Rozporządzenie o Ochronie Danych Osobowych -jak przygotować firmę do wymogów nowych przepisów

Przemysław Perka, Anna Dopart

Fundusze Europejskie
PARP
Unia Europejska
Europejskie Fundusze Strukturalne i Inwestycyjne

Czym jest RODO?

Pełna nazwa - 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 (zwane „**RODO**" lub „GDPR")

RODO zastąpi obecnie obowiązującą Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

RODO zacznie obowiązywać bezpośrednio w krajowych porządkach prawnych od **25 maja 2018 r.**

Cel **- ujednolicenie przepisów** dotyczących ochrony danych osobowych w Państwach Członkowskich Unii Europejskiej, ułatwienie prowadzenie działalności transgranicznej, czyli **ułatwienie przepływu danych osobowych w UE**.

Obecnie obowiązująca ustawa o ochronie danych osobowych **ulegnie zmianie**, w niektórych kwestiach będzie ona stanowiła uzupełnienie lub doprecyzowanie przepisów RODO.

Istotne pojęcie -„dane osobowe"

Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

Zasady legalnego przetwarzania danych osobowych w świetle RODO

1. Zasada **zgodności z prawem** (zgodność z prawem, rzetelność i przejrzystość)
2. Zasada **ograniczenia celu**
3. Zasada minimalizacji danych (**adekwatności**)
4. Zasada prawidłowości (**aktualności**)
5. Zasada **ograniczenia przechowywania**
6. Zasada **integralności i poufności**
7. Zasada **rozliczalności**

Zasada zgodności z prawem

- ***zgoda*** osoby, której dane dotyczą na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest ***niezbędne do wykonania umowy***, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne ***do wypełnienia obowiązku prawnego*** ciążącego na administratorze danych
- przetwarzanie jest ***niezbędne do ochrony żywotnych interesów osoby***, której dane dotyczą lub innej osoby fizycznej;
- przetwarzanie jest niezbędne ***do wykonania zadania realizowanego w interesie publicznym*** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne ***do celów wynikających zprawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią***,

Nowe prawa osoby, której dane są przetwarzane

Zwiększenie praw podmiotów danych, zwiększenie ochrony osób fizycznych, których dane są przetwarzane, przyznanie nowych uprawnień

- wprowadzenie procedury „right to be forgotten”
- wprowadzenie procedury przeniesienia danych

1. prawo dostępu dodanych i informacji
2. prawo do sprostowania danych, które są nieprawidłowe i uzupełnienia danych, które są niekompletne z uwzględnieniem celu przetwarzania ;

(warto wprowadzić zatem wewnętrzną procedurę „prostowania danych" i dostosować odpowiednio system)

3. prawo do ograniczenia przetwarzania
4. prawo do usunięcia danych (prawo do bycia zapomnianym)
5. prawo do przenoszenia danych

Obowiązki administratora danych

1. privacy by design –uwzględnienie ochrony danych w fazie projektowania
2. privacy by default–domyślna ochrona danych
3. privacy impact assessment–przeprowadzenie oceny skutków przetwarzania dla ochrony danych
4. wyznaczenie inspektora ochrony danych
5. prowadzenie rejestru wewnętrznego
6. zgłaszanie naruszeń RODO do GIODO oraz poinformowanie o naruszeniu podmiotu danych
7. kodeksy postępowania i mechanizmy certyfikacji
8. kompleksowe uregulowanie umów o powierzeniu przetwarzania danych
9. wprowadzenie odpowiednich zabezpieczeń danych i procedur związanych z ochroną danych

Inspektor Ochrony Danych

Obowiązek wyznaczenia:

- organ lub podmiot publiczny
- główna działalność polega na regularnym i systematycznym monitorowaniu osób na dużą skalę
- główna działalność polega na przetwarzania danych wrażliwych na dużą skalę
- jeżeli wymaga tego prawo UE lub prawo państwa członkowskiego.

W innych przypadkach administrator lub podmiot przetwarzający może wyznaczyć IOD (DPO)

Kto:

1. osoba, która ma kwalifikacje zawodowe, wiedzę fachową nt. prawa i praktyk w dziedzinie ochrony danych osobowych;
2. może to być odpowiednia osoba z personelu administratora, o ile jest to możliwe do pogodzenia i nie powoduje konfliktu interesów, możliwy outsourcing funkcji IOD, może być jeden dla grupy przedsiębiorców, opracowanie procedury wyboru i działania IOD
3. podlega bezpośrednio najwyższemu kierownictwu

Obowiązki:

1. Informowanie o obowiązkach, doradzanie;
2. Monitorowanie przestrzegania RODO i innych przepisów, działania zwiększające świadomość, szkolenia
3. Udział w Privacy Impact Assessment
4. Kontakt z organem nadzorczym i punkt kontaktowy dla osób, których dane są przetwarzane

Zgłaszanie naruszeń do organu nadzorczego i zawiadomienia podmiotu

Nowy obowiązek:
1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je GIODO, **chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**. Do zgłoszenia przekazanego GIODO po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Administrator ma obowiązek **dokumentowania wszelkich naruszeń**. Oznacza to powinność przygotowania procedury zgłaszania naruszeń i przeprowadzenia szkoleń dot. tego, czym jest naruszenie ochrony danych wśród pracowników–mechanizmy wykrywania i raportowania wewnątrz o naruszeniu
Zawiadomienie nie jest wymagane, w następujących przypadkach:
a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których

dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Sankcje

Nowy mechanizm nakładania **kar pieniężnych**. Kary mają być skuteczne, proporcjonalne i odstraszające.

I. **do 10.000.000 EUR** a w przypadku przedsiębiorstw **do 2proc. Jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego**, przy czym zastosowanie ma kwota wyższa w przypadku naruszenia obowiązków administratora i podmiotu przetwarzającego w postacim.in.:

- niezgodnego zprawemprzetwarzaniadanychosobowychdzieckawwiekuponiżej16lat;
- niezastosowanie privacy by design i privacy by default;
- niezgodne z prawem współadministrowanie danymi;
- niezgodne z prawem przetwarzanie danych przez podmiot przetwarzający;
- brak upoważnień do przetwarzania danych;
- naruszenie obowiązku rejestrowania czynności przetwarzania;
- naruszenie obowiązków zgłaszania naruszeń ochrony danych;
- brak zastosowania privacy impact assessment;
- naruszenie obowiązków w zakresie wyznaczenia IOD.

II. **do 20.000.000 EUR** a w przypadku przedsiębiorstw do **4proc. Jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego**, przy czym zastosowaniem a kwota wyższa za naruszenie:

- podstawowych zasad przetwarzania, w tym warunków zgody;
- praw osób, których dane dotyczą;
- przepisów dot. przekazywania danych do państw trzecich;
- nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.

Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO)
- najważniejsze obszary zmian

1. Czym jest RODO?

1.1. 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 (zwane „RODO" lub „GDPR").

1.2. RODO zastąpi obecnie obowiązującą Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

1.3. RODO zacznie obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r., to oznacza, że będzie bezpośrednio oddziaływało na prawa i obowiązki obywateli.

1.4. RODO ma na celu ujednolicenie przepisów dotyczących ochrony danych osobowych w Państwach Członkowskich Unii Europejskiej, co ułatwi prowadzenie działalności transgranicznej, czyli ułatwienie przepływu danych osobowych w UE.

1.5. Obecnie obowiązująca ustawa o ochronie danych osobowych ulegnie zmianie, w niektórych kwestiach będzie ona stanowiła uzupełnienie lub doprecyzowanie przepisów RODO.

2. Zakres terytorialny

2.1. Podmioty unijne

2.1.1. RODO ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego (czyli podmiotu przetwarzającego dane w imieniu administratora) w UE, niezależnie od tego, czy samo przetwarzanie odbywa się w UE.

2.2. Podmioty spoza UE

2.2.1. Podmioty spoza UE mają obowiązek stosować zasady wynikające z RODO jeśli będą przetwarzały dane osobowe osób przebywających na terytorium UE, gdy czynności przetwarzania wiążą się z:

2.2.1.1. oferowaniem towarów lub usług takim osobom w UE, których dane dotyczą, niezależnie od tego, czy wymaga się od tych osób zapłaty lub

2.2.1.2. monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE.

2.2.2. Obowiązek wyznaczenia przedstawiciela w UE (art. 27 RODO).

3. Istotne pojęcie: „dane osobowe" :

3.1. Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej

3.2. **Możliwa do zidentyfikowania osoba fizyczna** to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

4. Istotne pojęcie: „**przetwarzanie**"

4.1. Oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

4.1.1. zbieranie, utrwalanie

4.1.2. organizowanie, porządkowanie, przechowywanie

4.1.3. adaptowanie, modyfikowanie

4.1.4. pobieranie

4.1.5. przeglądanie

4.1.6. wykorzystywanie

4.1.7. ujawnianie poprzez:

4.1.7.1. przesłanie

4.1.7.2. rozpowszechnianie

4.1.7.3. innego rodzaju udostępnianie

4.1.7.4. dopasowywanie, łączenie

4.1.7.5. ograniczanie

4.1.7.6. usuwanie lub niszczenie.

5. Zasady legalnego przetwarzania danych osobowych w świetle RODO

5.1. **Zasada zgodności z prawem** (zgodność z prawem, rzetelność i przejrzystość) – przejrzystość oznacza, iż wszelkie informacje kierowane do podmiotów danych były jasne, zwięzłe, wyraźne, nie drobnym drukiem.

5.2. **Zasada ograniczenia celu** – oznacza, że dane mogą być zbierane jedynie w konkretnych, wyraźnych i prawnie usprawiedliwionych celach, które są wskazane podmiotowi danych w chwili pozyskiwania danych, na każdy cel musi być podstawa przetwarzania danych, o każdym celu administrator musi informować podmioty danych.

5.3. **Zasada minimalizacji danych (adekwatności)** – ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane, ograniczone do

minimum, nie przetwarzamy więcej danych, niż to niezbędne, ograniczamy zakres danych.

5.4. **Zasada prawidłowości (aktualności)** – należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

5.5. **Zasada ograniczenia przechowywania** - przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

5.6. **Zasada integralności i poufności** - przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

6. Zasada zgodności z prawem

6.1. RODO stanowi, iż przetwarzanie danych osobowych jest wtedy zgodne z prawem, gdy spełniony jest jeden z poniższych warunków (zamknięty katalog):

- **6.1.1.** osoba, której dane dotyczą wyraziła ***zgodę*** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- **6.1.2.** przetwarzanie jest ***niezbędne do wykonania umowy***, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- **6.1.3.** przetwarzanie jest niezbędne ***do wypełnienia obowiązku prawnego*** ciążącego na administratorze danych (podstawa musi być określona w prawie UE lub w prawie państwa członkowskiego);
- **6.1.4.** przetwarzanie jest ***niezbędne do ochrony żywotnych interesów osoby***, której dane dotyczą lub innej osoby fizycznej;
- **6.1.5.** przetwarzanie jest niezbędne ***do wykonania zadania realizowanego w interesie publicznym*** lub w ramach sprawowania władzy publicznej powierzonej administratorowi (podstawa musi być określona w prawie UE lub w prawie państwa członkowskiego);
- **6.1.6.** przetwarzanie jest niezbędne ***do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią***, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

7. **Nowe pojęcie zgody -** zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

7.1. Warunki wyrażenia zgody według RODO:

7.1.1. Oceniając, czy zgodę wyrażono **dobrowolnie**, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

7.1.2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, **które dotyczy także innych kwestii**, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

7.2. Nowe pojęcie zgody:

7.2.1. Zgoda musi być wyrażona na wszystkie cele, w jakich przetwarzane będą dane osobowe podmiotu.

7.2.2. Zgoda może być udzielona ustnie, ale na administratorze danych ciąży obowiązek wykazania, że osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych.

7.2.3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie **wycofać zgodę**. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, **jest o tym informowana, zanim wyrazi zgodę**. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

7.2.4. Wycofanie zgody oznacza konieczność zaprzestania przetwarzania danych osobowych w zakresie cofnięcia, o ile nie zachodzi inna podstawa przetwarzania danych. W praktyce oznacza to konieczność usunięcia danych ze wszystkich baz administratora oraz z bazy każdego podmiotu, któremu przekazano dane osobowe.

7.2.5. Przetwarzanie danych bez zgody lub innej podstawy przetwarzania jest nielegalne (niezgodne z prawem), podobnie jak przetwarzanie danych na podstawie zgody nieprawidłowo pozyskanej (pozyskanej niezgodnie z zasadami prawnymi).

8. **Zasada rozliczalności**

8.1. Administrator danych jest odpowiedzialny za przestrzeganie przepisów dotyczących zasad przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie.

8.2. Administrator musi być w stanie udowodnić przestrzeganie, opisanego w art. 25 RODO, obowiązku uwzględniania ochrony danych w fazie projektowania oraz zapewnienia domyślnej ochrony danych.

9. Nowe obowiązki informacyjne

9.1. Modyfikacja obowiązku informacyjnego.

9.2. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych a przed rozpoczęciem przetwarzania podaje jej wszystkie następujące informacje:

- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; (adres e-mail, telefon)
- gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych; (gdy doszło do powołania takiego inspektora)
- cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania; (przepis prawa, zgoda)
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; (odbiorca to każdy podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, stroną trzecią jest podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe)
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w określonych przepisach RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu; (np. dane będą przetwarzane do czasu przedawnienia roszczeń)
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na

zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

- informacje o prawie wniesienia skargi do organu nadzorczego;
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

10. Nowe prawa osoby, której dane są przetwarzane

10.1. **prawo dostępu do danych i informacji** (Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji dotyczących przetwarzania danych wskazanych w przepisach RODO, jak również ma prawo do uzyskania kopii swoich danych podlegających przetwarzaniu).

10.2. **prawo do sprostowania danych**, które są nieprawidłowe i uzupełnienia danych, które są niekompletne z uwzględnieniem celu przetwarzania;

10.3. **prawo do ograniczenia przetwarzania** - Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

10.4. **prawo do usunięcia danych (prawo do bycia zapomnianym)** – prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy

przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.
- Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

10.5. prawo do przenoszenia danych - Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz w sposób zautomatyzowany. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

11. Obowiązki administratora danych

- privacy by design – uwzględnienie ochrony danych w fazie projektowania
- privacy by default – domyślna ochrona danych
- privacy impact assessment – przeprowadzenie oceny skutków przetwarzania dla ochrony danych
- wyznaczenie inspektora ochrony danych
- prowadzenie rejestru wewnętrznego
- zgłaszanie naruszeń RODO do GIODO oraz poinformowanie o naruszeniu podmiotu danych
- kodeksy postępowania i mechanizmy certyfikacji
- kompleksowe uregulowanie umów o powierzeniu przetwarzania danych

- wprowadzenie odpowiednich zabezpieczeń danych i procedur związanych z ochroną danych.

12. Privacy by design

12.1. Nowa strategia ochrony danych osobowych wprowadzona w art. 25 ust. 1 RODO, zgodnie z którą: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą".

12.2. Z powyższego wynika obowiązek administratora zapewnienia, aby już na etapie projektowania nowego systemu służącego do przetwarzania danych oraz na etapie wykorzystywania go do przetwarzania danych wprowadzić do niego odpowiednie środki techniczne, które zapewnią ochronę danych osobowych i zgodność z przepisami RODO.

13. Privacy by default - Zasada domyślnej ochrony danych

13.1. Zasada powyższa została sformułowana w art. 25 ust. 2 RODO, który stanowi: **Administrator wdraża odpowiednie środki techniczne i organizacyjne**, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do **ilości** zbieranych danych osobowych, **zakresu** ich przetwarzania, **okresu ich przechowywania** oraz ich **dostępności**. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

13.2. Powyższe oznacza przyjęcie ustawień chroniących prywatność w sposób domyślny we wszystkich systemach.

13.3. Ustawienia domyślne powinny przewidywać najdalej posunięte zabezpieczenia danych i udostępniać minimalną ilość danych. Poszerzenie ilości informacji powinno nastąpić jedynie przez zmianę ustawień przez użytkownika.

14. Privacy impact assessment

14.1. Nowy mechanizm wprowadzony do systemu ochrony danych przez art. 35 RODO – ocena wpływu przetwarzania danych osobowych na prywatność osób, których dane są przetwarzane.

14.2. Administrator ma obowiązek przed rozpoczęciem przetwarzania danych przeprowadzić ocenę skutków planowanych operacji przetwarzania danych dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

14.3. Powyższą ocenę przeprowadza się w szczególności gdy:

- dokonuje się profilowania;
- przetwarzane są dane na dużą skalę dane wrażliwe lub dane dot. wyroków skazujących i naruszeń prawa;
- monitoruje się na dużą skalę miejsca dostępnie publicznie.

15. Inspektor Ochrony Danych

15.1. Obowiązek wyznaczenia ma:

15.1.1. organ lub podmiot publiczny

15.1.2. główna działalność polega na regularnym i systematycznym monitorowaniu osób na dużą skalę

15.1.3. główna działalność polega na przetwarzania danych wrażliwych na dużą skalę

15.1.4. jeżeli wymaga tego prawo UE lub prawo państwa członkowskiego.

15.2. W innych przypadkach administrator lub podmiot przetwarzający może wyznaczyć IOD (DPO).

15.3. Kto może być IOD:

- osoba, która ma kwalifikacje zawodowe, wiedzę fachową nt. prawa i praktyk w dziedzinie ochrony danych osobowych;
- może to być odpowiednia osoba z personelu administratora, który obok swojej pracy wykonuje obowiązki IOD, o ile jest to możliwe do pogodzenia i nie powoduje konfliktu interesów, możliwy outsourcing funkcji IOD, może być jeden dla grupy przedsiębiorców, opracowanie procedury wyboru i działania IOD
- podlega bezpośrednio najwyższemu kierownictwu, zakaz otrzymywania instrukcji dot. wykonywania zadań.

16. Rejestrowanie czynności przetwarzania

Do tej pory w ustawie o ochronie danych osobowych funkcjonował obowiązek rejestrowania zbiorów danych osobowych. RODO znosi ten obowiązek, ale wprowadza obowiązek administratora danych prowadzenia wewnętrznego rejestru czynności przetwarzania danych osobowych, jednak tylko w odniesieniu do niektórych przedsiębiorstw.
Rejestr ma formę pisemną, w tym formę elektroniczną.
Obowiązek prowadzenia rejestru nałożony został na przedsiębiorców zatrudniających więcej niż 250 osób. Zatrudniający mniej niż 250 osób mają obowiązek jeśli, przetwarzanie, którego dokonują może powodować ryzyko naruszenia praw i wolności

osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje dane wrażliwe i inne szczególne dane.
W rejestrze należy umieścić informacje dot. danych administratora, IOD, celów przetwarzania, opis kategorii osób, których dane dotyczą, kategorie odbiorców danych, przekazania danych do państwa trzeciego, planowane terminy usunięcia danych, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

17. **Zgłaszanie naruszeń do organu nadzorczego i zawiadomienia podmiotu**

Nowy powszechny obowiązek administratora danych zgłaszania naruszeń :
1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je GIODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego GIODO po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
Zawiadomienie nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

18. Kodeksy postępowania i mechanizmy certyfikacji

Nowe rozwiązania. Stosowanie zatwierdzonych kodeksów postępowania i zatwierdzonych mechanizmów certyfikacji ma ułatwić administratorom wdrożenie zasad ochrony danych osobowych ukształtowanych przez RODO. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.
Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.
Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie RODO.
Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych

mających świadczyć o zgodności z niniejszym rozporządzeniem_operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Certyfikacja jest dobrowolna.

19. Umowy o powierzeniu przetwarzania danych

Administrator może powierzyć przetwarzanie danych osobowych tylko takiemu podmiotowi przetwarzającemu, który zapewni wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie było zgodne z RODO i chroniło prawa osób, których dane dotyczą.

Podmiot przetwarzający przetwarza dane na podstawie umowy.

20. Bezpieczeństwo danych

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

1. pseudonimizację i szyfrowanie danych osobowych;
2. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
3. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
4. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Wywiązywanie się z powyższych obowiązków można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

21. Sankcje

Nowy mechanizm nakładania kar pieniężnych. Kary mają być skuteczne, proporcjonalne i odstraszające.

W zależności od kategorii naruszenia wysokość kar pieniężnych przedstawia się następująco:

I. do 10.000.000 EUR a w przypadku przedsiębiorstw do 2 proc. jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa w przypadku naruszenia obowiązków administratora i podmiotu przetwarzającego w postaci m.in.:

- niezgodnego z prawem przetwarzania danych osobowych dziecka w wieku poniżej 16 lat;
- niezastosowanie privacy by design i privacy by default;

- niezgodne z prawem współadministrowanie danymi;
- niezgodne z prawem przetwarzanie danych przez podmiot przetwarzający;
- brak upoważnień do przetwarzania danych;
- naruszenie obowiązku rejestrowania czynności przetwarzania;
- naruszenie obowiązków zgłaszania naruszeń ochrony danych;
- brak zastosowania privacy impact assessment;
- naruszenie obowiązków w zakresie wyznaczenia IOD.

Sankcje
II. do 20.000.000 EUR a w przypadku przedsiębiorstw do 4 proc. jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa za naruszenie:

- podstawowych zasad przetwarzania, w tym warunków zgody;
- praw osób, których dane dotyczą;
- przepisów dot. przekazywania danych do państw trzecich;
- nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.

Pytania i odpowiedzi

1. Od czego zacząć, jaki powinien być plan przygotowań do wdrożenia RODO?

Należyte przygotowanie wymaga znajomości nowych obowiązków, uzyskanie odpowiedniej wiedzy o rozporządzeniu.
W skrócie proces ten może przybrać następujące etapy:

a) weryfikacja dotychczasowych zasobów i ich lokalizacja, tzn. gdzie są zgromadzone dane osobowe i gdzie następuje ich przetwarzanie;
b) ocena ryzyk w sferach przetwarzania danych osobowych w przedsiębiorstwie;
c) zapewnienie środków kontroli dostępu;
d) zdefiniowanie procedur przetwarzania danych, np. poprzez aktualizację polityk bezpieczeństwa;
e) posiadanie środków technicznych;
f) ustalenie procesów obsługujących wykrywanie i reagowanie na incydenty bezpieczeństwa.

2. Dlaczego tak ważne jest prawidłowe przygotowanie procesu pozyskiwania zgody?

Z uwagi na zasadę rozliczalności, gdyż w każdym momencie administrator danych powinien móc wykazać w trakcie kontroli przeprowadzanej przez organ nadzoru, że przetwarzane przez niego dane osobowe są przetwarzane zgodnie z prawem, a najczęściej tą podstawą jest właśnie zgoda podmiotu, którego dane dotyczą. Ponadto ważnym bodźcem są wysokie sankcje, które grożą administratorom za naruszenia przepisów rozporządzenia, w tym za przetwarzanie danych bez podstawy prawnej.

3. Czy wdrożenie wymagań RODO wiąże się z dużymi kosztami?

Każdy przedsiębiorca powinien podejść do sprawy swoich wdrożenia RODO indywidualnie, gdyż koszty mogą być różne w zależności od tego jaki stopień ochrony danych osobowych został wprowadzony w przedsiębiorstwie dotychczas i ile trzeba zrobić, żeby spełnić wymagania RODO, kiedy rozporządzenie wejdzie w życie. Wprowadzenie niektórych rozwiązań (zwłaszcza technicznych i informatycznych) będzie musiało wiązać się z poniesieniem wydatków. Dlatego warto szczegółowo zaplanować harmonogram wdrożenia tak, aby rozłożyć kwestię kosztów w czasie.

4. Kto powinien przeprowadzić badanie oceny skutków/ryzyka dla ochrony danych DPIA i jak je przeprowadzić?

Jest wiele podmiotów które zajmują się takimi badaniami. Ważne, aby byli to kompetentni ludzie w swojej branży. Nieodzowna jest jednak podczas takiego badania współpraca całego przedsiębiorstwa począwszy od zarządu po szeregowych pracowników, gdyż to oni najlepiej znają procesy przetwarzania danych osobowych w przedsiębiorstwie. Nie należy zapominać również o innych bardzo ważnych podmiotach takich jak: project managerach, Inspektorze Ochrony Danych (DPO), ludziach od bezpieczeństwa informacji itd.

Takie badanie to studium konkretnego przypadku. Często jest procesem bardzo skomplikowanym, wymagającym złożonej wiedzy technologicznej, która może wykraczać poza kompetencje DPO w danej organizacji. Wymagana jest zarówno wiedza informatyczna jak i prawnicza.

5. Czy wymaganiom RODO muszą poddać się wszyscy przedsiębiorcy?

W pierwszej kolejności należy odnieść się do definicji zawartych w RODO – w szczególności – czym są dane osobowe i ich przetwarzanie. Z uwagi na szerokie definicje, teoretycznie wszyscy będą musieli przestrzegać przepisów RODO, gdyż praktycznie każdy przedsiębiorca przetwarza dane osobowe, bo ma kontrahentów, klientów czy pracowników, którzy są osobami fizycznymi. Z uwagi na zakres terytorialny - RODO obowiązywać będzie podmioty z Unii Europejskiej, jak również spoza Unii, kiedy wystąpią przesłanki wskazane w RODO.