Uniwersytet Wrocławski

ADMINISTRATOR, PODMIOT PRZETWARZAJĄCY I INSPEKTOR OCHRONY DANYCH

WYKŁAD 4
STUDIA STACJONARNE PRAWA

lukasz.gozdziaszek@uwr.edu.pl
www.gozdziaszek.pl
www.facebook.com/gozdziaszek
BLOG: www.prawo-internetu.pl

dr Łukasz Goździaszek

ADMINISTRATOR

oznacza **osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot**, który samodzielnie lub wspólnie z innymi **ustala cele i sposoby przetwarzania** danych osobowych.

Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

PODMIOT PRZETWARZAJĄCY (tzw. procesor)

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, **który przetwarza dane osobowe w imieniu administratora**.

ODBIORCA

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, **któremu ujawnia** się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

STRONA TRZECIA

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, **które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać** dane osobowe.

GŁÓWNA JEDNOSTKA ORGANIZACYJNA

oznacza:
a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego **centralna administracja w Unii**, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, **w której zapadają takie decyzje**;
b) jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego **centralna administracja w Unii** lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się **główne czynności przetwarzania** w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia.

PRZEDSTAWICIEL

oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, **która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający** na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia.

PRZEDSIĘBIORCA

oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące **regularną działalność** gospodarczą.

GRUPA PRZEDSIĘBIORSTW

oznacza przedsiębiorstwo **sprawujące kontrolę** oraz przedsiębiorstwa przez nie **kontrolowane**.

Art. 24 RODO. Obowiązki administratora

1. Uwzględniając **charakter, zakres, kontekst i cele** przetwarzania oraz **ryzyko** naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, **administrator wdraża odpowiednie środki techniczne i organizacyjne**, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i **aby móc to wykazać**. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują **wdrożenie** przez administratora odpowiednich **polityk ochrony danych**.
3. Stosowanie zatwierdzonych **kodeksów postępowania**, o których mowa wart. 40, lub zatwierdzonego mechanizmu **certyfikacji**, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Podejście oparte na ryzyku (risk-based approach)

Art. 25 RODO. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. 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 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.
2. 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.
3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu **certyfikacji** określonego w art. 42.

Zasada ochrony danych w fazie projektowania (privacy by design)

Zasada domyślnej ochrony danych (privacy by default)

Art. 26 RODO. Współadministratorzy

1. Jeżeli **co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania**, są oni współadministratorami. W drodze **wspólnych uzgodnień** współadministratorzy w **przejrzysty** sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

2. Uzgodnienia, o których mowa w ust. 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. **Zasadnicza treść uzgodnień** jest udostępniana podmiotom, których dane dotyczą.

3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.

Art. 28 RODO. Podmiot przetwarzający

1. Jeżeli przetwarzanie ma być **dokonywane w imieniu administratora**, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające **gwarancje** wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. (…)

Art. 30 ust. 1 RODO. Rejestrowanie czynności przetwarzania

1. Każdy **administrator** oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą **rejestr czynności przetwarzania** danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:
a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.
(…)

Rejestr czynności przetwarzania danych osobowych

Art. 30 ust. 2 RODO. Rejestrowanie czynności przetwarzania

2. Każdy **podmiot przetwarzający** oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą **rejestr wszystkich kategorii czynności przetwarzania** dokonywanych w imieniu administratora, zawierający następujące informacje:
a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.
(…)

Rejestr wszystkich kategorii czynności przetwarzania

Art. 30 ust. 3-5 RODO. Rejestrowanie czynności przetwarzania

3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną.
4. Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego.
5. Obowiązki, o których mowa w ust. 1 i 2, **nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych**, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

Art. 32 RODO. Bezpieczeństwo przetwarzania

1. 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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić **stopień bezpieczeństwa odpowiadający temu ryzyku**, (…)

Art. 33 RODO. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

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. (…)
5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

Art. 34 RODO. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. 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. (…)

Art. 35 RODO. Ocena skutków dla ochrony danych

1. 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. (…)

Oceny skutków dla ochrony danych
(data protection impact assessment - DPIA, privacy impact assessment - PIA)

Art. 37 RODO. Wyznaczenie inspektora ochrony danych

1. Administrator i podmiot przetwarzający wyznaczają **inspektora ochrony danych, zawsze gdy**:
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, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10. (…)

Art. 39 RODO. Zadania inspektora ochrony danych

1. Inspektor ochrony danych ma następujące **zadania**:
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) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Art. 40 RODO. Kodeksy postępowania

1. 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.
2. Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie niniejszego rozporządzenia, (…)
11. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie zatwierdzone kodeksy podstępowania, zmiany i rozszerzenia i udostępnia je opinii publicznej za pomocą odpowiednich środków.

Art. 42 RODO. Certyfikacja

1. 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. (…)
3. Certyfikacja jest dobrowolna, a proces jej uzyskania musi być przejrzysty. (…)

dr Łukasz Goździaszek

Adiunkt w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

Adwokat

Specjalizuje się w Prawie Internetu i Technologii

Autor książek:
„Prawo blogosfery”,
„Cywilnoprawne granice swobody wypowiedzi w Internecie”,
„Internetowy system pozasądowego rozstrzygania sporów konsumenckich w Unii Europejskiej. Komentarz”,
„Identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym Unii Europejskiej. Komentarz”
i „Elektroniczne postępowanie upominawcze”