BARTA LITWIŃSKI
KANCELARIA
RADCÓW PRAWNYCH
I ADWOKATÓW
SPÓŁKA PARTNERSKA

Nowe prawo ochrony danych osobowych

adw. dr Paweł Litwiński

Rozporządzenie ogólne

- Najdłuższy proces legislacyjny w historii Unii Europejskiej;
- Największy lobbing sektora prywatnego;
- Jeden z aktów prawa wtórnego UE o najszerszym zakresie zastosowania;

Rozporządzenie ogólne

- **2010 r. –** Komunikat Komisji Europejskiej w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej;
- **06.07.2011 r.** – Rezolucja Parlamentu w sprawie całościowego podejścia do kwestii ochrony danych osobowych;
- **25.01.2012 r.** – Wniosek ustawodawczy Komisji Europejskiej dotyczący rozporządzenia o ochronie danych osobowych;
- **12.03.2014 r.** - projekt zmian do rozporządzenia został przyjęty w pierwszym czytaniu przez Parlament Europejski zdecydowaną większością głosów (za projektem opowiedziało się **621** parlamentarzystów);
- **11.06.2015 r.** - Rada UE przyjęła tzw. ogólne podejście w sprawie w sprawie projektu rozporządzenia ogólnego;
- **14.04.2016 r.** – Parlament na posiedzeniu plenarnym przyjął ogólne rozporządzenie;
- **04.05.2016 r.** – Rozporządzenie zostało opublikowane w Dzienniku Urzędowym UE L 119;
- **25.05.2016** r. – Rozporządzenie weszło w życie;
- **25.05.2018 r. – Rozporządzenie zaczyna być bezpośrednio stosowane**

Trzy główne założenia unijnej reformy ochrony danych

- Stworzenie uniwersalnych ram prawnych zapewniających skuteczną ochronę danych osobowych mimo stałego rozwoju nowych technologii (chmura obliczeniowa, profilowanie, rozwój aplikacji mobilnych itp.);
- Zapewnienie ochrony danych osobowych na każdym etapie projektowania rozwiązania;
- Wprowadzenie efektywnych mechanizmów współpracy w sprawach ochrony danych osobowych;

Opinie WP29

- 13 grudnia 2016 r. – pierwsze opinie dotyczące ogólnego rozporządzenia;
  - Przewodnik dla inspektorów ochrony danych osobowych;
  - Przestrzeganie zasady rozliczalności przetwarzania danych osobowych;
- Niewiążąca ale w praktyce respektowalna treść opinii;
- Problem losu prawnego opinii po 25 maja 2018 r;

Na co jeszcze czekamy?

- Działania legislacyjne Komisji Europejskiej
- Działalność opiniodawcza Grupy Roboczej art. 29
- Działalność ustawodawcza państw członkowskich
- Działania organów nadzorczych państw członkowskich (GIODO)

Rozporządzenie ogólne

- Komisja Europejska uprawniona jest do wydawania aktów wykonawczych oraz aktów delegowanych które uzupełniają regulację unijną.
- Uprawnienie Komisji Europejskiej aktywizuje się z chwilą rozpoczęcia stosowania rozporządzenia tj. od 25 maja 2018 r.
- Z deklaracji wydawanych dotychczas przez Komisję Europejską wynika, że wyda ona akty wyłącznie na podstawie art. 43 RODO tj. dotyczących mechanizmów certyfikacji oraz znaków jakości i oznaczeń.
- Z deklaracji wydanych dotychczas przez Komisję Europejską wynika, że nie będzie ona podejmowała działań legislacyjnych w obszarach objętych wykładnią Grupy Roboczej art. 29.

Rozporządzenie ogólne

- Uregulowanie **danej kwestii w RODO wyłącza możliwość jej przyjęcia przez krajowe ustawodawstwo państw członkowskich chyba, że przepisy ogólnego rozporządzenia powyższe przewidują.** W takim przypadku państwa członkowskie mogą uregulować daną kwestię w zakresie, w jakim nie wyłącza to ani nie utrudnia stosowania przepisów ogólnego rozporządzenia. **W RODO mamy około 60 takich przepisów.**

Przykład:

Art. 8 wprowadza warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego wskazując, że państwa mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat.

Art. 6 ust. 2. Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów niniejszego rozporządzenia w odniesieniu do spełniania technicznych warunków przetwarzania danych osobowych.

Organy ochrony danych

- Wzmocnienie organów nadzorczych;
- Gwarancje niezależności organów nadzorczych;
- Większy zakres uprawnień i obowiązków;
- Autonomia proceduralna państw członkowskich UE

Rozporządzenie to akt prawny który ma obowiązywać przez kilkadziesiąt lat. Jakie instrumenty zastosowano, by jego postanowienia były zawsze aktualne?

Uelastycznienie przepisów i obowiązków

Art. 25

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.

Art. 32

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**.

Art. 8 ust. 2

W takich przypadkach administrator, **uwzględniając dostępną technologię,** podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

Motyw 84

Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi **środkami z punktu widzenia dostępnej technologii** i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.

Reforma ochrony danych

- Rozporządzenie opiera się na założeniu, że ma pozostać ono aktualne niezależnie od stałego rozwoju nowych technologii;
- Brak jest konkretnych technicznych wymogów ochrony danych – o tym jakie środki powinny zastać przyjęte decydować powinny okoliczności stanu faktycznego;
- Administrator zobowiązany jest uwzględnić najdalej idące możliwe, uznane za stabilne, skuteczne i powszechnie dostępne techniczne i organizacyjne środki ochrony danych;
- W każdym przypadku GIODO oceni, czy poziom ochrony danych jest wystarczający;

Aby rozporządzenie było możliwie najbardziej uniwersalne i unifikowało wszystkie porządku prawne państw członkowskich, wprowadzono do niego znaczną liczbę klauzul generalnych;

Przykłady:

Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny (motyw 26).

Klauzule generalne

Aby rozporządzenie było możliwie najbardziej uniwersalne i unifikowało wszystkie porządku prawne państw członkowskich, wprowadzono do niego znaczną liczbę klauzul generalnych;

Przykłady:

Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny (motyw 26).

Rezygnacja z zasady adekwatności przetwarzania danych na rzecz zasady minimalizacji.

Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. **Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych** (motyw 78).

Art. 5 ust. 1 pkt c. Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („**minimalizacja danych**").

Zmiana modelu odpowiedzialności

Co do zasady **podmiotem odpowiedzialnym** za wykonywanie obowiązków ochrony danych osobowych **jest wyłącznie administrator (podmiot przetwarzający).** To administrator (podmiot przetwarzający) decyduje więc o tym które z jego zadań wykonywał będzie w praktyce inspektor ochrony danych (obecny administrator bezpieczeństwa informacji).

Zasada rozliczalności

Administrator jest odpowiedzialny za przestrzeganie przepisów o ochronie danych osobowych i **musi być w stanie wykazać ich przestrzeganie („rozliczalność").**

Najważniejsze nowe instrumenty prawne ochrony danych osobowych

Ocena skutków

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, **administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.** Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę (art. 35).

Przyjmując prawo, które ma być dla organu lub podmiotu publicznego podstawą do wykonywania zadań i ma regulować konkretną operację przetwarzania lub konkretny zestaw operacji, **państwa członkowskie mogą uznać, że przed takimi czynnościami przetwarzania należy koniecznie przeprowadzić taką ocenę** (motyw 93).

Najważniejsze nowe instrumenty prawne ochrony danych osobowych

Kary finansowe

Każde państwo członkowskie wprowadza kary administracyjne w wysokości nie wyższej niż 10 000 000 lub 20 000 000 EURO lub 2 lub 4 % rocznego światowego obrotu.

Państwa członkowskie powinny określić, czy i w jakim zakresie administracyjnym karom pieniężnym powinny podlegać organy publiczne (motyw 150).

Bez uszczerbku dla uprawnień naprawczych organu nadzorczego, o których mowa w ust. 58 ust. 2, każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim (art. 83 ust. 7).

Najważniejsze nowe instrumenty prawne ochrony danych osobowych

Wyznaczenie inspektora ochrony danych (były ABI)

Administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych zawsze gdy przetwarzania dokonują organ lub podmiot publiczny z wyjątków sprawowania przez nie wymiaru sprawiedliwości, gdy dane przetwarzane są dużą skalę i dotyczą szczególnych kategorii danych osobowych bądź działania oparte są na monitorowaniu osób.

Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych

Najważniejsze nowe instrumenty prawne ochrony danych osobowych

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona 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 wynikające z przetwarzania, administrator 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.

Co już możemy zrobić?

Obowiązek notyfikacji naruszeń

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 organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Możliwe obecne działania

Wdrożenie formalnej procedury informowania administratora danych oraz administratora bezpieczeństwa informacji o wszelkich naruszeniach zasad ochrony danych.

Co już możemy zrobić?

Kary za naruszenie zasad ochrony danych osobowych

Naruszenia przepisów dotyczących ochrony danych osobowych podlegają administracyjnej karze pieniężnej w wysokości **do 20 000 000 EUR**, a w przypadku przedsiębiorstwa – w wysokości do **4 %** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego

Co już możemy zrobić?

Privacy by design

Zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża się 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 rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Privacy by default

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Co już możemy zrobić?

Wprowadzenie już teraz obowiązku dołączania do wszelkiej dokumentacji projektowej oceny wpływu rozwiązania, na ochronę danych osobowych.

Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych.

Co już możemy zrobić?

Budowanie świadomości pracowników o nowych zasadach ochrony danych osobowych poprzez organizowanie szkoleń oraz warsztatów.

Dziękuję za uwagę

adw. dr Paweł Litwiński

litwinski@bartalitwinski.pl