RODO – Akademia Aktywnego Mieszkańca (6 X 2021)

Marek Mirosławski
Urząd Miasta Krakowa
Wydział Organizacji i Nadzoru
Zespół Inspektora Ochrony Danych

Dlaczego o tym mówimy?

- Bo żyjemy w erze informacji i musimy stosować specjalistyczne narzędzia do jej przetwarzania
- Bo informacje są cennym towarem
- Bo rozwija się przestępczość związana z informacją
- Bo w przypadku incydentu mogą być konsekwencje
- Bo chcemy ograniczyć koszty
- Bo mamy działać zgodnie z prawem
- Bo lepiej zapobiegać niż leczyć
- Bo leży to w naszym interesie
- Bo lepiej coś wiedzieć, niż nie wiedzieć nic
- Bo…

Porządek prawny w zakresie ochrony danych osobowych – Konstytucja RP

Art. 51.

- 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
- 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
- 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
- 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
- 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Porządek prawny w zakresie ochrony danych osobowych – RODO

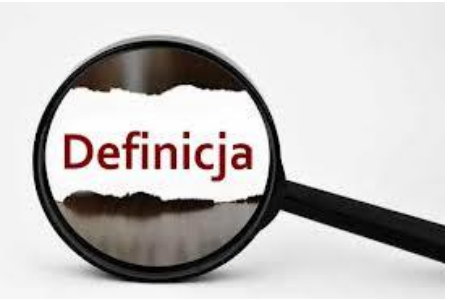
- **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)**
  (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)
- **Unijne ogólne rozporządzenie o ochronie danych; rozporządzenie 2016/679, RODO**
- Weszło w życie 24 maja 2016 r.
- Jego przepisy stosujemy od dnia 25 maja 2018 r.
- Stosujemy je wprost (bez implementacji do krajowego porządku prawnego) we wszystkich krajach członkowskich Unii Europejskiej.
- „Dyrektywa policyjna” (2016/680)
- Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125)

Sens, idea i cel RODO

- **Chroń dane najlepiej jak potrafisz. My ci nie powiemy jak, ale… bądź pewien, że jak popełnisz błąd, to konsekwencje cię nie ominą.**
- Wydanie tego rozporządzenia wpisuje się w art. 8 ust. 1 Karty praw podstawowych UE i art. 16 ust. 1 Traktatu o funkcjonowaniu UE:
  Każda osoba ma prawo do ochrony danych osobowych jej dotyczących.
- Art. 16 ust. 2 Traktatu powierza Parlamentowi Europejskiemu i Radzie określenie zasad ochrony osób fizycznych w zakresie przetwarzania danych osobowych.
- **Cel rozporządzenia: ochrona podstawowych praw i wolności osób fizycznych**
- **Celem RODO nie jest ochrona danych osobowych!**

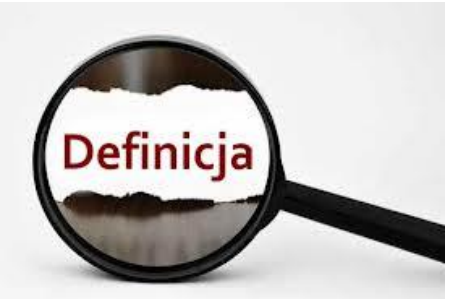
5

Pojęcia, które warto znać



- **Dane osobowe** – wszystkie te informacje, za pomocą których mogę zidentyfikować daną konkretną **osobę fizyczną** (także np. czynniki genetyczne, biometryczne)
- **Przetwarzanie danych** – każda operacja na danych (nawet ta bierna, np. przechowywanie, ale także usuwanie)

Pojęcia, które warto znać



- **Administrator** – ten, kto decyduje o **celach** i **sposobach** przetwarzania danych (z faktu lub z ustawy)

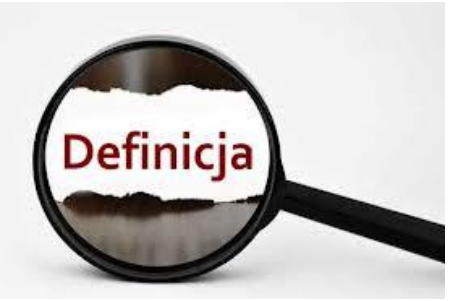
Np. Ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi

- Art. 25b. Wójt (burmistrz, prezydent miasta) jest administratorem danych, o których mowa w art. 25a ust. 1 i 2, przetwarzanych przez powołaną przez niego gminną komisję rozwiązywania problemów alkoholowych.

Np. Starosta rejestruje pojazd, ale administratorem danych w CEPiK jest Minister Cyfryzacji.

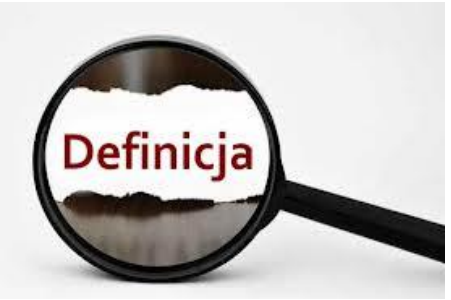
- **Odbiorca** – każdy, komu ujawnia się dane (ale nie osoba, której dane dotyczą, nie administrator i nie ten kto żąda danych, bo prowadzi postępowanie na podstawie przepisów prawa)
- **Inspektor Ochrony Danych** – ten, kto wspomaga administratora i czuwa nad przestrzeganiem przepisów RODO

Pojęcia, które warto znać



- **Cel przetwarzania danych**
- **Kategoria osób** – o jakiej grupie osób mówimy, np.: wnioskujący o wydanie dowodu osobistego, mieszkańcy biorący udział w konsultacjach społecznych, skarżący
- **Kategoria danych** – opis zakresu danych identyfikujących osobę fizyczną, np.: imię i nazwisko, numer ewidencyjny PESEL, data urodzenia, adres zamieszkania, numer telefonu, informacja o niepełnosprawności
- **Kategoria przetwarzania** – opis operacji przetwarzania, np.: 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

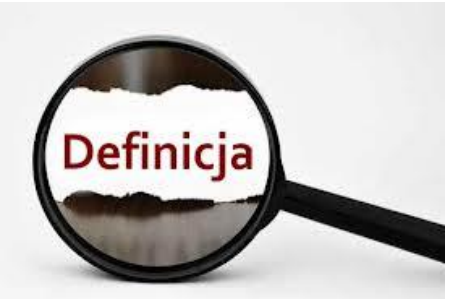
Pojęcia, które warto znać



Rodzaj danych – mamy trzy rodzaje danych!

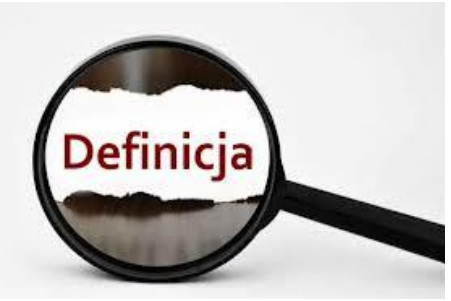
- **Dane zwykłe** (inne niż wymienione poniżej)
- **Dane szczególnych kategorii** (art. 9 RODO) – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej [art. 9 łącznie z art. 6]
- **Dane dot. wyroków skazujących i czynów zabronionych** (art. 10 RODO) – dane te dotyczą także tzw. powiązanych środków bezpieczeństwa

Pojęcia, które warto znać



- **Okres retencji danych** – czas, po upływie którego dane osobowe należy usunąć (trwale!) – ‚Planowane terminy usunięcia poszczególnych kategorii danych’
- Z reguły czas ten określa Jednolity Rzeczowy Wykaz Akt lub inne przepisy prawa.
- Może się okazać, że dane przechowujemy wieczyście i to też jest prawidłowa sytuacja (choć powinna być wyjątkiem, a nie regułą).

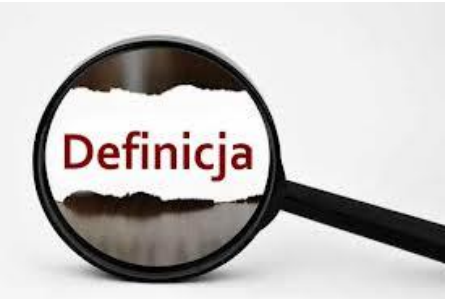
Pojęcia, które warto znać



- **Odbiorca danych** – 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.
- **Jest odbiorcą danych:**
  - Podmiot przetwarzający
  - Nowy administrator, któremu przekazuje się dane
- **Nie jest odbiorcą danych:**
  - Osoba, której dane dotyczą
  - Komórka organizacyjna UMK, która zbiera dane jako administrator (PMK)
  - Policja lub inny organ, która zadaje pytanie o osobę, prowadząc postępowanie na podstawie ustawy

Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. *(Art. 51 ust. 1 Konstytucji RP)*

Pojęcia, które warto znać



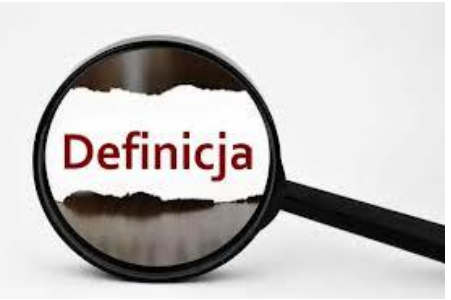
- **Strona trzecia** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż:
  - osoba, której dane dotyczą,
  - administrator,
  - podmiot przetwarzający,
  - osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej

„Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej”.

Opis technicznych i organizacyjnych środków bezpieczeństwa

Pojęcia, które warto znać



- **Profilowanie** – forma zautomatyzowanego przetwarzania danych, które polega na wykorzystaniu ich do oceny niektórych czynników osobowych osoby fizycznej, np. analizy jej preferencji, sytuacji ekonomicznej, zainteresowań, nawyków itp.

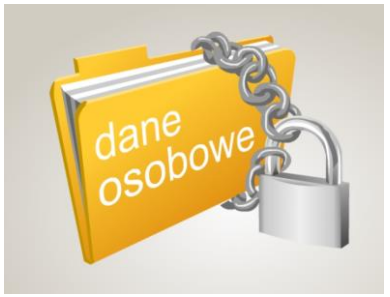
Profilowanie przy wydawaniu decyzji administracyjnych

- **Anonimizacja** – proces, w wyniku którego nie można przypisać danych informacji do konkretnej osoby w żaden sposób; jest nieodwracalny
- **Pseudonimizacja** – proces przetworzenia danych w taki sposób, by nie można ich było już przypisać konkretnej osobie, bez użycia dodatkowych informacji; jest odwracalny (np. kodowanie prac maturalnych)

Obowiązki administratora

- Wdrożenie środków technicznych i organizacyjnych, aby przetwarzanie było zgodne z RODO i trzeba móc to wykazać (art. 24)
- Uwzględnianie ochrony danych w fazie projektowania (przy określaniu sposobów przetwarzania), minimalizacja danych (art. 25 ust. 1)
- Domyślnie przetwarzamy tylko te dane, które służą realizacji celu przetwarzania – dotyczy to ilości zbieranych danych, zakresu ich przetwarzania, okresu przechowywania oraz ich dostępności (art. 25 ust. 2)

Paralela BHP i ODO



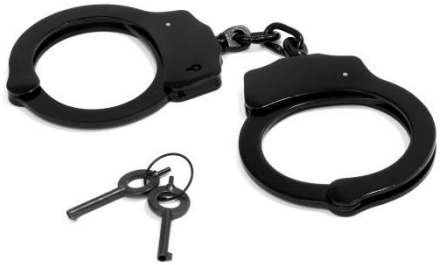
Kto odpowiada za BHP/ODO?	Pracodawca	Administrator
Kto wspomaga, szkoli, kontroluje?	Służba BHP	Inspektor Ochrony Danych

Ryzyko

Najczęstsze błędy

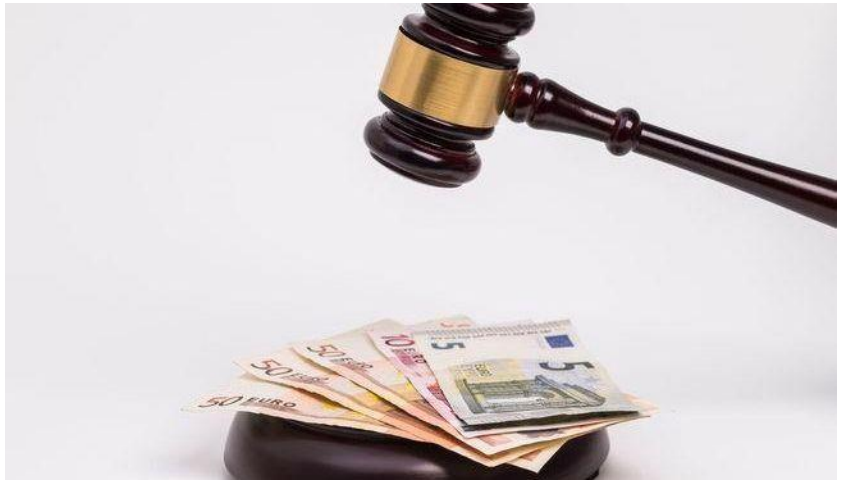
- pozostawienie dokumentów, aktywnej aplikacji bez nadzoru osoby upoważnionej
- pozostawianie kartek z loginami, hasłami, kodami w miejscu ogólnodostępnym
- rozmowa telefoniczna w miejscu publicznym, bądź w obecności osób nieuprawnionych
- pozostawienie dokumentów na ksero
- pozostawienie wydruku w ogólnodostępnej drukarce sieciowej
- otwarcie podejrzanego załącznika w poczcie elektronicznej
- nieświadomie udzielona istotna informacja osobie podającej się za personel techniczny lub serwis
- oddanie do serwisu dysku z danymi
- brak kopii bezpieczeństwa
- wyrzucanie niezniszczonych trwale kopii testowych, dodatkowych wydruków, rolek (klisz) z faksu itp. do kosza
- brak kontroli dostępu do pomieszczeń, w których przetwarza się dane

Środki ochrony prawnej



- Prawo do skargi do organu nadzorczego (art. 77)
- Prawo do sądu przeciwko organowi nadzorczemu (art. 78)
- Prawo do sądu przeciwko administratorowi lub podmiotowi przetwarzającemu (art. 79)
- Możliwość reprezentacji przez organizację społeczną (art. 80)
- Prawo do odszkodowania – odpowiedzialność na zasadzie winy (art. 82)

Administracyjne kary pieniężne (art. 83 RODO)



- W przypadku naruszenia przepisów RODO krajowy organ nadzorczy ma prawo nałożyć administracyjną karę pieniężną.
- Kary pieniężne stanowią dochód budżetu państwa.
- Inne sankcje – domena państw członkowskich (art. 84 RODO) – „skuteczne, proporcjonalne, odstraszające”
- W ustawie o ochronie danych osobowych – analogiczne kary jak do tej pory (górna granica: 2 lata / 3 lata pozbawienia wolności)

Przesłanka legalizacyjna przetwarzania – art. 6 ust. 1 RODO – wybieramy jedną!

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

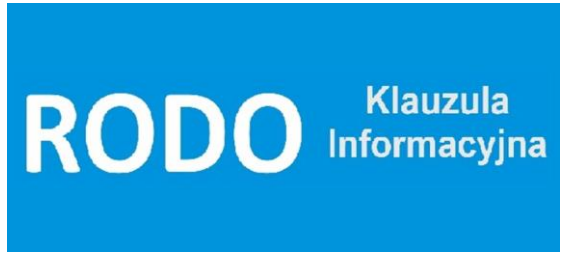
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub
w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

IPDO – Informacja o przetwarzaniu danych osobowych Obowiązek / „klauzula informacyjna” – art. 13

- Gdy zbieramy dane od osoby, której dane dotyczą
- Na temat danego administratora, celu itd. informujemy tylko jednokrotnie!
- Wzory
- Za brak podpisania informacji nie ma żadnych sankcji

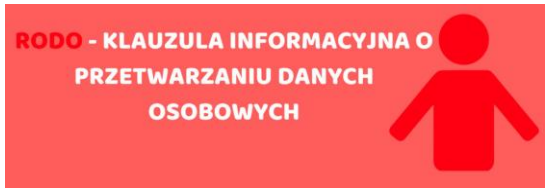


Najczęstsze błędy w IPDO

- Suchy, prawniczy, nieprzystępny język
- Brak danych kontaktowych administratora
- Niejasny, niekonkretny cel przetwarzania
- Zbyt ogólna podstawa prawna przetwarzania
- Niewłaściwy katalog praw z art. 15–22 RODO
- Informacja o prawie do sprzeciwu nie jest wyodrębniona
- Problem z określeniem odbiorców/kategorii odbiorców danych
- Problemy z określeniem okresu retencji danych
- Umieszczanie informacji wszędzie, np. w stopce e-maila
- Informacji nie należy umieszczać na piśmie procesowym (np. Kpa) ale dawać jako osobny dokument
- Możliwość warstw informacyjnych w elektronicznej klauzuli

IPDO – Informacja o przetwarzaniu danych osobowych Obowiązek / „klauzula informacyjna” – art. 14

- Gdy zbieramy dane nie od osoby, której dane dotyczą
- Na temat danego administratora, celu itd. informujemy tylko jednokrotnie!
- Jeżeli te dane mamy z powodu przepisu – nie informujemy (co wynika z art. 14 ust. 5 lit. c) RODO).
- Jeżeli dane muszą być poufne z powodu tajemnicy zawodowej – nie informujemy (co wynika z art. 14 ust. 5 lit. d) RODO).



RODO określa
prawa osoby, której dane dotyczą

- Prawo dostępu do danych (art. 15)
- Prawo do sprostowania danych (art. 16)
- Prawo do usunięcia danych (art. 17)
- Prawo do ograniczenia przetwarzania (art. 18)
- Prawo do przenoszenia danych (art. 20)
- Prawo do sprzeciwu (art. 21)
- Uprawnienia związane z profilowaniem oraz zakazem automatyzacji rozstrzygnięć indywidualnych (art. 22)

24

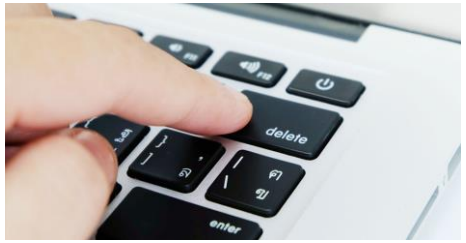
Prawo dostępu (art. 15)

- Przysługuje zawsze
- Kto przetwarza moje dane, w jakim celu, komu przekazuje, do kiedy przetwarza, jeśli nie ma moich danych ode mnie, to od kogo je ma?
  (wyjątki dot. skargi – zob. art. 74a, art. 236 § 2 Kpa; art. 179a Op)
- Prawo do uzyskania kopii danych osobowych podlegających przetwarzaniu
- Pierwsza kopia za darmo ☺

Prawo do sprostowania (art. 16)

- Przysługuje zawsze
- Obejmuje również prawo do żądania uzupełnienia niekompletnych danych.
- Jak poprawimy, to musimy poinformować wszystkich odbiorców o tym fakcie.

Prawo do usunięcia danych („do bycia zapomnianym”) (art. 17)



- Nie zawsze przysługuje!
- Jeżeli przetwarzamy na podstawie lit. c) albo lit. e), to właściwie nie przysługuje.
- Usuwamy gdy np.:

  - ustał cel (koniec procesu rekrutacji, roszczenia przedawnione),

  - wycofano zgodę,

  - wniesiono sprzeciw i nie ma nadrzędnych interesów administratora.
- Jak załatwiamy pozytywnie, to musimy poinformować wszystkich odbiorców o tym żądaniu.

Prawo do ograniczenia przetwarzania (art. 18)

- Oznacza zaprzestanie przetwarzania, z wyjątkiem przechowywania.
- Ograniczamy gdy: osoba kwestionuje prawidłowość swoich danych; przetwarzanie nie było zgodne z prawem, ale osoba sprzeciwia się ich usunięciu; nie potrzebujemy danych, ale potrzebuje ich dana osoba do ustalenia, dochodzenia lub obrony roszczeń; przeprowadzamy wstępne postępowanie ws. wniesionego sprzeciwu.
- Jak załatwiamy pozytywnie, to musimy poinformować wszystkich odbiorców o tym żądaniu.
- Jak uchylamy ograniczanie, to musimy poinformować o tym tę osobę.

Prawo do przenoszenia danych (art. 20)

- Kumulatywnie: przetwarzamy na podstawie
  a) [zgoda] albo b) [umowa]
  i w sposób zautomatyzowany
- *Przykład: przenoszenie historii kredytowej, historii rachunku z banku X do banku Y*

Prawo do sprzeciwu wobec przetwarzania (art. 21)

- Przysługuje gdy przetwarzamy dane na podstawie
  e) [władza publiczna administratora] albo
  f) [prawnie uzasadnione interesy administratora]
- *… z przyczyn związanych z jej szczególną sytuacją…*
- Administratorowi nie wolno już przetwarzać tych danych, chyba że istnieją przesłanki nadrzędne nad interesami, prawami i wolnościami osoby, której dane dotyczą
- *Przykład*

Niepodleganie profilowaniu (art. 22)

- Prawo do niepodleganiu decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu
- Wyjątki: lit. b) [umowa], dozwolone prawem Unii lub państwa członkowskiego, lit. a) [wyraźna zgoda]
- Środki ochrony praw i wolności danej osoby minimum: interwencja ludzka ze strony administratora, wyrażenie własnego stanowiska i zakwestionowanie tej decyzji

Procedura realizacji praw (art. 12)

- Nie jest to procedura z Kpa, Op czy innej ustawy proceduralnej. Jest to postępowanie autonomiczne, w oparciu o przepisy RODO
- Zwięzła, przejrzysta, zrozumiała i łatwo dostępna forma; jasny i prosty język
- Termin – bez zbędnej zwłoki; nie później niż miesiąc od otrzymania żądania (wyjątkowo 2 miesiące)
- Jeżeli odpowiedź jest **negatywna** => obowiązkowe informacje o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem
- Postępowanie co do zasady jest wolne od opłat.
- Kwestia identyfikacji tożsamości osoby w przypadkach uzasadnionych wątpliwości
- Procedurę realizuje administrator.

Podmiot przetwarzający (art. 28)

- Przetwarza w imieniu administratora i na jego udokumentowane polecenie
- Musi dawać gwarancje wdrożenia środków technicznych i organizacyjnych
- Uprzednia pisemna zgoda administratora na podpowierzanie (pp korzysta z usług innego pp)
- Przetwarzanie na podstawie umowy lub innego instrumentu prawnego wiążącego strony
- Wymogi – art. 28 ust. 3
- Podpowierzanie – analogicznie…

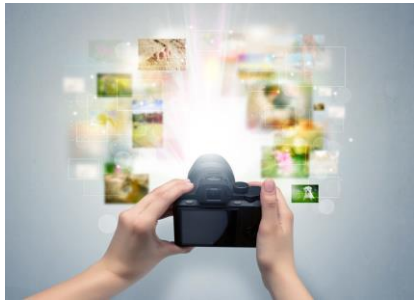
Powierzenie przetwarzania a udostępnienie

	Powierzenie	Udostępnienie
Administrator	Nie zmienia się	Zmienia się
Cel	Ten sam	Inny
Instrument prawny	Umowa lub inny	Brak (może być przepis prawa)
Przetwarzanie	W imieniu i na rzecz administratora	Administrator w swoim imieniu

Przykład powierzenia przetwarzania danych osobowych

- Jestem pasażerem KMK i mam bilet okresowy.
- Zadanie organizacji publicznego transportu zbiorowego wykonuje gmina.
- Administratorem moich danych jest zatem Zarząd Transportu Publicznego w Krakowie.
- Podmiotem przetwarzającym jest MPK S.A. w Krakowie.

Rozpowszechnianie wizerunku



Ustawa o prawie autorskim i prawach pokrewnych

Art. 81. 1. Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

2. Zezwolenia nie wymaga rozpowszechnianie wizerunku:

1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku
z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;

2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.