RODO

adw. **Karolina Szmit** – partner w Kancelarii Adwokackiej Knapek Rybczyński Szmit i Partnerzy. Specjalizuje się w indywidualnej obsłudze przedsiębiorców, w tym wdrożeniu procedur RODO w przedsiębiorstwie; doświadczony i ceniony szkoleniowiec.

Od 25 maja 2018 r. obowiązuje nowe unijne rozporządzenie o ochronie danych osobowych – RODO. Wszystkim przedsiębiorcom, którzy nie zdążyli przygotować się do nowych przepisów, podpowiadamy, jakie procedury wdrożyć w firmie, żeby zapewnić bezpieczeństwo przetwarzanych danych.

RODO NA SKRÓTY w pytaniach i odpowiedziach

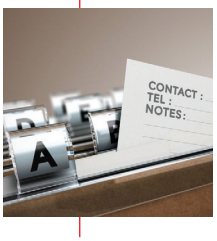
1. Co to jest RODO?

Skrót RODO oznacza Rozporządzenie o Ochronie Danych Osobowych, tj. Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 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. RODO zastąpiło polską ustawę o ochronie danych osobowych z 1997 r.

2. Kogo dotyczy RODO?

Przepisy te regulują **kwestie związane z ochroną danych osobowych i ich przetwarzaniem przez przedsiębiorców – tj. osoby fizyczne lub prawne prowadzące działalność gospodarczą,** niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą. **UWAGA!** Dane osobowe przedsiębiorcy prowadzącego jednoosobową działalność gospodarczą są chronione w takim samym zakresie jak osoby fizycznej nieprowadzącej takiej działalności. **Przepisy te nie dotyczą przetwarzania danych osobowych przez osoby fizyczne w celach prywatnych.**

3. Co zaliczamy do danych osobowych?



Wszelkie informacje, które pozwalają na zidentyfikowanie osoby fizycznej na podstawie identyfikatora takiego jak: **imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową czy społeczną tożsamość osoby fizycznej** (art. 6 RODO). W związku z tym **wizerunek osoby fizycznej** też stanowi jej daną osobową. **Szczególna kategoria danych osobowych** obejmuje m.in. pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby (art. 9 RODO).

4. Co to jest przetwarzanie danych osobowych?

To wszelkie czynności, jakie podejmujemy z posiadanymi danymi osobowymi, takie jak: **zbieranie**, **utrwalanie**, **organizowanie**, **porządkowanie**, **przechowywanie**, **adaptowanie** lub **modyfikowanie**, **pobieranie**, **przeglądanie**, **wykorzystywanie**, **ujawnianie przez przesłanie**, **rozpowszechnianie** lub **innego rodzaju udostępnianie**, **dopasowywanie** lub **łączenie**, **ograniczanie**, **usuwanie** lub **niszczenie**.

Przetwarzanie następuje niezależnie od użytego do tego celu narzędzia czy formy (np. zautomatyzowanej lub niezautomatyzowanej).

Aby móc przetwarzać dane osobowe, należy mieć do tego podstawę prawną, jak zgoda osoby fizycznej, umowa czy prawnie uzasadniony interes administratora.

5. Kto jest odpowiedzialny za ochronę danych osobowych?

Administrator, czyli osoba fizyczna lub prawna, która wykorzystuje w swojej działalności dane osobowe. Określa on, w jakim celu przetwarza dane osobowe oraz sposoby przetwarzania. Administratorem danych osobowych jest zawsze określony podmiot:

- **w przypadku jednoosobowej działalności gospodarczej** → osoba fizyczna prowadząca działalność, np. Jan Kowalski, właściciel „Piekarni Kowalski";
- **w przypadku osoby prawnej**, np. spółki z ograniczoną odpowiedzialnością → firma (podmiot), np. Chleb sp. z o.o., a nie jej pracownik czy osoba stanowiąca zarząd spółki.

w piekarni i cukierni krok po kroku

Praktycznie każdy przedsiębiorca przetwarza w swojej firmie dane osobowe. RODO reguluje zasady bezpiecznego i zgodnego z prawem postępowania z takimi danymi, jak zbieranie, przechowywanie, rozpowszechnianie czy niszczenie. Warto wspomnieć, że dane osobowe to nie tylko imię i nazwisko, ale także numer telefonu, e-mail czy adres zamieszkania. RODO w domyśle ma chronić osoby fizyczne. Przepisy ustawy chronią również dane osobowe przedsiębiorców prowadzących firmy w formie jednoosobowej działalności gospodarczej.

Cztery etapy wdrożenia

Wdrożenie RODO w przedsiębiorstwie można podzielić na cztery etapy: analizę, przygotowanie dokumentacji i procedur bezpieczeństwa, wdrożenie dokumentacji i procedur oraz monitorowanie.

Krok pierwszy – analiza

Na etapie analizy należy dokonać inwentaryzacji posiadanych zasobów danych osobowych, ustalić podstawę prawną, która pozwala przetwarzać dane osobowe w przedsiębiorstwie, oraz przeanalizować ryzyka związane z ich przetwarzaniem. Przeglądając zasoby danych osobowych, należy podzielić je według kategorii osób, których dane przetwarzamy, m.in. **pracowników**, **współpracowników** i **klientów**.

6. Jakie obowiązki nakłada RODO na przedsiębiorcę (administratora)?

- Nakłada **obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych**, aby przetwarzanie odbywało się zgodnie z prawem unijnym.
- Kładzie nacisk na **bezpieczne przetwarzanie danych osobowych,** czyli takie, które chroni dane osobowe przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, ujawnieniem lub nieuprawnionym dostępem*.
- Administrator **musi być w stanie wykazać, że podjął odpowiednie środki** celem bezpiecznego przetwarzania danych osobowych.

*Przykładowe środki techniczne i organizacyjne:

- stosowanie zamykanych szaf, w których przechowujemy dokumenty zawierające dane osobowe,
- zainstalowanie programu antywirusowego oraz hasła dostępu do logowania na komputerze, za pomocą którego przetwarzamy dane osobowe,
- odpowiednie przeszkolenie pracowników przedsiębiorstwa w zakresie bezpiecznego przetwarzania danych osobowych.

7. Czy istnieje obowiązkowa dokumentacja, którą należy przygotować?

Przedsiębiorcy zatrudniający poniżej 250 osób (czyli mikro-, mali i średni przedsiębiorcy) mają inne obowiązki w zakresie przygotowania dokumentacji RODO niż duże podmioty. → Bezwzględnie należy przygotować **tzw. klauzulę informacyjną**, która wskaże osobie fizycznej podstawowe informacje dotyczące przetwarzania jej danych osobowych. → Jeżeli administrator przekazuje innemu podmiotowi zewnętrznemu dane osobowe do przetwarzania w jego imieniu, należy zawrzeć **umowę o powierzeniu przetwarzania danych osobowych**. Dokumentacja ta może mieć formę elektroniczną.

8. Czy warto podjąć inne kroki w związku z RODO?

Warto przygotować pełną dokumentację związaną z wdrożeniem RODO:

- → politykę ochrony danych osobowych,
- → rejestr czynności przetwarzania,
- → rejestr wszystkich kategorii przetwarzania (jeżeli przetwarzamy dane osobowe w ramach powierzenia),
- → klauzulę informacyjną,
- → wzór zgody na przetwarzanie danych osobowych,
- → umowę o powierzeniu przetwarzania danych osobowych (jeśli przekazujemy podmiotowi zewnętrznemu dane osobowe lub sami otrzymujemy je od administratora),
- → upoważnienie do przetwarzania danych osobowych w imieniu administratora (jeżeli zatrudniamy pracowników lub korzystamy ze zleceniobiorców, którzy mają dostęp do danych osobowych przetwarzanych przez administratora),
- → rejestr incydentów naruszenia danych osobowych.

Dokumentacja ta w razie konieczności pomoże nam wykazać, że działalność przedsiębiorstwa jest zgodna z RODO w zakresie przetwarzania danych osobowych.

9. Czy należy obawiać się kar finansowych wskazanych w RODO?

Niekoniecznie. Przewidziane w rozporządzeniu kary administracyjne mają być nakładane przez organ nadzorczy oprócz lub zamiast innych środków opisanych w rozporządzeniu, takich jak wydanie ostrzeżenia czy udzielenie upomnień administratorowi danych osobowych w związku z naruszeniem. Organ nadzorczy przed wydaniem decyzji o nałożeniu administracyjnej kary pieniężnej, decydując, czy w ogóle ją nałożyć, obowiązany jest rozważyć indywidualnie m.in.: charakter naruszenia, jego umyślność czy stopień współpracy z organem nadzorczym w celu usunięcia naruszenia i złagodzenia jego ewentualnych skutków.

Następnie do każdej z wyróżnionych kategorii trzeba dopasować podstawę prawną, pozwalającą na przetwarzanie danych osobowych konkretnej osoby fizycznej. Najczęściej ową podstawą prawną będzie:

- **zgoda osoby, której dotyczy przetwarzanie**,
- **umowa łącząca przedsiębiorcę z osobą fizyczną**
- oraz **obowiązek prawny ciążący na administratorze danych osobowych**.

Wszelkie podstawy prawne przetwarzania znajdują się w art. 6 RODO.

Jeżeli okaże się, że nie znajdujemy przepisu, który zezwala nam legalnie na wykorzystywanie danych osobowych, konieczne jest zaprzestanie przetwarzania i usunięcie danych. Po przeprowadzeniu szczegółowej analizy przetwarzanych danych osobowych można przejść do kolejnego kroku.

Krok drugi – dokumentacja i procedury

Pełne wdrożenie RODO obejmuje przygotowanie odpowiednich procedur i dokumentacji bezpieczeństwa w związku z przetwarzaniem danych osobowych. Projektując w naszym przedsiębiorstwie procedurę ochrony danych osobowych, należy – zgodnie z przepisami RODO – wziąć pod uwagę:

- **stan wiedzy technicznej**,
- **koszt wdrożenia**,
- **zakres i cele przetwarzania**
- oraz **ryzyko naruszenia praw i wolności osób fizycznych.**

W związku z tym jeżeli w prowadzonej piekarni lub cukierni przetwarzamy dane osobowe tylko w ograniczonym zakresie, to mamy inne obowiązki w zakresie ochrony danych osobowych niż przedsiębiorca, który przetwarza je na dużą skalę, np. w celach marketingowych. Niezależnie od tego przyjęta procedura przetwarzania danych osobowych ma wskazywać na ich bezpieczne przetwarzanie w przedsiębiorstwie. Należy przez to rozumieć podjęcie odpowiednich środków zaradczych, które zapewnią, że nie dojdzie do np. przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych. Zaprojektowana w przedsiębiorstwie procedura przetwarzania danych osobowych powinna znaleźć odzwierciedlenie w tzw. polityce ochrony danych.

Oprócz wymienionej polityki w ramach wspomnianej dokumentacji należałoby przygotować: rejestr czynności przetwarzania, rejestr wszystkich kategorii przetwarzania (jeżeli przetwarzamy dane osobowe w ramach powierzenia), klauzulę informacyjną, wzór zgody na przetwarzanie danych osobowych, umowę powierzenia danych osobowych (jeśli przekazujemy podmiotowi zewnętrznemu dane osobowe lub sami otrzymujemy je od administratora), rejestr incydentów naruszenia danych osobowych.

Stworzenie dokumentacji w zakresie polityki ochrony danych osobowych, rejestru czynności przetwarzania i wszystkich kategorii przetwarzania nie jest obowiązkowe dla małych przedsiębiorców. W związku z tym można zrezygnować z przygotowania tych dokumentów pod warunkiem, że będziemy w stanie w inny sposób wykazać, że realizujemy obowiązki nałożone na przedsiębiorcę przepisami RODO. Nowe przepisy unijne wskazują bowiem, że jedną z zasad, którą należy kierować się przy przetwarzaniu danych osobowych, jest tzw. rozliczalność. W praktyce najłatwiej to wykazać właśnie poprzez przygotowanie odpowiedniej pełnej dokumentacji. Ponadto jeżeli w prowadzonym biznesie przetwarzamy dane osobowe tylko na podstawie zawartej umowy (np. zamówieniach składanych przez klientów na produkty piekarni lub cukierni), to nie jest nam potrzebna osobna zgoda na przetwarzanie danych niezbędnych do realizacji zawartej umowy i nie musimy przygotowywać wzoru zgody na ich przetwarzanie.

Krok trzeci – wdrożenie

Po przygotowaniu procedur i dokumentacji bezpieczeństwa pora na rozpoczęcie etapu wdrażania. RODO, regulując bezpieczeństwo przetwarzania danych, wskazuje na konieczność podjęcia odpowiednich środków organizacyjnych i technicznych. Wskazane środki organizacyjne i techniczne mają charakter przykładowy i są uzależnione od narzędzia lub nośnika, jakiego używamy do ich przetwarzania.

Jeżeli w danym przedsiębiorstwie przetwarza się dane osobowe przy użyciu papieru, należy zapewnić odpowiednie przechowywanie, które uniemożliwi dostęp osób nieuprawnionych, zniszczenie lub utratę. Można to osiągnąć. np. przechowując dokumenty w zamykanych szafach czy pomieszczeniu. Jeżeli przetwarzamy dane osobowe przy użyciu komputera, to konieczne jest stosowanie technicznych zabezpieczeń, takich jak hasło dostępu, szyfrowanie, używanie programu antywirusowego. Jeżeli w przedsiębiorstwie przesyłamy dane za pośrednictwem poczty elektronicznej, to stosujemy odpowiednie zabezpieczenia sieci internetowej, tak aby uniemożliwić dostęp osób nieupoważnionych.

Etap wdrożenia obejmuje również konieczność przeszkolenia zatrudnianych pracowników. W tym celu warto skorzystać z pomocy podmiotów zewnętrznych lub uczynić to we własnym zakresie. Ważne, aby pracownicy danego przedsiębiorstwa mieli podstawową wiedzę w na temat danych osobowych oraz przyjętych w danym przedsiębiorstwie środków bezpieczeństwa.

Krok czwarty – monitorowanie

Ostatni etap wdrożenia RODO polega na regularnym testowaniu oraz ocenianiu skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Na administratorze danych osobowych spoczywa obowiązek poddawania przeglądom i uaktualniania zastosowanych środków technicznych i organizacyjnych. Mając na względzie szybki postęp techniczny, istotnym elementem skutecznej ochrony danych osobowych jest regularne upewnianie się, że podjęte w przedsiębiorstwie środki bezpieczeństwa spełniają swoje zadanie. Sposób, w jaki zamierzamy monitorować aktualność podjętych środków zaradczych, oraz częstotliwość monitorowania powinny zostać określone w polityce ochrony danych.

***

Wskazane kroki wdrożenia RODO w przedsiębiorstwie przedstawiają w sposób ogólny czynności, które należy podjąć w celu spełnienia wymogów rozporządzenia Parlamentu Europejskiego i Rady UE w sprawie ochrony danych osób fizycznych. Środki techniczne i organizacyjne mające zapewnić bezpieczeństwo przetwarzania danych osobowych muszą być indywidualnie dostosowane do działalności każdego przedsiębiorstwa. ■