyfrowania na różnego rodzaju nośnikach;
7. pozostawianie wydruków z danymi klientów na ogólnodostępnych urządzeniach;
8. udostępnianie haseł do komputera osobom trzecim;

9. telefoniczne udostępnianie danych niezidentyfikowanemu rozmówcy;
10. rozmowy o sprawach firmowych z podawaniem nazwisk osób, których ta rozmowa dotyczy.
---

Wiele postanowień RODO pewnie w ogóle nie dotyczy Państwa działalności - np. uregulowania dot. profilowania, prowadzenia rejestru czynności przetwarzania, itp. Niemniej jednak - należy zapoznać się z przepisami RODO aby nie okazało się, że niedopełnienie obowiązków wynikających z tego aktu narazi Państwa na sankcje finansowe czy karne.

Z poważaniem

**Wojciech Ulanowski**
**radca prawny, mobile: +48 604 820 687**