

Elektroniczny obrót gospodarczy i jego bezpieczeństwo

*Wykład nr 3
2019/2020*

Dr Sylwia Kotecka-Kral

**Centrum Badań Problemów Prawnych
i Ekonomicznych Komunikacji Elektronicznej
WPAiE UWr**

**MECHANIZM ŚLEDZENIA
I PROFILOWANIA W SIECI – JAK Z
KLIENTA STAJESZ SIĘ TOWAREM.
OCHRONA DANYCH OSOBOWYCH W UE**

Źródło dotyczące śledzenia, użyte w prezentacji

- K. Szymielewicz, „Śledzenie i profilowanie w sieci: W czym problem? Co się zmieni w prawie? Jak może wyglądać przyszłość?”
 - raport Fundacji Panoptikon,
https://panoptikon.org/sites/default/files/publikacje/sledzenie_i_profilowanie_w_sieci_scenariusze_po_reformie_ue_wrzesien_2017.pdf
- Polecam też: K. Szymielewicz, K. Iwańska, *Śledzenie i profilowanie w sieci. Jak z klienta stajesz się towarem*, Raport Fundacji Panoptikon (styczeń 2019),
 - https://panoptikon.org/sites/default/files/publikacje/panoptikon_raport_o sledzeniu_final.pdf
- O pojęciach: reklamy behawioralnej, reklamy kontekstowej, reklamy segmentowej, reklamy targetowanej zob. S. Kotecka-Kral, *Zagrożenia związane z przetwarzaniem danych osobowych osób fizycznych w celu profilowania* (w:) A. Dańko-Roesler (red.), M. Leśniak (red.), M. Skory (red.), B. Sołtys (red.), *Ius est ars boni et aequi. Księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi*, Wrocław 2018, s. 563-564.
- Zob. także Opinia Grupy Roboczej Art. 29 nr 2/2010 (WP 171) w sprawie internetowej reklamy behawioralnej, przyjęta dnia 22.06.2010 r.
 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_pl.pdf

?

- Ile aplikacji zainstalowali Państwo na swoich smartfonach?
- Do czego służą te aplikacje?
- Do jakich danych mają dostęp te aplikacje?
- Po co aplikacjom dostęp do tych danych?
- Czy często dokonują Państwo zakupów przez Internet?
- Czy spotkali się Państwo z pojęciem „cookies”? Co to jest?

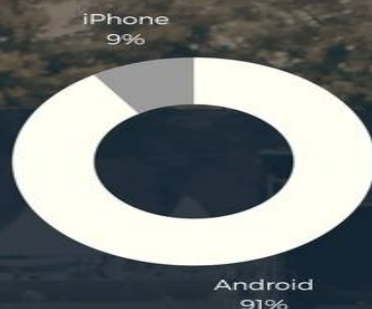
Smartfony

- **Przeciętny użytkownik smartfona korzysta aktywnie z około 27 aplikacji miesięcznie. Tylko nieliczni inwestują czas i uwagę w zapoznanie się z ich regulaminami i politykami prywatności.**
- Zob. artykuł pt. „Skąd wiadomo, że 14% uczestników Open'era stara się o dziecko?” (zdjęcia na następnych slajdach ze strony:
 - <https://niebezpiecznik.pl/post/za-darmowe-aplikacje-mobilne-placisz-informacjami-o-sobie-wyjasniamy-smartfonowy-skandal-z-openera/>)

OPEN'ER FESTIVAL 2017

użytkownicy smartfonów w liczbach

118 421
użytkowników smartfonów



operatorzy:



51,5%

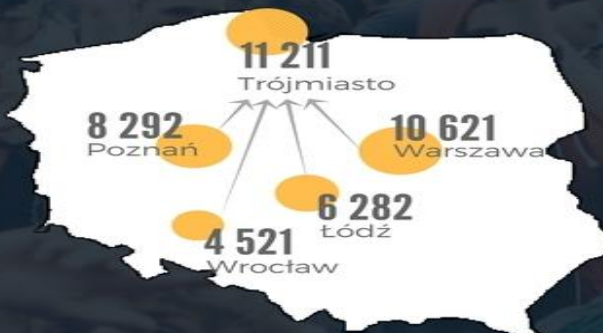
mężczyźni



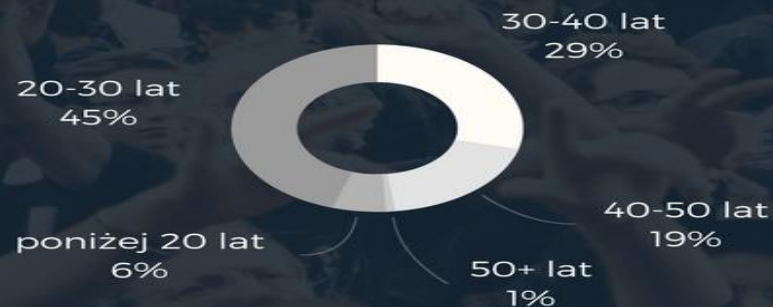
48,5%

kobiety

najwięcej uczestników wg. miast:



struktura wieku:





PROFILE UŻYTKOWNIKÓW

Kobiety starające się o dziecko	14%
Osoby, które były przez ostatnie 6 miesięcy za granicą	28%
Osoby słuchające muzyki na smartfonie	89%
Klienci Lidl i Biedronki	82%
Osoby aktywnie uprawiające sport	14%
Osoby dbające o zdrowie (dieta, sport itp.)	32%
Mieszkańcy 30 największych miast w Polsce	44%
Rodzice dzieci w wieku 0-12m	1%
Rodzice dzieci w wieku 1-3 lat	1,5%
Rodzice dzieci w wieku 4-5 lat	4%
Mniejszości seksualne	11%
Osoby aktywnie poszukujące partnera	29%
Osoby zainteresowane kredytem i chwilówkami	16%
Osoby zainteresowane zakupem nieruchomości	4%

*Dane w infografice pochodzą z silnika danych Selectiv DMP (Data Management Platform). Zbierane są za pośrednictwem bezpłatnych aplikacji zainstalowanych przez użytkownika na smartfonie. W/w profile są konstruowane na podstawie aktywności użytkownika w aplikacjach oraz na mobilnych stronach WWW. „Kobiety starające się o dziecko” to profil zawierający użytkowniczki aplikacji takich jak PeriodTracker, WomanLog, GetBaby i ich polskich odpowiedników. Profil „mniejszości seksualne” to zbiór użytkowników aplikacji randkowych dedykowanych dla społeczności LGBT. Osoby zainteresowane zakupem nieruchomości to osoby, które odwiedziły fizycznie w ciągu ostatnich 6 miesięcy targi mieszkaniowe.

Smartfony

- Katalizatorem i kluczowym narzędziem śledzenia i profilowania na potrzeby komercyjne stały się smartfony – komputery osobiste nowej generacji, z którymi większość użytkowników nie rozstaje się przez całą dobę, w jednym urządzeniu łącząc sferę osobistą i zawodową oraz angażując się w setki (o ile nie tysiące) drobnych interakcji dziennie.
- Standardowo korzystanie z aplikacji mobilnych generuje metadane: adres IP, czas dostępu, długość trwania sesji, rodzaj używanego oprogramowania, lokalizację urządzenia.
- Z metadanych – w połączeniu z informacjami o tym, w jaki sposób dana osoba korzystała z aplikacji czy usługi (gdzie kliknęła, czego szukała, co kupiła) – powstaje dokładny profil użytkownika, obejmujący także jego cechy osobowości i opis przyzwyczajzeń i indywidualnego trybu życia.
- **Przeciętny użytkownik smartfona korzysta aktywnie z około 27 aplikacji miesięcznie.** Tylko **nieliczni** inwestują czas i uwagę w zapoznanie się z ich regulaminami i politykami prywatności.

Dane osobowe nową walutą

- **Dane osobowe pod różnymi postaciami stały się nową walutą.** Szacuje się, że wartość rynkowa ogółu danych przetwarzanych online na terenie Unii Europejskiej osiągnie do 2020 r. wartość 739 miliardów euro
 - źródło: Komisja Europejska, European Data Market Study, <https://ec.europa.eu/digital-single-market/en/news/final-resultseuropean-data-market-study-measuring-size-and-trends-eu-data-economy>.
- Analiza zainteresowań, potrzeb i słabości użytkowników Internetu służy w praktyce do ich kategoryzowania i hierarchizowania.
- Firmy opracowały strategie włączania całych grup klientów do określonych działań promocyjnych i wyłączania ich z nich, taktyki wpływania na ich zachowania (odtworzone na podstawie zebranych danych) oraz metody mierzenia i optymalizowania wyników takich działań. Strategie i modele biznesowe firm w coraz większym stopniu opierają się na ilości i jakości danych osobowych, jakie są w stanie pozyskać lub sprzedać innym.

Śledzenie

w celu oferowania produktów

- Usługi internetowe, w szczególności serwisy informacyjne, utrzymują się głównie dzięki targetowanej reklamie (skierowanej do określonych kategorii użytkowników).
- Pytanie, czy rynek reklamowy musi się rozwijać w oparciu o nieprzejrzyste i nieetyczne praktyki, takie jak śledzenie ludzi bez ich wiedzy i zgody.
- Techniki śledzenia i profilowania stają się coraz bardziej inwazyjne, nie oszczędzając żadnej sfery życia prywatnego. Dane dotyczące zdrowia (także intymnego czy psychicznego), sytuacji finansowej, pochodzenia etnicznego, relacji osobistych, nałogów, słabości, marzeń i aspiracji miliardów ludzi są zbierane lub generowane (na zasadzie predykcji - przewidywania) oraz integrowane w sposób, który nie uwzględnia możliwych ryzyk.
- Kojarzeniem tego typu danych poza kontrolą ludzi, których one dotyczą, są zainteresowani nie tylko ubezpieczyciele czy potencjalni pracodawcy, ale coraz częściej także partie konkurujące w wyścigach wyborczych.

Jakie dane są pożądane przez aplikacje

- Bez względu na rodzaj i funkcje zainstalowanej aplikacji – użytkownik zapewne będzie musiał zezwolić jej na:
 - dostęp do swoich kontaktów,
 - dostęp do kalendarza,
 - dostęp do historii przeglądanych stron i zakładek,
 - dostęp do wrażliwych logów aplikacji systemowych,
 - dostęp do aplikacji aktywnych na danym urządzeniu,
 - dostęp do historii wybieranych numerów,
 - dostęp do wszystkich profili użytkownika na danym urządzeniu,
 - dostęp do treści i metadanych wysyłanych SMS-ów,
 - dostęp do załączników e-maili,
 - możliwość zmiany ogólnych ustawień telefonu.

Jakie dane są pożądane przez aplikacje

- Uprawnienie do dostępu do aktywnych aplikacji zapewne nie wzbudzi zastrzeżeń w przypadku aplikacji służących do zarządzania zadaniami (często zintegrowanych z kalendarzem czy kontem pocztowym). Jeśli jednak o taki dostęp „prosi” oprogramowanie typu latarka czy fitness tracker...?
- Do czego potrzebny jest dostęp do kontaktów aplikacji (np. latarce), która nie oferuje żadnej funkcji związanej z zarządzaniem kontaktami?
- Twórcy aplikacji nie kryją, że często ich główną intencją i powodem, dla którego oferują coś za darmo, jest **zebranie danych, których sama aplikacja nie wykorzystuje, ale które mają realną, rynkową wartość**.
- Dlatego **większość aplikacji dostępnych na rynku przekazuje dane stronom trzecim**
 - takim, z którymi użytkownik aplikacji nie nawiązuje umowy

Polityki prywatności

- Do głębszej analizy polityk prywatności zniechęca **adhezyjny charakter umów**: jedyne, co użytkownicy mogą zrobić, to pójść gdzie indziej.
- Ostatecznie korzystanie z wielu urządzeń mobilnych nie jest dziś możliwe bez konta na serwerze Google'a, Microsoftu czy Apple'a.

Śledzenie lokalizacji użytkownika

- Nagminność śledzenia lokalizacji przez aplikacje mobilne to jeden z najpoważniejszych problemów w sferze ochrony prywatności.
- Skutecznych sposobów na ustalenie lokalizacji bez wiedzy i zgody użytkownika jest wiele: w grę może wchodzić np.
 - dostęp do technicznych danych o logowaniu telefonu do stacji przekąźnikowych,
 - śledzenie przy pomocy czipu GPS zainstalowanego w telefonie lub
 - wewnętrznego rejestru lokalizacji (location logs).
- Przybliżone dane o położeniu użytkownika można również odtworzyć na podstawie:
 - historii zapamiętanych sieci WiFi (nawet jeśli nie doszło do połączenia z siecią),
 - historii przypisanych danemu urządzeniu adresów IP,
 - metadanych zapisanych na tym urządzeniu zdjęć, które standardowo zawierają współrzędne geograficzne ustalone w momencie robienia zdjęcia.

Internet rzeczy

(Internet of Things, IoT)

- Czytniki e-booków, smart TV, termostaty, czujniki gazu, inteligentne lodówki, okulary, szczoteczki do zębów i zabawki, a ostatnio nawet autonomiczne odkurzacze zasilają bazy danych nowymi wskaźnikami, zbieranymi i nierzadko przekazywanymi dalej w czasie rzeczywistym.
- Tego typu urządzenia, analogicznie do smartfonów, zapewniają firmom rosnący dostęp do informacji na temat preferencji i przyzwyczajeń ich klientów w wielu obszarach życia codziennego.
- Dostęp do zebranych danych mogą mieć również tzw. platformy IoT – zaawansowane aplikacje ułatwiające firmom analizowanie i zarządzanie danymi, dostarczane i obsługiwane przez wyspecjalizowane korporacje

Internet rzeczy

(Internet of Things, IoT)

- Przykład – inteligentne liczniki poboru energii elektrycznej:
 - https://www.tvn24.pl/wideo/z-anteny/zdradliwe-napiecie,721467.html?playlist_id=23566
 - ważne są wypowiedzi Wojciecha Wiewiórowskiego, byłego już Generalnego Inspektora Ochrony Danych Osobowych
- Zysk z komercjalizacji danych osobowych może czerpać wiele niezależnych podmiotów. Dobrym przykładem jest wykorzystanie sensorów i inteligentnego oprogramowania w samochodach. Terabajty danych generowane przez inteligentne auta to realna wartość dla:
 - producentów,
 - dealerów samochodowych,
 - leasingodawców,
 - autorów wyspecjalizowanych w tej branży aplikacji,
 - producentów oprogramowania do telefonów komórkowych takich jak Google czy Apple,
 - brokerów danych,
 - agencji reklamowych,
 - służb porządkowych,
 - windykatorów.

Skrypty śledzące i targetowane reklamy

- Dostawcy treści w Internecie (wydawcy gazet, właściciele blogów, media społecznościowe) utrzymują się przede wszystkim ze sprzedaży przestrzeni reklamowej.
- Ich realnym klientem jest nie ten, kto odwiedza stronę, ale ten, kto płaci za wyświetlenie na niej reklamy
 - reklama kontekstowa, skierowana do zdefiniowanego odbiorcy – i to w momencie, w którym jest szansa, że ten konkretny człowiek kupi oferowany mu produkt.
- Tylko znając ich zainteresowania, siłę nabywczą i sposoby reagowania, dostawcy treści są w stanie zapewnić swoim klientom odpowiedni wskaźnik klikalności (ang. *click through rate*) i uzyskać dobrą cenę za wyświetlane reklamy.
- Taka operacja marketingowa wymaga rzetelnych danych na temat wieku, płci, miejsca zamieszkania, zainteresowań, sytuacji życiowej, sytuacji majątkowej, historii zakupów, sieci społecznościowej, a nawet cech osobowości potencjalnego klienta.
- **Ilu z nich ujawnia je świadomie, z własnej woli?**

Mechanizm real time bidding (RTB)

- Dostawcy treści internetowych wystawiają na sprzedaż profile swoich użytkowników oraz wyświetlaną im przestrzeń reklamową za pośrednictwem tzw. **platform podaży** (ang. Supply Side Platforms) – wyspecjalizowanego oprogramowania, które w czasie rzeczywistym umożliwia komunikację z innymi graczami na giełdzie reklam.
- Liczą się tylko cechy decydujące o skłonności użytkownika do dokonania konkretnego zakupu. Dlatego pośrednicy posługują się **unikatowym numerem użytkownika**, do którego przypisany jest profil o znaczeniu marketingowym (zainteresowania, siła nabywcza, stan zdrowia, ważny moment w życiu etc.).
- Dane wystawiane przez sprzedawców przestrzeni reklamowej odbierają i analizują tzw. **platformy popytu** (ang. *Demand Side Platforms*), zaprogramowane w celu znalezienia użytkowników o określonym profilu.
- Profile poszukiwanych użytkowników określają agencje mediowe, realizujące zlecenia „**Daj mi klienta, który kupi po jak najlepszej cenie to, co mam do sprzedania**”.

Mechanizm real time bidding (RTB)

- Zadaniem **agencji** jest określenie, jakie cechy ma taka osoba i gdzie ją można znaleźć w sieci. Podstawą ich wiedzy o potencjalnych klientach są **dane o zakupach pochodzące bezpośrednio od reklamodawców**. Aby je wygenerować, większość firm utrzymuje systemy zarządzania relacjami (CRM), programy lojalnościowe i własne sklepy internetowe.
- Z informacji o tym, kto i co kupił w przeszłości, wyciągane są cechy typowego klienta. Agencje mediowe mierzą dalej: próbują ustalić, jakie cechy i zachowania charakteryzują osoby, które jeszcze reklamowanego produktu nie kupiły, ale mogą to zrobić w przyszłości. W żargonie reklamowym ten **hipotetyczny profil klienta to *look-alike***.
- *Look-alike* to mieszanka twardych danych pochodzących od reklamodawców („**taki człowiek już u mnie kupił**”) i statystycznej wiedzy o ludziach („**taki człowiek może chcieć to kupić**”). Komponent statystyczny pochodzi z analizy tzw. **big data**, które agencje mediowe pozyskują od dostawców treści, mediów społecznościowych i brokerów danych.

Mechanizm real time bidding (RTB)

- Profile look-alike, wystawiane przez agencje mediowe, i profile faktycznych użytkowników, wystawiane przez dostawców treści (jednocześnie sprzedawców przestrzeni reklamowej), spotykają się na internetowych giełdach. Zadaniem giełdy jest optymalnie dopasować reklamę do użytkownika, który powinien ją zobaczyć. Mają na to **ułamki sekund**.
- Standardowa transakcja w modelu RTB rozpoczyna się w momencie nawiązania przez przeglądarkę połączenia ze stroną, którą ktoś właśnie próbuje załadować na swoje urządzenie. Strona ustala profil tego użytkownika, przypisuje mu unikatowy numer i notyfikuje serwer reklam. Serwer reklam łączy się z platformą podaży i przekazuje jej dane o dostępnej przestrzeni reklamowej oraz o profilu użytkownika, który czeka na jej załadowanie. Platforma podaży wystawia ten profil na giełdzie i czeka na ofertę.

Mechanizm real time bidding (RTB)

- Giełda reklam rozsyła unikatowy numer sprofilowanego użytkownika do współpracujących z nią platform popytu. Ten moment w żargonie to **ad call**. Potencjalni oferenci dowiadują się, że osoba o danym profilu właśnie czeka na wyświetlenie strony internetowej i że mogą dołączyć do niej swoją reklamę. Czy się na to zdecydują i ile zapłacą, zależy od tego, na ile ten profil pokrywa się z poszukiwanym przez nich look-alike.
- W ułamkach sekund, które mają na zawarcie transakcji, platformy popytu zaciągają dodatkowe dane na temat wystawionego profilu.
 - Co wiemy o jego przeszłych transakcjach?
 - Jakie strony odwiedził przed chwilą?
 - Czy porównywał ceny?
 - Czego szuka i ile jest w stanie zapłacić?
- Korzystając ze skryptów śledzących, a czasem też dodatkowych informacji pozyskanych od brokerów danych, podejmują decyzję (tak/nie) i wysyłają ofertę. Oferent, który zaproponował najwyższą stawkę, wygrywa prawo do wyświetlenia reklamy.

Mechanizm real time bidding (RTB)

- Ten proces jest w pełni zautomatyzowany i zdominowany przez algorytmy.
- Z punktu widzenia profilowanego użytkownika pozostaje całkowicie niezauważalny. Dlatego tylko nieliczni interesują się tym, co się dzieje na komercyjnym „zapleczu” Internetu.
- W rezultacie mamy do czynienia z niebezpieczną **asymetrią informacyjną**, którą profesjonalni gracze wykorzystują, by – w nieujawniony sposób – wpływać na zachowania nieświadomych użytkowników.

Mechanizm real time bidding (RTB)

- Niekwestionowanymi liderami w zautomatyzowanym handlu przestrzenią reklamową są największe platformy internetowe: Facebook i Google.
- Ich przewaga polega nie tylko na gigantycznych ilościach danych, jakie zebrały o ludziach, ale też na dostępie do technologii, która gwarantuje odpowiednią prędkość transakcji.
- Google stworzył rynek targetowanej reklamy, na którym kontroluje wszystkie kluczowe role: sprzedaje i kupuje przestrzeń reklamową oraz dostarcza dane i analizę danych po obu stronach transakcji. W tym momencie żaden inny gracz nie może z nim konkurować.
- W drugim szeregu działają brokerzy danych, czyli pośrednicy w handlu danymi, którzy zdobywają dane o użytkownikach Internetu za pośrednictwem innych firm (banków, sklepów, ubezpieczycieli etc.). Najwięksi gracze w tej kategorii to firmy amerykańskie, takie jak Acxiom, Experian czy Datalogix.

Mechanizm real time bidding (RTB)

- **Zakres danych, jakie są dostępne na temat konkretnych użytkowników** (w systemie RTB każdy ma przypisany unikatowy numer identyfikacyjny), w dużej mierze **zależy od rodzaju usług, z których taka osoba korzysta.**
- W szczególności od tego, czy korzysta z mediów społecznościowych lub innych platform (e-commerce, poczta elektroniczna), które wymagają zalogowania i podania prawdziwych danych, a zarazem umożliwiają ciągłe gromadzenie danych behawioralnych.

Mechanizm real time bidding (RTB)

- Na wielowarstwowe profile użytkowników standardowo składają się:
 - imię i nazwisko, adresy, numer telefonu, kod pocztowy, płeć, wiek, stan cywilny, poziom edukacji, sektor zatrudnienia, poziom dochodów, liczba osób pozostających na utrzymaniu użytkownika (i ich wiek), stan posiadania (samochody, nieruchomości etc.), profil etniczny i religijny,
 - szczegółowe dane o lokalizacji ustalone na podstawie współrzędnych GPS, sieci Wi-Fi i adresów IP, z którymi łączyło się urządzenie użytkownika,
 - dane techniczne, takie jak rodzaj systemu operacyjnego, ustawienia przeglądarki i rozdzielczość ekranu, które składają się na (coraz bardziej unikatowy) „odcisk palca” urządzenia,
 - historia aktywności na stronie: w co użytkownik kliknął, co przykuło jego uwagę (i na jak długo), co ostatecznie kupił (i za ile).

Mechanizm real time bidding (RTB)

- Budując profil możliwego klienta (look-alike), agencje mediowe próbują ustalić nawyki, zainteresowania, słabości, ważne momenty z życia (takie jak ślub czy ciąża), cechy osobowościowe i demograficzne użytkowników.
- Na tej podstawie tworzą wąsko zdefiniowane kategorie, powiązane z cechami usługi czy produktu, który mają za zadanie sprzedać: „aktywny styl życia i SUV”, „dom, zdrowe jedzenie”, „przede wszystkim dzieci”, „miejski styl życia, singiel” czy „ponadprzeciętny dochód, dobra luksusowe”.
- Podobnie działają brokerzy danych, którzy w swoich ofertach dla agencji mediowych i innych nabywców wyodrębniają segmenty klientów odpowiadające określonym cechom lub przewidywanym zachowaniom oraz punktację (ang. score) wskazującą na prawdopodobieństwo, że takie cechy lub zachowania się potwierdzą.

Mechanizm real time bidding (RTB)

- Dane osobowe zbierane i przetwarzane w celach marketingowych mają różne źródła i charakter.
- Mogą **pochodzić bezpośrednio od użytkowników**, jeśli zostały przez nich udostępnione w sposób dobrowolny (np. na etapie zawierania umowy) lub zadeklarowane (np. w ramach badania).
- Inną kategorię stanowią **dane „zaobserwowane”**, wynikające z monitorowania realnej aktywności użytkowników w sieci, często w sposób niejawny lub enigmatycznie wspomniany w ogólnych warunkach świadczenia usług.
- Bez względu na źródło pozyskania dane, które odnoszą się do zweryfikowanych cech i zachowań użytkowników, są uważane za „rzeczywiste”.
- Obok nich coraz większą wartość marketingową zyskują **dane „wynioskowane”** (czy też: „wymodelowane”), czyli przypuszczenia na temat ukrytych cech lub przewidywanych zachowań użytkownika generowane na podstawie danych rzeczywistych.

Mechanizm real time bidding (RTB)

- Na opisane kategorie danych nakłada się jeszcze inny podział na:
 - „dane z pierwszej ręki” (pozyskane przez firmy mające bezpośredni związek z klientem) i
 - „dane strony trzeciej” (zgromadzone czy nabyte od innych podmiotów).
- Z regulacyjnego punktu widzenia dane pochodzące od stron trzecich są szczególnie problematyczne, ponieważ użytkownicy, których te informacje charakteryzują, mają nad ich gromadzeniem i wykorzystywaniem najmniejszą kontrolę.

Jak się uwolnić od numeru identyfikacyjnego przypisanego do marketingowego profilu?

- Dla smartfonów z systemem Android
 - Ustawienia / Google / Reklamy / Resetuj identyfikator wyświetlania reklam
- Możliwość rezygnacji z personalizacji reklam
- Zob. także informacja „Reklamy Google”

**PRAWNE PODSTAWY HANDLU
ELEKTRONICZNEGO (CZ. 2)
- UNIJNA REFORMA 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 Nr 119 z 4.05.2016 r., s. 1
 - **stosowane – jako część krajowego porządku prawnego - od 25 maja 2018 r.**

RODO

- **„Profilowanie”** oznacza dowolną formę **zautomatyzowanego przetwarzania danych osobowych**, które polega na **wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej**, w szczególności **do analizy lub prognozy** aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się
— art 4 pkt 4 RODO

Cechy profilowania

- Trzy cechy, które musi wykazywać profilowanie, aby podlegać przepisom RODO:
 1. wykorzystanie danych osobowych;
 2. w sposób zautomatyzowany;
 3. do oceny czynników osobowych osoby fizycznej.
- Przepisy RODO mają zastosowanie tylko do profilowania zautomatyzowanego.
- Profilowanie można określić jako formę przetwarzania danych osobowych polegającą na wykorzystaniu dostępnych informacji o osobie fizycznej do analizowania lub przewidywania pewnych aspektów dotyczących tej osoby fizycznej (np. preferencji, zainteresowań, wiarygodności), czyli na wyprowadzaniu wniosków dotyczących osoby fizycznej na podstawie posiadanych informacji.
- **Profilowanie nie jest celem przetwarzania danych osobowych, ale rodzajem opracowania danych na potrzeby określonego celu.**

Dwie postaci profilowania

1. Analizowanie lub prognozowanie aspektów dotyczących osoby fizycznej przez **zestawianie ze sobą informacji dotyczących tylko tej osoby** („opracowanie profilu”)
 - przesyłanie klientowi, który kupił dany towar, ofert dotyczących tego samego segmentu towarów
2. **Przypisywanie osobie fizycznej dodatkowych cech, pochodzących z analizy statystycznej** informacji dotyczących innych ludzi („przypisanie do profilu”)
 - jeżeli osoba profilowana ma znane profilującemu cechy występujące w zbiorowości, to ma również inne cechy, którymi ta zbiorowość się charakteryzuje
 - ten rodzaj profilowania przydatny zwłaszcza do analizy ryzyk, np. ubezpieczeniowego czy kredytowego

Dwa rodzaje profilowania wg RODO

- Profilowanie prowadzone w celu automatycznego podejmowania decyzji, które **wywołuje wobec podmiotu danych skutki prawne lub w podobny sposób istotnie na niego wpływa** („szczególne”)
 - przykładowe skutki prawne: automatyczne odrzucenie wniosku kredytowego, elektroniczne metody rekrutacji bez interwencji ludzkiej, odrzucenie wniosku o objęcie ochroną ubezpieczeniową
 - przykładowy istotny wpływ: automatyczne ustalanie wysokości składki ubezpieczeniowej oraz wysokości lub zabezpieczeń udzielanego kredytu.
- Pozostałe profilowanie („zwykłe”)

RODO

- Aby stwierdzić, czy czynność przetwarzania można uznać za „**monitorowanie zachowania**” **osób, których dane dotyczą**, należy ustalić, czy osoby fizyczne są obserwowane w Internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.
 - motyw 24 preambuły RODO

Przesłanki dopuszczalności profilowania

- Jeżeli decyzja, na potrzeby której prowadzone jest profilowanie:
 1. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą a administratorem (art. 22 ust. 2 lit. a RODO);
 2. jest dozwolona prawem UE lub prawem państwa członkowskiego, któremu podlega administrator, przy zastrzeżeniu, że przewiduje ono „właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą” (art. 22 ust. 2 lit. b RODO);
 3. opiera się na wyraźnej zgodzie osoby, której dane dotyczą (art. 22 ust. 2 lit. c RODO).
- Wystarczy zaistnienie jednej z tych przesłanek.

Profilowanie w celu zautomatyzowanego podejmowania decyzji

- Nie może opierać się na:
 - przesłance niezbędności dla celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora danych lub inny podmiot
 - przesłance niezbędności do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej
- **Przepis prawa, aby uzasadniał tego typu profilowanie, musi wprost zezwalać na zautomatyzowane podjęcie decyzji.**

Profilowanie w celu zautomatyzowanego podejmowania decyzji

- Ograniczenie wykorzystania do profilowania „szczególnego” danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, oraz danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej.
- Wykorzystanie takich danych jest możliwe po spełnieniu łącznie przesłanek:
 1. osoba, której dane dotyczą, wyraziła **wyraźną zgodę** lub **przetwarzanie jest niezbędne** ze względów związanych z ważnym interesem publicznym, na podstawie prawa UE lub prawa państwa członkowskiego;
 2. istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą (przede wszystkim udział czynnika ludzkiego w rozstrzyganiu zastrzeżeń do decyzji).

Przesłanki profilowania „zwykłego”

- Standardowe przesłanki przetwarzania danych osobowych określone w art. 6 ust. 1 i art. 9 ust. 2 RODO.

RODO

- Zasady rzetelnego i przejrzystego przetwarzania wymagają, **by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach.**
- **Należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania.** Jeżeli gromadzi się dane osobowe od osoby, której dane dotyczą, należy ją też poinformować, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.
- Informacje te można przekazać w połączeniu ze standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawiają sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, powinny nadawać się do odczytu maszynowego.
 - motyw 60 preambuły RODO

RODO

- **Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących** oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem.
- Każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, **w szczególności w zakresie celów**, w jakich dane osobowe są przetwarzane, w miarę możliwości **okresu**, przez jaki dane osobowe są przetwarzane, **odbiorców** danych osobowych, **założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych** oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania.

RODO

- W miarę możliwości administrator powinien mieć możliwość **udzielania zdalnego dostępu** do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych.
- Prawo to **nie powinno negatywnie wpływać na prawa lub wolności innych osób**, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie.
- Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji.
- Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, **sprecyzowała informacje lub czynności przetwarzania**, których dotyczy jej żądanie.
 - motyw 63 preambuły RODO

RODO

- Jeżeli **dane osobowe są przetwarzane do celów marketingu bezpośredniego**, osoba, której dane dotyczą, powinna mieć prawo wnieść w dowolnym momencie, bezpłatnie **sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego – w tym profilowania**, o ile jest ono powiązane z marketingiem bezpośrednim.
- Prawo to powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji.
 - motyw 70 preambuły RODO

RODO

- Osoba, której dane dotyczą, powinna mieć **prawo do tego, by nie podlegać decyzji** – mogącej obejmować określone środki – **która ocenia jej czynniki osobowe, opiera się wyłącznie na przetwarzaniu zautomatyzowanym i wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa**, jak na przykład automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej.
- **Do takiego przetwarzania zalicza się „profilowanie”** – które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności **analizować lub prognozować** aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa.

RODO

- Niemniej podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, powinno być **dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego**, któremu podlega administrator, w tym do celów monitorowania i zapobiegania – zgodnie z uregulowaniami, standardami i zaleceniami instytucji Unii lub krajowych podmiotów nadzorujących – oszustwom i uchylaniu się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora, lub **gdy jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem**, lub **gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę**.
- Przetwarzanie takie powinno zawsze **podlegać odpowiednim zabezpieczeniom**, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji.
- **Takie przetwarzanie nie powinno dotyczyć dzieci.**

RODO

- Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien:
 - stosować odpowiednie matematyczne lub statystyczne procedury profilowania,
 - wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów,
 - zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą oraz

RODO

- **zapobiegający m.in. skutkom w postaci dyskryminacji osób fizycznych** z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub skutkujący środkami mającymi taki efekt.
- Zautomatyzowane podejmowanie decyzji i **profilowanie oparte na szczególnych kategoriach danych osobowych** powinny być **dozwolone wyłącznie przy zachowaniu szczególnych warunków**.
 - motyw 71 preambuły RODO

RODO

- **Ocena skutków przetwarzania danych** powinna mieć **zastosowanie w szczególności do operacji przetwarzania o dużej skali** – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – **oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób**, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw.

RODO

- **Oceny skutków dla ochrony danych** należy także dokonywać w przypadkach, w których **dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej** po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych **na podstawie profilowania tych danych** lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych środków bezpieczeństwa.

RODO

- **Ocena skutków dla ochrony danych** jest niezbędna również w przypadku **monitorowania na dużą skalę miejsc publicznie dostępnych** – w szczególności za pomocą urządzeń optyczno-elektronicznych – lub wszelkich innych operacji, względem których właściwy organ nadzorczy uznaje, że przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności dlatego, że operacje te uniemożliwiają osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy lub mają systematyczny charakter i dużą skalę.
- Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa.
 - motyw 91 preambuły RODO

RODO

- 2. Podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania (...):
 - **f) informacje o zautomatyzowanym podejmowaniu decyzji**, w tym **o profilowaniu**, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
- 3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.
 - art. 13 **Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą**

RODO

- Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą: (...):
- g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
 - **Art 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą**

RODO

- 1.Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora **potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące**, a jeżeli ma to miejsce, jest **uprawniona do uzyskania dostępu do nich** oraz następujących informacji (...):
 - h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
- 2.Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem.
 - art. 15 **Prawo dostępu przysługujące osobie, której dane dotyczą**

RODO

- **3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.** Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
- **4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.**
 - **art. 15 Prawo dostępu przysługujące osobie, której dane dotyczą**

RODO

- 1.Osoba, której dane dotyczą, ma **prawo w dowolnym momencie wnieść sprzeciw** – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
- 2.Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
- 3.Jeżeli osoba, której dane dotyczą, wnieśnie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

RODO

- 4. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
- 5. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.
- 6. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
 - art. 21 **Prawo do sprzeciwu**

RODO

- 1.Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
- 2.Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
 - a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
 - b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
 - c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

RODO

- 3.W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
- 4.Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
 - art. 22 **Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie**

RODO

- 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.
- 2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

RODO

- 3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:
- a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
- c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

RODO

- 4. Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.
- 5. Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.
- 6. Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.

RODO

- 7.Ocena zawiera co najmniej:
 - a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
 - b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
 - c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
 - d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
- 8.Oceniając – w szczególności do celów oceny skutków dla ochrony danych – skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40.
- 9.W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.

RODO

- 10. Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.
- 11. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
 - art. 35 **Ocena skutków dla ochrony danych**

- **Dziękuję za uwagę!**