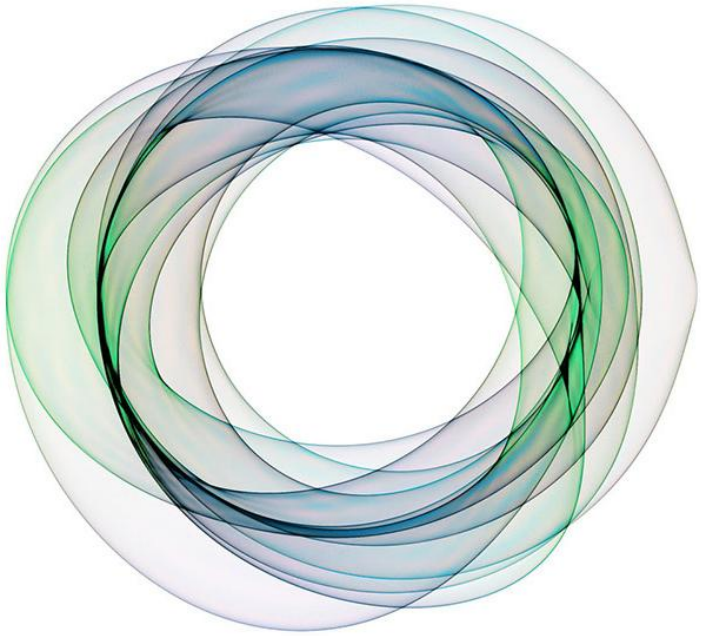
ALLEN & OVERY



Nowe unijne rozporządzenie w sprawie ochrony danych osobowych

8 czerwca 2016

Prace nad nowym rozporządzeniem

Terminarz prac nad rozporządzeniem

Styczeń 2012	Opublikowanie pierwszej propozycji Rozporządzenia
Maj 2012 – Marzec 2013	Prace w Parlamencie Europejskim. Konsultacje PE z parlamentami Państw Członkowskich
II połowa 2013	Nieformalne negocjacje między PE a Komisją
Marzec 2014	Głosowanie w PE
Maj 2014 – Czerwiec 2015	Prace w Komisji
Czerwiec 2015	Początek rozmów trójstronnych Komisji i PE z Radą UE
Grudzień 2015	Zakończenie prac w ramach rozmów trójstronnych
14 kwietnia 2016	Przyjęcie wiążącego tekstu Rozporządzenia przez PE
4 maja 2016	Publikacja tekstu w Dzienniku Urzędowym UE
24 maja 2018	Wejście Rozporządzenia w życie

Jurysdykcja

Jurysdykcja

Zakres terytorialny Rozporządzenia:

- **Podmioty z siedzibą w Unii Europejskiej**
- **Podmioty z siedzibą w państwach trzecich?**

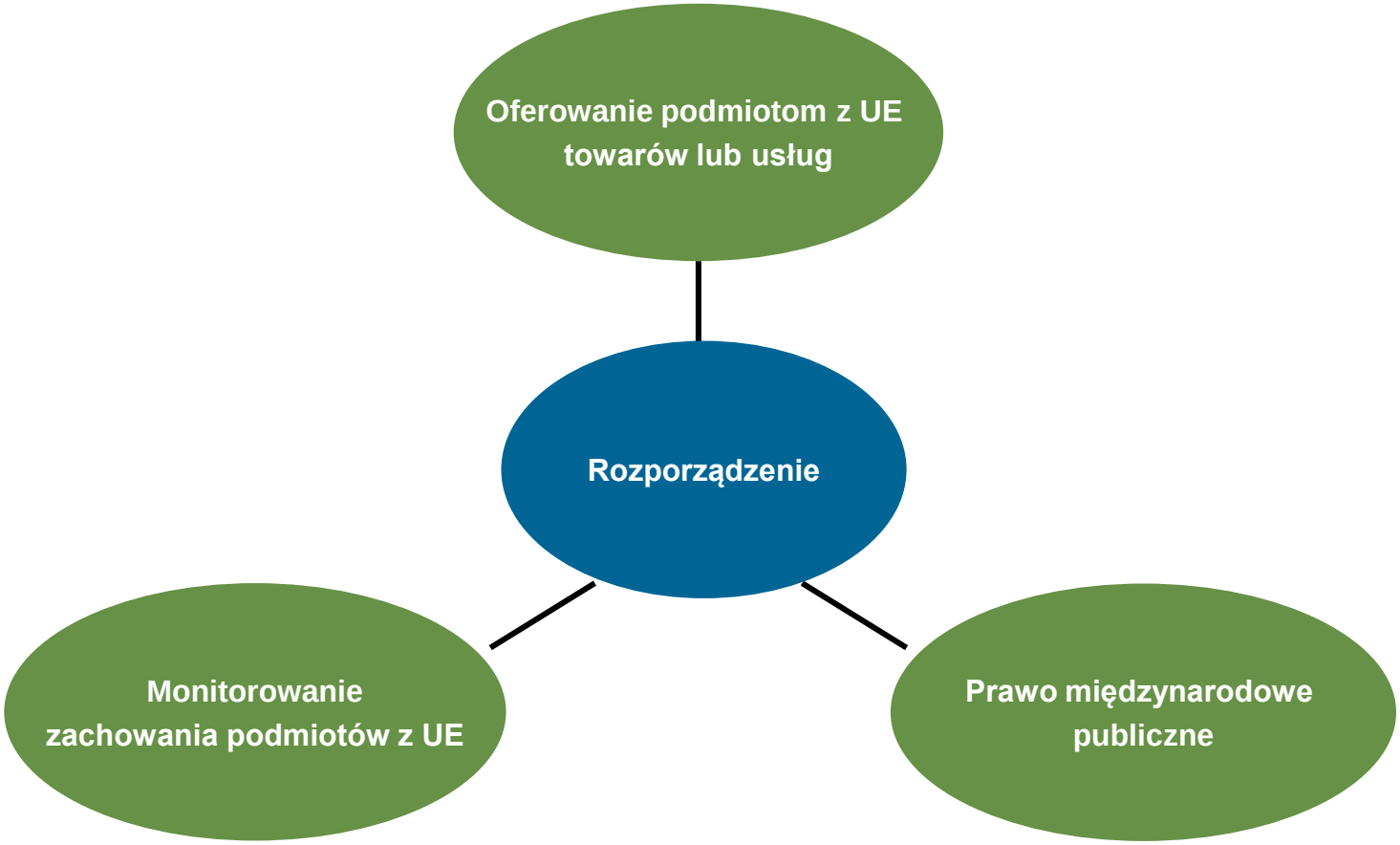
Tzw. „one-stop-shop”, czyli punkt kompleksowej obsługi

Współpraca organów:

- **Wzajemna pomoc**
- **Wspólne operacje**
- **Obowiązek współpracy**

Mechanizm zgodności (Europejska Rada Ochrony Danych Osobowych)

Podmioty z państw trzecich



Nowe zasady przetwarzania danych

Warunki przetwarzania danych

Nowe zasady przetwarzania: transparentność i rozliczalność

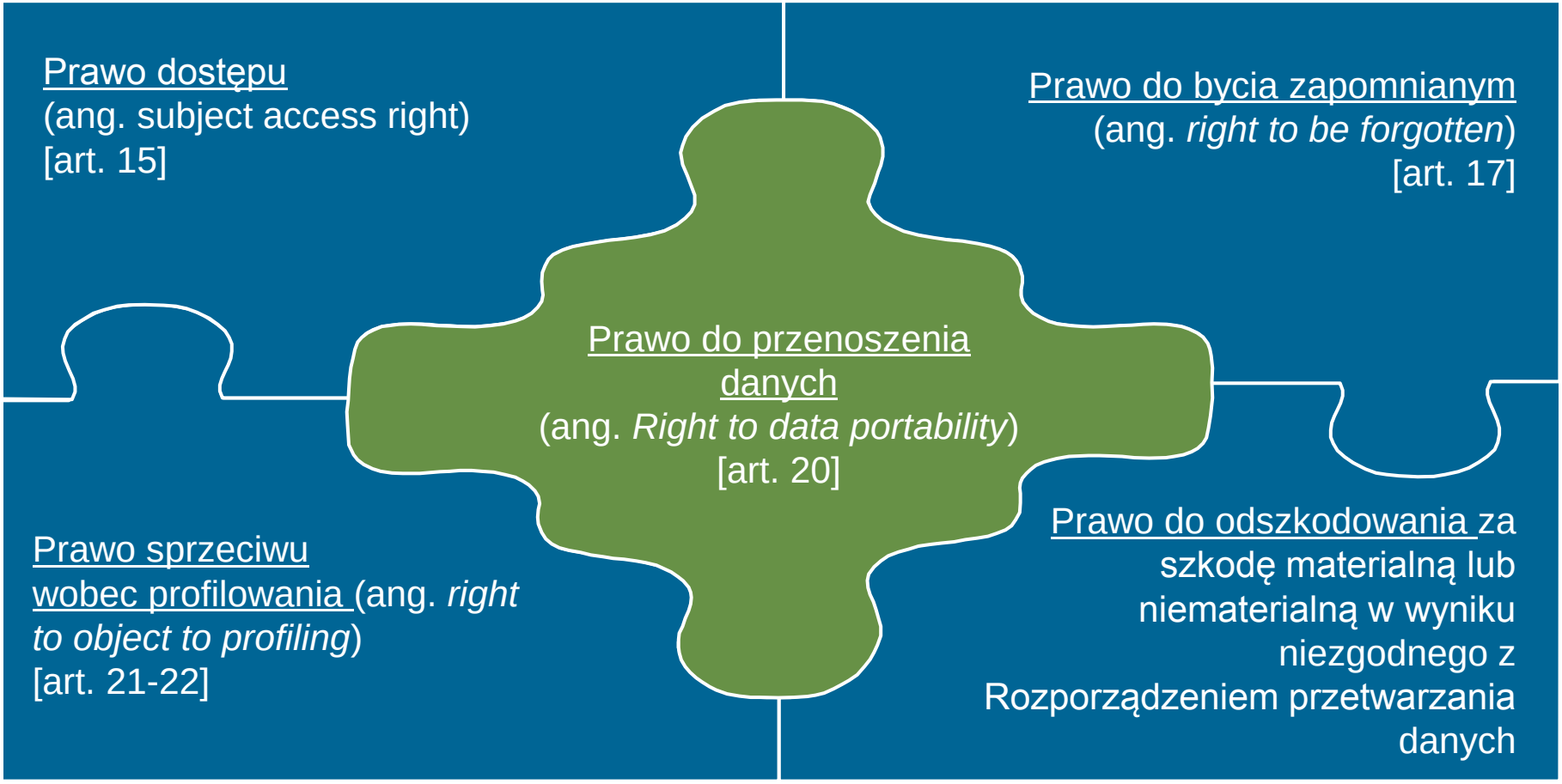
Kryteria jakie musi spełniać zgoda na przetwarzanie danych osobowych:

- Tzw. *informed consent*
- Tzw. *purpose limited consent*

Nowe wytyczne co do obowiązku informacyjnego administratora danych [podstawa: art. 12 - 14]

Tzw. *European Data Protection Seal*

Prawa podmiotu danych



Nowe obowiązki administratora danych

Nowe obowiązki administratora danych

Wprowadzony zostanie obowiązek:

- Informowania o naruszeniu danych
- Ochrony prywatności w fazie projektowania
- Ocen skutków prowadzonych operacji przetwarzania danych osobowych
- Zatrudnienia inspektora ochrony danych osobowych

Zniesiony zostanie obowiązek:

- Rejestracji zbiorów danych (zastąpi go obowiązek rejestrowania i przechowywania dokumentacji operacji przetwarzania)

Informowanie o naruszeniu [art. 33 i 34]

Kto jest adresatem powiadomienia?

- Organ nadzorczy [art. 33]
- Podmiot danych [art. 34]

W jakim terminie informujemy?

Kiedy informujemy podmiot danych?

Jakie obowiązki ma przetwarzający?

Co powinno zawierać powiadomienie?

- Charakter naruszenia,
- Kategorię i liczbę osób, których dotyczy naruszenie,
- Kategorię i liczbę rekordów danych, których dotyczy naruszenie
- Opis możliwych konsekwencji i środków zaradczych przedsięwziętych lub proponowanych

Privacy by design and by default [art. 25]

Zasada „ochrony prywatności w fazie projektowania”

• Obowiązek wdrożenia technologicznych i organizacyjnych środków należnych dla ochrony praw podmiotów danych już na etapie projektowania

Zasada „domyślnej ochrony prywatności”

• Obowiązek projektowania procesów tak, aby potrzeba wykorzystania danych osobowych była z założenia (domyślnie) jak najmniejsza

Data Protection Impact Assessment [art. 35]

Ocena skutków operacji jakie wywierają dokonywane operacje przetwarzania danych (DPIA) pod kątem istnienia zagrożeń dla praw z zakresu ochrony danych osobowych

Otwarty katalog operacji, które wymagają przeprowadzenia oceny skutków

Operacje przetwarzania danych wskazane wprost jako wymagające oceny skutków to:

- Czynności z zakresu profilowania (tzn. przetwarzania danych w celu "odgadnięcia" określonych cech danego podmiotu danych, np. wieku lub płci)
- Systemy monitoringu wideo w przestrzeni publicznej
- Przetwarzanie na dużą skalę danych sensytywnych

Wyjątki (art. 35 ust. 10)

Inspektor ochrony danych [art. 37-39]

- Obowiązek czy dobrowolność wyznaczenia inspektora danych osobowych (*Data Protection Officer*, DPO)?
- Kiedy należy powołać własnego DPO?
- Jakie wymagania musi spełniać DPO?
- Jakie zadania będzie miał DPO?

Obowiązek rejestrowania czynności przetwarzania [art. 30]

Brak obowiązku rejestracji zbioru danych - zastępuje go obowiązek prowadzenia rejestru czynności przetwarzania i przechowywania dokumentacji dotyczącej dokonywanych operacji przetwarzania

Kto ma dostęp do dokumentacji?

Dokumentacja powinna zawierać:

- Informacje nt. administratora danych oraz DPO, a także wszystkich osób będących odbiorcami danych
- Informacje nt. celu dokonywanych procesów przetworzenia danych osobowych
- Informacje nt. kategorii danych osobowych i podmiotów danych objętych przetwarzaniem
- Informacje nt. okresów przechowywania danych

Wyłączenia?

Nowe obowiązki procesora

Powierzenie przetwarzania danych

Nowe obowiązki procesorów [art. 28 w zw. z art. 3(1)]

- Prowadzenie rejestru czynności przetwarzania danych
- Współpraca z organem nadzorczym
- Zawiadomienie o naruszeniu bezpieczeństwa
- Wdrożenie odpowiednich środków technicznych i organizacyjnych
- Wyznaczenie DPO

Nowe wymagania odnośnie umowy o powierzenie przetwarzania [podstawa: art. 28-29]

- Prawo właściwe
- Forma
- *Essentialia negotii*
- Dalsze powierzenie
- Odpowiedzialność
- Gwarancje bezpieczeństwa
- Klauzule modelowe

Transfer danych do państw trzecich

Transfer danych (rozdział V Rozporządzenia)

Decyzja Komisji	Odpowiednie gwarancje	Odstępstwa w sytuacjach szczególnych
• Odpowiedni poziom ochrony • Istnienie i skuteczne działanie organu nadzorczego • Międzynarodowe zobowiązania zaciągnięte przez państwo trzecie • Mechanizm okresowego przeglądu	• BCR • Model clauses • Mechanizm certyfikacji • Prawnie egzekwowalny instrument	• Zgoda podmiotu danych • Wykonanie umowy • Interes publiczny • Dochodzenie roszczeń • Przekazanie z rejestru • Ważny uzasadniony interes administratora

Organ nadzorczy

Nowe uprawnienia GIODO [art. 57-58]

Dochodzeniowe	Korekcyjne	Autoryzacyjne i doradcze
• Nakaz dostarczenia informacji • Dochodzenia • Dostęp do informacji • Dostęp do pomieszczeń • Weryfikacja certyfikacji	• Ostrzeżenia • Upomnienia • Nakazy • Zakazy • Grzywny administracyjne	• Porady • Opinie • Zezwolenia • Akredytacje

Grzywny administracyjne – wysokość (I)

Wysokość	Rodzaj naruszenia
maks. **10 000 000 EUR** lub w przypadku przedsiębiorstwa **2% całkowitego rocznego obrotu światowego** z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa)	- Zgoda dziecka - Naruszenie zasady „*privacy by default*" i „*privacy by design*" - Naruszenie zasad współadministrowania danymi - Brak przedstawiciela w UE - Naruszenie zasad powierzania przetwarzania danych - Naruszenie obowiązków rejestrowania czynności przetwarzania - Zaniechanie wdrożenia odpowiednich środków w zakresie bezpieczeństwa przetwarzania lub brak możliwości wykazania przestrzegania przepisów Rozporządzenia - Zaniechanie ostrzeżenia lub powiadomienia organu nadzorczego lub podmiotu danych o naruszeniu ochrony danych lub nie zgłoszenie takiego naruszenia w zakreślonym terminie - Zaniechanie przeprowadzenia oceny skutków pod kątem ochrony danych (tzw. DPIA) - Nieprzeprowadzenie oceny DPIA - Brak DPI

Grzywny administracyjne – wysokość (II)

Wysokość	Rodzaj naruszenia
maks. **20 000 000 EUR** lub w przypadku przedsiębiorstwa **4% całkowitego rocznego obrotu światowego** z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa)	- Naruszenie podstawowych zasad przetwarzania, w tym warunków zgody - Niedopełnienie obowiązków informacyjnych względem podmiotu danych - Niezapewnienie podmiotowi danych dostępu do jego danych - Przetwarzanie danych osobowych po sprzeciwie - Naruszenie prawa do poprawiania danych - Naruszenie prawa do bycia zapomnianym - Naruszenie prawa do przenoszenia danych - Naruszenie prawa do ograniczenia przetwarzania - Naruszenie przepisów o przetwarzaniu danych w sytuacjach szczególnych - Naruszenie zasad przekazywania danych do państw trzecich - Naruszenie nakazu, ograniczenia lub zawieszenia przetwarzania lub przepływu danych orzeczonego przez organ nadzorczy - Niezapewnienie dostępu do danych na żądanie organu nadzorczego - Nieprzestrzeganie nakazów wydanych przez organ nadzorczy

Kary

- Państwo członkowskie ma możliwość ustalenia kar za naruszenie Rozporządzenia
- Państwo członkowskie ma możliwość ustalenia systemu wykonania kar
- Kary muszą być skuteczne, proporcjonalne i odstraszające

Zakończenie

Dane kontaktowe

Prof. Krystyna Szczepanowska-Kozłowska
Partner

Tel +48 22 820 61 76
Fax +48 22 820 61 99
krystyna.szczepanowska@allenovery.com

Justyna Ostrowska
Adwokat / Starszy Prawnik

Tel +48 22 820 61 72
Fax + 48 22 820 61 99
justyna.ostrowska@allenovery.com

Pytania?

Niniejsze slajdy stanowią jedynie prezentację. Informacje zawarte w tych slajdach nie stanowią porady i nie należy ich wykorzystywać jako podstawy do udzielenia definitywnej porady bez sprawdzenia źródeł.

Allen & Overy oznacza Allen & Overy LLP oraz/lub jej jednostki powiązane. Termin partner używany jest w odniesieniu do członka Allen & Overy lub pracownika lub konsultanta o równoważnym statusie i kwalifikacjach lub osoby o równoważnym statusie w jednej z jednostek powiązanych Allen & Overy LLP.