#RODO2018

podstawowe szkolenie
z zakresu ochrony danych osobowych

Bartosz Armknecht
- ADVISER Armknecht i Partnerzy, Radcowie Prawni sp.k.
→www.adviser.gdynia.pl
- Biuro Usług Szkoleniowych Maria Hertel

Plan szkolenia

- **Panel – I: Informacje podstawowe o RODO**

  Czym jest RODO?

- **Panel – II: Prawa i obowiązki wynikające z RODO**

  Co robić a czego nie robić żeby być RODOzgodnym?

- **Panel – III: Studium przypadku RODO?**

  Jakie są najczęściej popełniane błędy przy zbieraniu i przetwarzaniu danych osobowych?

Czym jest RODO?

RODO (ang. GDPR) - Ogólne **R**ozporządzenie o **O**chronie **D**anych **O**sobowych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r.) jest nowym aktem prawnym regulującym ochronę prywatności na terytorium UE. Celem RODO jest zapewnienie i zwiększenie kontroli osób fizycznych nad swoimi własnymi danymi osobowymi. W tym celu RODO nakłada nowe obowiązki na podmioty zbierające (gromadzące), przechowujące i przetwarzające dane osobowe.

- RODO weszło w życie w dniu 24 maja 2016 r., jednakże państwa członkowskie UE do dnia 24 maja 2018 r. mają czas na wprowadzenie regulacji ustawowych realizujących postanowienia RODO. **Po dniu 25 maja 2018 r. RODO** będzie stosowana bezpośrednio w tych krajach członkowskich, które nie wprowadziły regulacji ustawowych w tym zakresie. Tym samych w zakresie regulowanym RODO nie będzie stosowana **UODO** - ustawa z dnia 29 sierpnia 1997 r. o ochronie osobowych (Dz.U. z 2016 r., poz. 922 – t.j.).

***Deadline* RODOzgodności to dzień 25 maja 2018 r.**

Rozporządzenie UE, czyli ?

- Obok dyrektywy, decyzji zalecenia i opinii stanowi wtóre źródło prawa UE,
- ma zasięg ogólny, swoją treścią wiąże w całości i jest bezpośrednio stosowane (skuteczne) we krajach UE,
- nie wymaga implementacji do krajowego porządku prawnego → *sui genesis* stanowi źródło praw i obowiązków,
- jest bezpośrednio skuteczne ze skutkiem natychmiastowym i przyznaje podmiotom indywidualnym prawa, które sądy krajowe mają obowiązek chronić.

Co to są dane osobowe według RODO?

- Zgodnie z art. 4 ust. 1 **RODO** – *Dane osobowe, to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.*
- Zgodnie z art. 6 ust. 1 **UODO** – *Dane osobowe, to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.*

RODO i UODO nie definiują **pojęcia osoby zidentyfikowanej** (brak definicji legalnej).

Zgodnie z przyjętą praktyką osobą zidentyfikowaną jest osoba, co do której nie trzeba przeprowadzać identyfikacji, ponieważ jej tożsamość jest już znana - administrator danych osobowych ma możliwość powiązania posiadanej informacji z konkretną osobą, bez konieczności podejmowania dalszych działań.

Pojęcie osoby możliwej do zidentyfikowania

- **art. 6 ust. 2 UODO** – *osobą możliwą do zidentyfikowania jest osoba, której tożsamości można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na: numer identyfikacyjny, kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, kulturowe lub społeczne.*

art. 4 ust. 1 Rodo – *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
– jeden lub kilka szczególnych czynników określających: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

motyw 30 preambuły – *osobom fizycznym mogą zostać przypisane **identyfikatory internetowe** – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawieniem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i identyfikowania tych osób.*

RODO czyli co nowego?

- Prawo do prywatności
- Kontrole i powiadomienia (zawiadomienia)
- Transparentność gromadzenia, przechowywania i przetwarzania danych osobowych
- Faktyczne szkolenia, audyty systemów IT, umów => samokontrola

Prawo do prywatności według RODO

Celem RODO jest zwiększenie ochrony osób fizycznych w zakresie zbierania, przechowania i przetwarzania ich danych osobowych, w szczególności poprzez:

- zapewnienie dostępu do własnych danych osobowych,
- umożliwienie usunięcia własnych danych osobowych,
- Udostępnienie własnych danych osobowych w celu ich edycji (poprawa błędów, wprowadzenie zmian),
- zapewnienie prawa do odmowy przetwarzania własnych danych osobowych.

Kontrole i powiadomienia (zawiadomienia)

W celu zapewnienia uprawnień osób fizycznych RODO nakłada nowe obowiązki na podmioty zbierające (gromadzące), przechowujące i przetwarzające dane osobowe, takie jak:

- ochrona danych osobowych za pomocą odpowiednich (adekwatnych) środków bezpieczeństwa,
- niezwłoczne powiadomienie odpowiednich władz o naruszeniach danych osobowych,
- uzyskanie zgody na gromadzenie, przechowywanie i przetwarzanie danych osobowych,
- prowadzenie rejestru historii przetwarzania danych osobowych.

Transparentność gromadzenia, przechowywania i przetwarzania danych osobowych

Obowiązki, które zostały przez RODO nałożone na podmioty zbierające (gromadzące), przechowujące i przetwarzające dane osobowe, muszą zostać wewnętrznie uregulowane i spełniać następujące kryteria:

- wprost określony cel zbierania danych osobowych,
- wskazanie i uzasadnienie celu, sposobu i czasu przechowywania danych osobowych,
- wskazanie zasad przechowywania, edycji i usuwania danych osobowych.

Faktyczne szkolenia, audyty systemów IT, umów => samokontrola

Zgodnie z RODO, podmioty zbierające (gromadzące), przechowujące i przetwarzające dane osobowe mają obowiązek:

- zapoznać pracowników z **najlepszymi praktykami bezpieczeństwa danych osobowych** (faktyczne szkolenia),
- przeprowadzać audyty i aktualizować zasady dotyczące przetwarzania danych osobowych,
- powołać inspektora ochrony danych, jeśli to konieczne,
- zapewnić zgodność umów z dostawcami usług wchodzącymi w zakres czynności związanymi z danymi osobowymi z RODO.

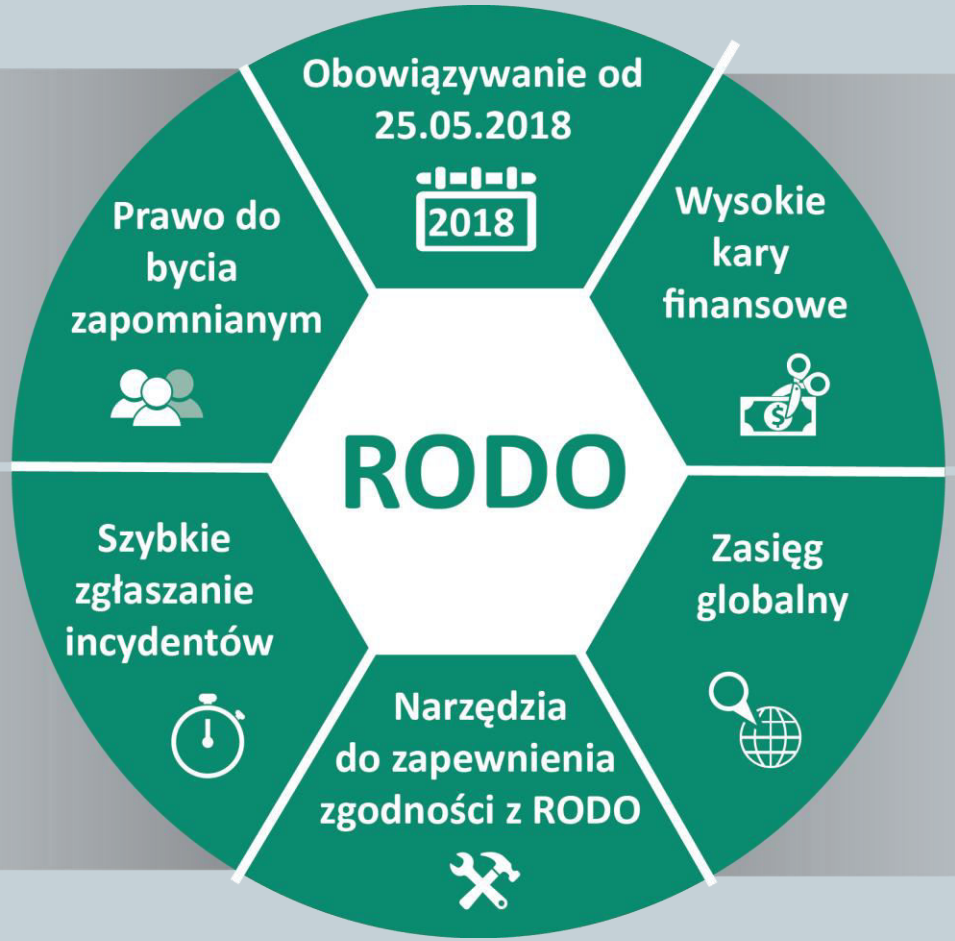
Podstawowe porównanie regulacji ochrony danych osobowych

UODO	RODO
• krajowe regulacje, niejednolite w UE, • wymóg rejestracji zbioru danych osobowych w GIODO, • katalog danych wrażliwych, • zgłaszanie zbiorów danych *post factum*, • *right to be forgotten*.	• regulacja UE – ujednolicenie zasad, • wymóg prowadzenia rejestru czynności przetwarzania danych, • zgłoszenie naruszenia ochrony danych nie później niż 72h od naruszenia, • rozszerzenie katalogu o dane genetyczne i biometryczne, • *privacy by design*, • prawo do przenoszenia danych, edycji, sprzeciwu i roszczenia odszkodowawcze.

RODO – najważniejsze założenia – wstępne podsumowanie

PRAWO PODMIOTU DANYCH
- rozbudowane prawo do informacji, prawo do bycia zapomnianym

ZGŁASZANIE INCYDENTÓW
- do 72 godzin, wysokie kary za brak zgłoszenia



KARY FINANSOWE
- do 20 mln euro lub 4% wartości rocznego obrotu

ZASIĘG GLOBALNY
- wszędzie tam, gdzie przetwarzane są dane osobowe obywateli EU

Źródło infografiki: http://adaptiverodo.pl/

Sankcje wynikające z braku RODOzgodności (I)

Sankcja: 10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa za:

- Art. 25 RODO: naruszenie zasad ochrony danych osobowych w fazie projektowania (*privacy by design*) oraz domyślna ochrona danych (*privacy by default*),
- Art. 29 RODO: przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego,
- Art. 30 RODO: rejestrowanie czynności przetwarzania,
- Art. 31 RODO: współpraca z organem nadzorczym,
- Art. 32 RODO: bezpieczeństwo przetwarzania.

Sankcje wynikające z braku RODOzgodności (II)

Sankcja: 20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa za:

- Art. 5 RODO: naruszenie zasad dotyczących przetwarzania danych osobowych,
- Art. 7 RODO: naruszenie warunków wyrażenia zgody na przetwarzanie danych,
- Art. 15 RODO: naruszenie wykonania prawa dostępu przysługującego osobie, której dane dotyczą,
- Art. 16 RODO: naruszenie wykonania prawa do sprostowania i usuwania danych.

Kogo pytać, czy przetwarzamy dane osobowe?

Administratora Bezpieczeństwa Informacji (ABI) do 25 maja 2018r., a od tego dnia Inspektora Ochrony Danych (IOD), w uproszczeniu dane osobowe, to dane:

- pracowników,
- podmiotów ujawnionych w Centralnej Ewidencji i Informacji Działalności Gospodarczej,
- otrzymywane od tzw. „Procesorów” (podmioty przekazujące dane osobowe).

Wyznaczenie IOD – art. 37 RODO

- Administrator i podmiot przetwarzający wyznaczają IOD, zawsze gdy:
  - przetwarzania dokonują **organ lub podmiot publiczny,** z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.
  - 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 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.
- Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.
- 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 IOD.
- IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.
- IOD może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
- Administrator lub podmiot przetwarzający publikują dane kontaktowe IOD i zawiadamiają o nich organ nadzorczy.

Status IOD - art. 38 RODO

- Administrator oraz podmiot przetwarzający zapewniają, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
- Administrator oraz podmiot przetwarzający wspierają IOD w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
- Administrator oraz podmiot przetwarzający zapewniają, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. IOD bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
- Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
- IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.
- IOD może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Zadania IOD - art. 39 RODO

- 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;
- 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;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- współpraca z organem nadzorczym;
- 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.

Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Obowiązki pracownika wynikające z RODO

- zapoznanie się i przestrzeganie ustanowionych procedur wewnętrznych, jak np.:
  - fizyczne i techniczne zabezpieczenie miejsca pracy,
  - **zgłaszanie dokonanie naruszenia ochrony danych osobowych,**
- stosowanie się do poleceń i zaleceń IOD,
- aktywne uczestnictwo w szkoleniach.

Incydenty ochrony danych osobowych (I)

- **Korespondencja:**
  - niewłaściwy adresat,
  - niewłaściwa treść,
  - ujawnienie zbyt dużej ilości danych.

- **Nieuprawnione udostępnienie danych, poprzez dostęp:**
  - elektroniczny,
  - fizyczny,
  - telefoniczny.

Incydenty ochrony danych osobowych (II)

- **Utrata nośników** - zagubienie albo kradzież nośnika: telefonu, laptopa pamięci przenośnej, na których nie tylko przechowywane są dane ale również za pomocą których można uzyskać dostęp do np. służbowej skrzynki e-mail, czy systemu zarządzania (CRM). Dotyczy to również takich nośników danych jak zapisane kartki, czy segregatory z aktami.

- Nieodpowiednie techniki usuwania danych:
  - zapisanych fizycznie np. w postaci notatek (brak użycia niszczarki),
  - zapisanych elektronicznie.

Incydenty ochrony danych osobowych (III)

- brak odebrania pisemnej zgody od osoby której dane osobowe będą przetwarzane,
- brak pouczenia tej osoby o fakcie przetwarzania jej danych osobowych,
- niewskazanie tej osobie podstawy prawnej obowiązku/ potrzeby przetwarzania jej danych osobowych i nie pouczenia jej o jej prawach w tym zakresie,
- nieudostępnienie tej osobie dokumentu wewnętrznego stanowiącego podstawę sposobu, zakresu przetwarzania jej danych osobowych.

Podsumowanie, RODO to:

- bezpośrednia odpowiedzialność przetwarzającego dane osobowe,
- zgłaszanie naruszeń – incydentów przy przetwarzaniu danych osobowych,
- nowe i rozszerzone prawa osób, których dane są przetwarzane,
- ograniczenie profilowania,
- wyznaczenie IOD,
- obowiązki dokumentacyjne i klasyfikacyjne,
- zgoda na przetwarzanie i obowiązki informacyjne,
- transfer danych osobowych poza UE.

Podstawowa literatura

- M.Kawecki, ***Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych***, Wolters Kluwer, Warszawa 2017,
- E.Bielak-Jomaa, D.Lubasz (red.), ***RODO - Ogólne Rozporządzenie o Ochronie Danych – komentarz***, Wolters Kluwer, Warszawa 2018,
- M.Kawecki, T.Osiej (red.), ***Ogólne Rozporządzenie o Ochronie Danych Osobowych. Wybrane zagadnienia***, CH Beck, Warszawa 2017.
- **RODO Informator, Warszawa**
  www.gov.pl/cyfryzacja/rodo-informator
- **Opinie i wytyczne grupy roboczej RODO**
  www.giodo.pl

Dziękuję za uwagę

W przypadku pytań zapraszam do kontaktu:
bartek@adviser.gdynia.pl

ARMKNECHT I PARTNERZY
ADVISER | RADCOWIE PRAWNI | ROK ZAŁ. 1989