Nazywam się Arkadiusz Szczudło

Jestem adwokatem, przedsiębiorcą i twórcą.

Robię prawo i biznes.

arkadiusz@creativa-legal.com

arkadiuszszczudlo.pl

Arkadiusz Szczudło

a_szczudlo

Arkadiusz Szczudło

RODO dla branży IT

Plan prezentacji

1. Kiedy stosujemy RODO
2. Ważne definicje
3. Powierzenie przetwarzania danych
4. Upoważnienia
5. Czym jest przetwarzanie danych
6. Zasady przetwarzania
7. Prawa podmiotów danych
8. Rejestr czynności przetwarzania
9. Zgłaszanie naruszeń i kary

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

Zasięg terytorialny RODO

- jednostka organizacyjna w UE
- oferowanie towarów i usług w UE
- monitorowanie zachowania osób w UE

Wyłączenie stosowania RODO m.in.:

- działalność nieobjęta zakresem prawa Unii (np. bezpieczeństwo narodowe)

- zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych lub wykonywanie kar, ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom - przez właściwe organy

- czynności o czysto osobistym lub domowym charakterze

Czynności o czysto osobistym lub domowym charakterze

- niezarobkowe
- czynności osób fizycznych
- związane z życiem prywatnym lub rodzinnym
- nienaruszające sfery osobistej innych osób

Czynności o czysto osobistym lub domowym charakterze

- spisy danych kontaktowych znajomych
- lista urodzin bliskich osób
- tabela uczestników na wyjazd
- domowy monitoring

Zacznijmy od kilku definicji...

Dane osobowe - 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 bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

Dane szczególnej kategorii, czyli dane wrażliwe

Zabrania się przetwarzania danych osobowych ujawniających:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne, przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych
- oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Możecie to robić, gdy m.in.:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach.

Przetwarzanie danych osobowych

- zbieranie
- utrwalanie
- organizowanie
- porządkowanie
- przechowywanie
- adaptowanie lub modyfikowanie
- pobieranie
- przeglądanie
- wykorzystywanie
- ujawnianie poprzez przesłanie

Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który ustala cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Personel – pracownicy firmy bez względu na podstawę prawną na jakiej pracują – umowa o pracę, zlecenia, dzieło, samozatrudniony.

Kim Ty jesteś?

Obowiązki administratora w przypadku powierzenia przetwarzania danych osobowych

- zawarcie umowy powierzenia
- sprawdzenie renomy podmiotu przetwarzającego

- udokumentowanie poleceń

Co w umowie powierzenia?

- przedmiot przetwarzania
- czas trwania przetwarzania
- charakter przetwarzania
- cel przetwarzania
- rodzaj danych
- kategorie podmiotów danych
- obowiązki i prawa administratora
- obowiązki przetwarzającego

Co w umowie powierzenia?

Co jeszcze (można) zawrzeć?

- kary umowne
- zasady przeprowadzania audytów i ich skutki (np. wiążące zalecenia)
- współpraca w przypadku kontroli

Obowiązki administratora w przypadku powierzenia przetwarzania danych osobowych

Co jeszcze (można) zawrzeć?

- kary umowne
- zasady przeprowadzania audytów i ich skutki (np. wiążące zalecenia)
- współpraca w przypadku kontroli

Zamiast umów
stosuj upoważnienia

Elementy upoważnienia

- Kto upoważnia
- Imię, nazwisko
- Stanowisko
- Zakres zbiorów danych
- Jakie czynności

Dodatkowo:

- Regulamin pracowniczy
- Zapoznanie się z dokumentacją wewnętrzną
- Zobowiązanie do poufności

Przejdźmy dalej...

Zasady przetwarzania danych

- zgodność z prawem, rzetelność, przejrzystość
- ograniczenie celu
- minimalizacja danych
- prawidłowość
- ograniczenie przechowywania
- integralność i poufność
- rozliczalność

Prawa podmiotów danych

- Prawo do informacji i przejrzystej komunikacji
- Prawo dostępu do danych
- Prawo do sprostowania i usunięcia danych
- Prawo do ograniczenia przetwarzania
- Prawo do przeniesienia danych
- Prawo do sprzeciwu
- Prawo do niepodlegania zautomatyzowanemu przetwarzaniu danych osobowych

Otrzymujesz bonus ☺️

Brak prawa do usunięcia danych

Jeśli przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji
- do wywiązania się z prawnego obowiązku na mocy prawa Unii lub prawa państwa członkowskiego, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych
- do ustalenia, dochodzenia lub obrony roszczeń

Rejestr (*kategorii) czynności przetwarzania

Rejestr czynności przetwarzania

- dane administratora, współadministratorów, przedstawiciela administratora, inspektora ochrony danych;
- cele przetwarzania;
- kategorie danych osobowych oraz podmiotów danych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- planowane terminy usunięcia poszczególnych kategorii danych;
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Rejestr kategorii czynności przetwarzania

Do pobrania z oficjalnej
strony internetowej PUODO

Najważniejsze,
unikaj ryzyka

Obowiązek zgłoszenia naruszenia ochrony danych organowi nadzorczemu

- niezwłocznie, max. 72 h po stwierdzeniu naruszenia

- ewentualnie: wyjaśnienie opóźnienia

- wyjątek: brak ryzyka naruszenia praw lub wolności osób fizycznych

Obowiązek zawiadomienia o naruszeniu osoby, której dane dotyczą

- bez zbędnej zwłoki.

Wyjątki:

- wdrożone były środki uniemożliwiające odczyt danych osobom nieuprawnionym
- zastosowano środki eliminujące wysokie ryzyko naruszenia praw lub wolności podmiotu danych
- niewspółmiernie duży wysiłek*

Co w zgłoszeniu?

- charakter naruszenia ochrony danych osobowych
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego,
- możliwe konsekwencje naruszenia
- środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu/zminimalizowania jego skutków

- **Jasnym i prostym językiem!**

Kary administracyjne za naruszenie ochrony danych osobowych

Do 10 milionów euro lub 2% rocznego światowego obrotu przedsiębiorstwa za poprzedni rok obrotowy:

- ✔ naruszenia obowiązków ciążących na administratorze i podmiocie przetwarzającym, np. wdrożenia odpowiednich środków dla ochrony danych osobowych lub powołania inspektora ochrony danych

Do 20 milionów euro lub 4% rocznego światowego obrotu przedsiębiorstwa za poprzedni rok obrotowy:

- ✔ naruszenia podstawowych zasad przetwarzania danych, np. uzyskiwania zgody na przetwarzanie, praw osób, których te dane dotyczą (np. prawa dostępu, sprostowania i usunięcia danych)

Co jest brane pod uwagę przy nakładaniu kar?

- charakter, waga i czas trwania naruszenia przy uwzględnieniu charakteru, zakres lub cel danego przetwarzania, liczba poszkodowanych osób, rozmiar poniesionej przez nie szkody
- umyślny lub nieumyślny charakter naruszenia
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem wdrożonych środków technicznych i organizacyjnych
- wszelkie stosowne wcześniejsze naruszenia
- stopień współpracy z organem nadzorczym
- kategorie danych osobowych, których dotyczyło naruszenie
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu
- stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji

Plan prezentacji

1. Kiedy stosujemy RODO
2. Ważne definicje
3. Powierzenie przetwarzania danych
4. Upoważnienia
5. Czym jest przetwarzanie danych
6. Zasady przetwarzania
7. Prawa podmiotów danych
8. Rejestr czynności przetwarzania
9. Zgłaszanie naruszeń i kary

Koniec ☺️