Magdalena Jacolik
Mgr Prawa Europejskiego
Aliant Krzyżowska
Międzynarodowa Kancelaria Prawna
e-mail: aliant@aliantlaw.pl

B. Regulatory Framework in EU.

Rozporządzenie ParlamentuEuropejskiego iRady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych wzwiązku zprzetwarzaniem danych osobowych iwsprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie oochronie danych)

Zgodnie z art. 99 tytułowego rozporządzenia, postanowienia w nim zawarte mają zastosowanie od 25 maja 2018 roku. Warto wspomnieć, iż zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej „rozporządzenie ma zasięg ogólny. Wiąże w całości i jest bezpośrednio stosowane we wszystkich Państwach Członkowskich". Zatem niniejsze rozporządzenie nie wymaga dodatkowej implementacji aktami prawa krajowego, **postanowienia w nim zawarte, wiążą od chwili jego wejścia w życie.** Cechą rozporządzeń jest również ich bezpośredni skutek, co oznacza, że zarówno państwa członkowskie, jak i jednostki mogą bezpośrednio powoływać się na regulacje zawarte w rozporządzeniu.

Rozporządzenie RODO dotyczy „ochrony osób fizycznych w związku w przetwarzaniem danych osobowych i (…) swobodnego przepływu takich danych". Do fundamentalnych kwestii w nim zawartych należą:

- Art. 4 pkt. 1) niniejszego aktu prawnego, który definiuje **pojęcie „danych osobowych"**, zgodnie z którym „"dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); 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 bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej" oraz art. 4 pkt. 2) który **definiuje pojęcie**

„przetwarzania”, w myśl którego „”przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie”.

- Warty podkreślenia pkt. (15) według którego ochrona dotycząca przetwarzania danych osobowych nie powinna być uzależniona od form służących przetwarzaniu danych. Również art. 2 pkt.2 d) zgodnie z którym, regulacje zawarte w rozporządzeniu nie powinny dotyczyć przetwarzania danych osobowych przez odpowiednie organy w celu np. ochrony bezpieczeństwa publicznego, narodowego, a także na mocy pkt. (26) - przetwarzania informacji o charakterze anonimowym w intencjach statycznych czy naukowych.
- Kwestia terytorialnego stosowania omawianego aktu prawnego, który jest określony w art. 3, zgodnie z którym „1. niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku **z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii,** niezależnie od tego, czy przetwarzanie odbywa się w Unii”, a także „ 2. (…) **do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii,** jeżeli czynności przetwarzania wiążą się z:
    a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
    b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii”.

  Również „3. (…) **do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego**”.
- Niekwestionowany fakt, iż wszelkie dane osobowe, które ulegają przetwarzaniu, muszą być przetwarzane **rzetelnie** – zgodnie z pkt. (60) rozporządzenia tzn., że administrator powinien poinformować osobę, której takie dane dotyczą o kontekście, celach oraz okolicznościach przetwarzanych informacji oraz **mieścić się w granicach**

prawa – zgodnie z pkt. (40) tzn., na gruncie zgody wyrażonej przez osobę, której to dane dotyczą bądź w oparciu o inną podstawę prawną.

Natomiast wszelkie wprowadzające w błąd informacje, a także te które są nieprawidłowe z punktu widzenia celów przetwarzania, winny zostać sprostowane lub usunięte, zgodnie z art. 5 pkt. 1 d) omawianego rozporządzenia.

- Art. 9 w myśl którego, co do zasady niedozwolone jest przetwarzania danych osobowych szczególnej kategorii, tzn. dotyczących m.in. orientacji seksualnej, poglądów politycznych, religijnych, pochodzenia rasowego/etnicznego, bądź też zdrowia.
- Art. 11 pkt. 1 w świetle którego, w sytuacji, gdy dane informacje nie wystarczają do identyfikacji danej osoby, administrator nie jest zobowiązany do uzyskania uzupełniających informacji potrzebnych do identyfikacji takiej osoby fizycznej, jeżeli cele przetwarzania do tego nie zobowiązują.
- Pkt. (50) rozporządzenia, według którego „przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, powinno być dozwolone wyłącznie w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały pierwotnie zebrane (…)", a „(…) jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w których dane osobowe zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o tym innym celu oraz dostarczyć jej innych niezbędnych informacji (…)" – art. 14 pkt. 4.
- Art. 15 rozporządzenia na gruncie którego, osoba fizyczna winna mieć dostęp do informacji, które jej dotyczą. Administrator, który otrzymuje dane od tej osoby, powinien ją poinformować m.in. o celach przetwarzania takich danych, o odbiorcach, a także o prawie do roszczenia względem administratora usunięcia, sprostowanie bądź złożenia sprzeciwu (w dowolnym momencie).
- Art. 17 który ustanawia **"Prawo do bycia zapomnianym"**, tzn., że osoba fizyczna, której dane dotyczą, może rościć sobie prawo względem administratora do usunięcia takich danych, przy zaistnieniu wyznaczonych okoliczności, tj.:
    a) „dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    b) osoba, której dane dotyczą, cofnęła zgodę (…);
    c) osoba, której dane dotyczą, wnosi sprzeciw (…);
    d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1. (…)".

- Pkt. 71 rozporządzenia, zgodnie z którym „(…) **podejmowanie decyzji na podstawie (…) profilowania**, powinno być dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, w tym do celów monitorowania i zapobiegania – zgodnie z uregulowaniami, standardami i zaleceniami instytucji Unii lub krajowych podmiotów nadzorujących – oszustwom i uchylaniu się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora, lub gdy jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, lub gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę (…)".
- Ograniczenia w prawie do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, są zasadne jeśli stoją na straży m.in.: bezpieczeństwa publicznego, zdrowia publicznego, bezpieczeństwa narodowego, czy zapobieganiu przestępczości (art. 23).
- Administrator oraz podmiot przetwarzający wdrażają właściwe metody, służące zapewnieniu bezpieczeństwa w przetwarzaniu danych (art. 32).
- Art. 33 który dotyczy **powinności zgłaszania naruszeń ochrony danych osobowych**,

  w myśl którego, „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 organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. 2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. (…)".
- Art. 35, na podstawie którego „1. (…) jeżeli dany rodzaj przetwarzania (…) 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 (…)".

- Art. 37 pkt. 1 na gruncie którego administrator oraz podmiot przetwarzający wyznaczają **Inspektora Ochrony Danych (IOD)**, w sytuacji kiedy:
    a) „przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
    b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
    c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10. (…)".

  Warto podkreślić, zasadą wyznaczania Inspektora Ochrony Danych są kwalifikacje zawodowe. Zgodnie z art. 38 pkt. 3, „(…) bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego". W świetle art. 39 pkt. 1, do jego zadań należą m.in.:
    a) „(…) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) (…)
    d) współpraca z organem nadzorczym; (…)".
- Komisja, Europejska Rada Ochrony Danych, Państwa Członkowskie oraz organy nadzorcze nakłaniają do opracowywania Kodeksów postępowania, które na celu mają wspierać odpowiednie stosowanie omawianego rozporządzenia (art. 40).

- Art. 42, według którego Komisja, Europejska Rada Ochrony Danych, Państwa Członkowskie oraz organy nadzorcze nakłaniają „(…) 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 (…)".
- W każdym państwie członkowskim jest niezależny organ nadzorczy (minimum jeden), który czuwa m.in. nad właściwą ochroną danych osób fizycznych w związku z ich przetwarzaniem oraz odpowiednim stosowaniem omawianego rozporządzenia (art. 51).
- Art. 68 rozporządzenia, na podstawie którego został ustanowiony organ Unii Europejskiej, jakim jest **Europejska Rada Ochrony Danych (EROD)**, która posiada osobowość prawną. „(…) 3. Do Europejskiej Rady Ochrony Danych należą: przewodniczący jednego organu nadzorczego każdego państwa członkowskiego oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele (…) 5. Komisja ma prawo do udziału w działaniach i posiedzeniach Europejskiej Rady Ochrony Danych, nie ma jednak prawa głosowania (…)". Tworzą ją również przewodniczący, który ją reprezentuje oraz dwóch wiceprzewodniczących (art. 73).

  Europejskiej Rady Ochrony Danych m.in. rozstrzyga spory (art. 65), monitoruje oraz wspiera odpowiednie stosowanie omawianego rozporządzenia, wydaje zalecenia, wytyczne i opinie, udziela Komisji Europejskiej opinii dotyczącej np. certyfikacji, posiada również funkcję doradczą (art. 70). Cechuje się niezależnością (art. 69).
- Rozporządzenie RODO na mocy art. 83 przewiduje **kary finansowe** za naruszenie zawartych w nim przepisów. Kary te, mają być proporcjonalne ale przede wszystkim skuteczne oraz odstraszające.

Bibliografia:

I Akty prawne:

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 (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE z 04.05.2016r., L119, s. 1.
2. Traktat o funkcjonowaniu Unii Europejskiej, Dz. Urz. z 2012 r., C 326, s. 1.
3. P. Justyńska, *Zasady prawa Unii Europejskiej,* [w:] J. Galster (red.) *Podstawy prawa Unii Europejskiej z uwzględnieniem Traktatu z Lizbony,* Toruń 2010, s. 251 i n, 326 i n.
4. http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM%3Al14522, stan na dzień 02.01.2018r.