

11 PAŹDZIERNIKA 2021 R.
WYKŁAD KDZ ORA WARSZAWA

PODSTAWY PRAWA OCHRONY DANYCH OSOBOWYCH

adw. Agnieszka Rapcewicz

Plan wykładu

1. Wprowadzenie: akty prawne regulujące ochronę danych osobowych.
2. Podstawowe pojęcia.
3. Podstawy prawne przetwarzania danych osobowych.
4. Obowiązek informacyjny.
5. Decyzje PUODO dot. ww. zagadnień.
6. Podsumowanie i pytania.



PRAWO OCHRONY DANYCH OSOBOWYCH

CZYLI NIE TYLKO RODO



**RODO - stosowanie
od 25 maja 2018 r.
(wejście w życie już
w 2016 r.)**

Przepisy krajowe

1. ustawa DODO (Dz.U. 2019 poz. 125),
2. ustawa o ochronie danych osobowych z 10 maja 2018 r. (Dz. U. 2018 poz. 1000),
3. ustawa z 21 lutego 2019 r. "dostosowująca do RODO" ok. 170 aktów prawnych (Dz. U. 2019 poz. 730):
 - kodeks pracy - przepisy dotyczące danych pozyskiwanych od kandydata lub pracownika, monitoring,
 - prawo o adwokaturze, ustawa o radcach prawnych - wyłączenie obowiązku realizacji praw podmiotów danych w zakresie, który miałby naruszać tajemnicę zawodową, wprowadzenie okresów przechowywania danych,
 - UŚUDE i Prawo telekomunikacyjne - wymagania zgody odpowiadające RODO

Ustawa o ochronie danych osobowych

Ustawa określa:

- 1. podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu;**
2. warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych, akredytowanego przez Polskie Centrum Akredytacji, zwanego dalej „podmiotem certyfikującym”, podmiotu monitorującego kodeks postępowania oraz certyfikacji;
3. tryb zatwierdzenia kodeksu postępowania;
- 4. organ właściwy w sprawie ochrony danych osobowych;**
- 5. postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;**
6. tryb europejskiej współpracy administracyjnej;
- 7. kontrolę przestrzegania przepisów o ochronie danych osobowych;**
- 8. odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem;**
- 9. odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych**

Ustawa o ochronie danych osobowych

1. Do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. z 2018 r. poz. 1914), a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5–9, art. 11, art. 13–16, art. 18–22, art. 27, art. 28 ust. 2–10 oraz art. 30 rozporządzenia 2016/679.
2. Do wypowiedzi akademickiej nie stosuje się przepisów art. 13, art. 15 ust. 3 i 4, art. 18, art. 27, art. 28 ust. 2–10 oraz art. 30 rozporządzenia 2016/679.



PODSTAWOWE POJĘCIA



Dane osobowe

wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); 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 lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej



DANE ZWYKŁE

art. 6 RODO

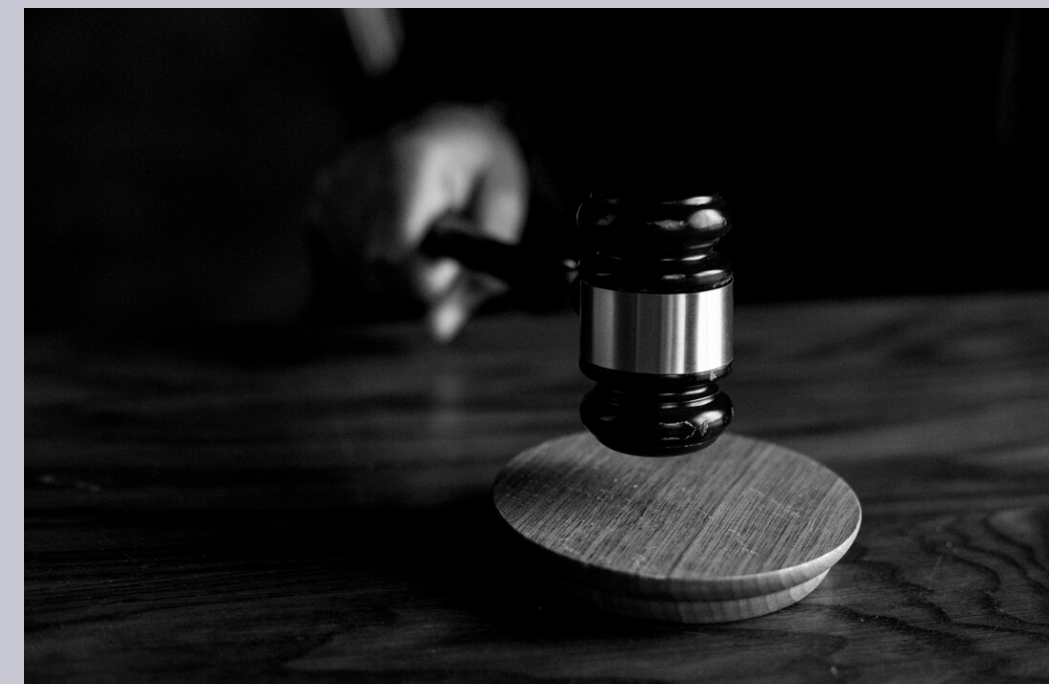
- imię, nazwisko
- dane kontaktowe
- PESEL, numer dokumentu tożsamości, NIP
- dane finansowe
- dane o stanie rodzinnym itd.



DANE SZCZEGÓLNE

art. 9 RODO

- dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych
- dane genetyczne, biometryczne
- dane dotyczące zdrowia, seksualności, orientacji seksualnej



WYROKI I NARUSZENIA

art. 10 RODO

- dane dotyczące wyroków skazujących
- dane dotyczące naruszeń prawa

PODZIAŁ DANYCH OSOBOWYCH

✓ IP (C-582/14 Breyer - teoria obiektywna danych osobowych), unikalny identyfikator reklamowy użytkownika, szeroko pojęta aktywność w Internecie

✓ lokalizacja (dane GPS)

✓ numer rejestracyjny pojazdu - zdaniem Prezesa UODO tak, odmienne stanowisko NSA (I OSK 2063/17)

✓ numer KW - tak; decyzja Prezesa UODO dot. GGK (DKN.5112.13.2020), wyrok WSA (II Sa/Wa 2222/20)

✓ numer telefonu - zdaniem Prezesa UODO tak, odmienne stanowisko WSA (II SA/Wa 1898/20)

✓ adres e-mail - to zależy: agnieszka.rapcewicz@domena.pl - tak; biuro@domena.pl - nie

DANE OSOBOWE



Dane osobowe - teoria subiektywna czy obiektywna?

Motyw 26 RODO:

Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.

Pseudonimizacja



- przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
- dane spseudonimizowane to dane osobowe
- pseudonimizacja jako środek ochrony danych osobowych
- czym innym jest anonimizacja danych osobowych

Stosowanie RODO

- przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz
- przetwarzanie w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych

Zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

Stosowanie RODO

DANE PRZETWARZANE W ZWIĄZKU Z DZIAŁALNOŚCIĄ ZAWODOWĄ/GOSPODARCZĄ

Nie ma znaczenia skala prowadzonej działalności. Do stosowania RODO są zobowiązane nie tylko spółki, ale również indywidualni przedsiębiorcy, także prowadzący działalność nierejestrowaną.

DANE DOTYCZĄCE PRZEDSIĘBIORCÓW I REPREZENTANTÓW

Ochronie podlegają nie tylko dane konsumentów, ale także przedsiębiorców prowadzących jednoosobową działalność, jak również reprezentantów przedsiębiorców (pełnomocników, prokurentów, członków zarządów) i pracowników /współpracowników tych podmiotów.

<https://uodo.gov.pl/pl/225/1577>

DANE DOSTĘPNE PUBLICZNIE

Nie ma znaczenia, czy dane osobowe są dostępne dla ograniczonej liczby osób, czy dostępne publicznie (strony internetowe, publiczne bazy, takie jak CEIDG, KRS itp. Dane osobowe z publicznie dostępnych źródeł również podlegają ochronie.

kara dla Bisnode:
decyzja UODO: ZSPR.421.3.2018

wyrok WSA: II SA/Wa 1030/19

Stosowanie RODO

Zakres terytorialny

przetwarzanie danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii

przykład: polska firma kieruje swoje usługi do obywateli Ukrainy

Stosowanie RODO

Zakres terytorialny

przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

- a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
- b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii

przykład: amerykańska firma kieruje swoje usługi/towary do obywateli z Unii Europejskiej (np. sklep internetowy)

Przetwarzanie

- operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany,
- przykłady: 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.

**PODMIOT
PRZETWARZAJĄCY**

vs.

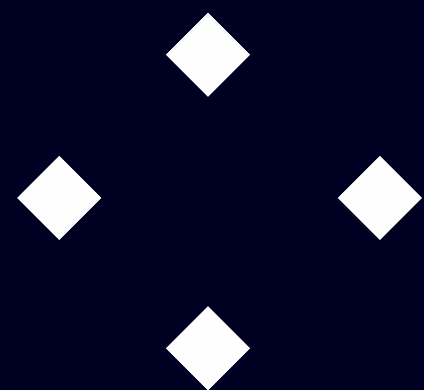
ADMINISTRATOR

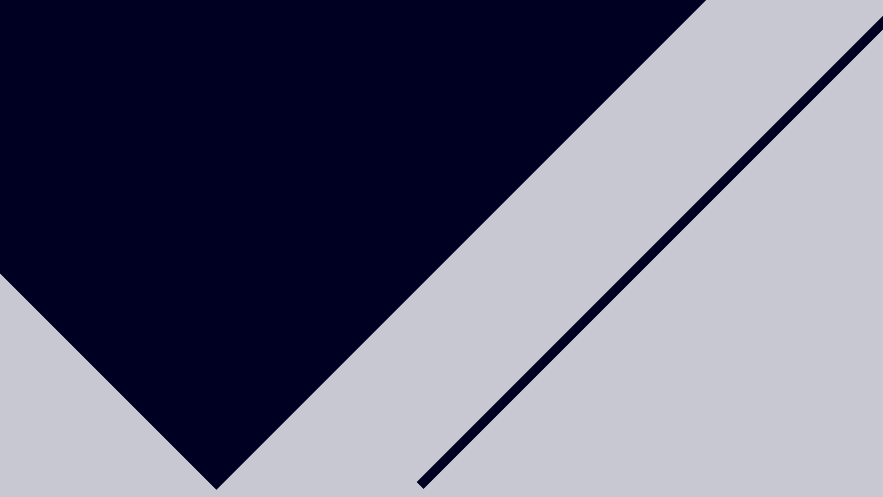
Administrator

- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot (czyli: nie tylko indywidualny przedsiębiorca czy spółka, ale też kasa zapomogowo - pożyczkowa, dom pomocy społecznej)
- samodzielnie lub wspólnie z innymi (=> współadministratorzy) 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
 - podstawa prawna - co do zasady umowa powierzenia zgodnie z art. 28 RODO
 - Guidelines 07/2020 on the concepts of controller and processor in the GDPR (https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en)



Z jakimi podmiotami należy zawrzeć umowę powierzenia?



firma informatyczna, aplikacje/systemy przetwarzające dane osobowe



obsługa kadrowo - księgowo



firma rekrutacyjna (gdy rekrutacja wyłącznie w imieniu i na zlecenie pracodawcy)



obsługa klienta (outsourcing)



obsługa biurowo - administracyjna (w tym najem wirtualnego biura z usługą skanowania korespondencji)



niszczenie i archiwizacja dokumentacji



obsługa prawna (inna niż adwokat/radca prawny lub adwokat/radca prawny, gdy zakres wykracza poza świadczenie pomocy prawnej w rozumieniu ustaw)



Administrator odpowiada w najszerszym zakresie, także za uchybienia swoich pracowników czy podmiotu przetwarzającego (np. sprawa SGGW).

Podmiot przetwarzający odpowiada za brak realizacji obowiązków nałożonych wprost przez RODO – przetwarzanie danych na podstawie umowy powierzenia, odpowiednie zabezpieczenie danych, zobowiązanie swojego personelu do zachowania poufności, prowadzenie rejestru kategorii czynności przetwarzania, usunięcie/zwrot danych po rozwiązaniu umowy powierzenia, odpowiedzialność za dalszy podmiot przetwarzający; wyjście poza polecenia administratora – procesor odpowiada jak administrator.

Kary administracyjne oraz odszkodowania wobec podmiotów danych.

Odpowiedzialność karna.

Odpowiedzialność

PODSTAWY PRAWNE PRZETWARZANIA

art. 6 ust. 1 RODO - dane zwykłe



zgoda - nie powinna być zbierana "na zapas"; decyzja greckiego organu nadzworu w sprawie PwC Business; wytyczne EROD Wytyczne 5/2020 w sprawie zgody na mocy rozporządzenia 2016/679



umowa; Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO



obowiązek prawny



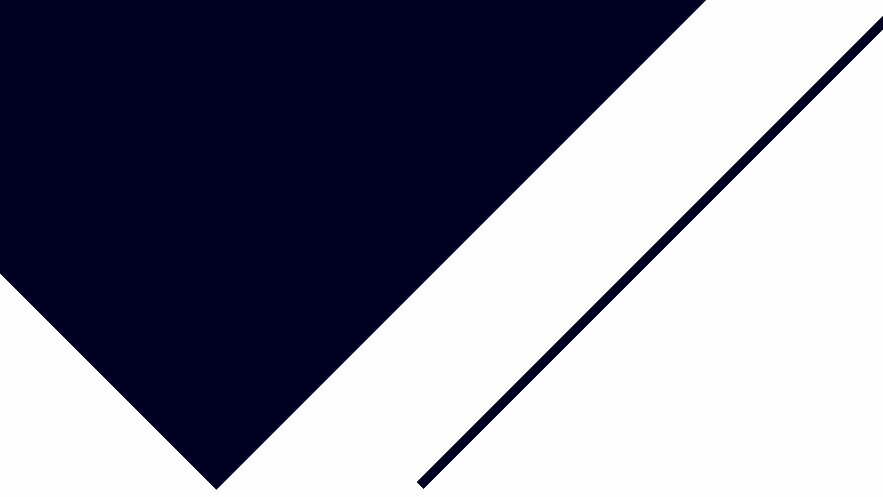
ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej



wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

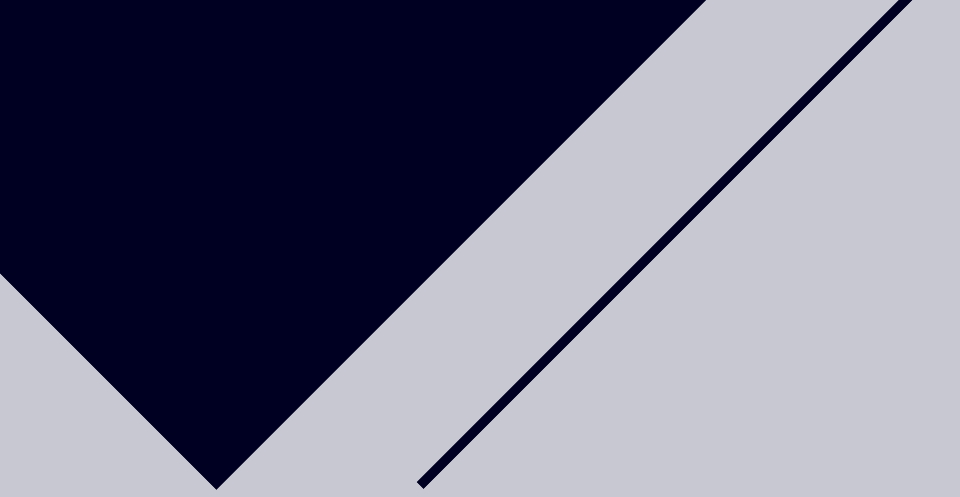


prawnie uzasadniony interes



art. 9 ust. 2 RODO - dane szczególne

- ✓ zgoda
 - ✓ obowiązki i szczególne prawa administratora lub osoby, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
 - ✓ ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody
 - ✓ uprawniona działalności prowadzona z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych
 - ✓ dane osobowe w sposób oczywisty upublicznione przez osobę, której dane dotyczą
-
- ✓ przetwarzanie niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego
 - ✓ niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego
 - ✓ interes publicznym w dziedzinie zdrowia publicznego
 - ✓ cele archiwalne w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych
 - ✓ stalenie, dochodzenie lub obrona roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy
- 



art. 10 RODO - wyroki skazujące i naruszenia prawa



na podstawie art. 6 ust. 1 RODO



wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą



OBOWIĄZEK INFORMACYJNY

Wobec kogo?

- wobec (potencjalnych) klientów
- wobec kontrahentów i ich reprezentantów/pracowników
- wobec własnych pracowników / współpracowników
- wobec użytkowników strony internetowej
- wobec subskrybentów newslettera
- wobec uczestników szkolenia
- wobec odwiedzających profile w mediach społecznościowych
- wobec osób objętych monitoringiem

art. 13 RODO - pozyskiwanie danych bezpośrednio od osoby, której dane dotyczą

art. 14 RODO - pozyskiwanie danych z innego źródła

art. 14 ust. 5 - wyłączenie obowiązku informacyjnego:

- osoba, której dane dotyczą, dysponuje już tymi informacjami;
- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
- pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy

art. 13 i 14 RODO

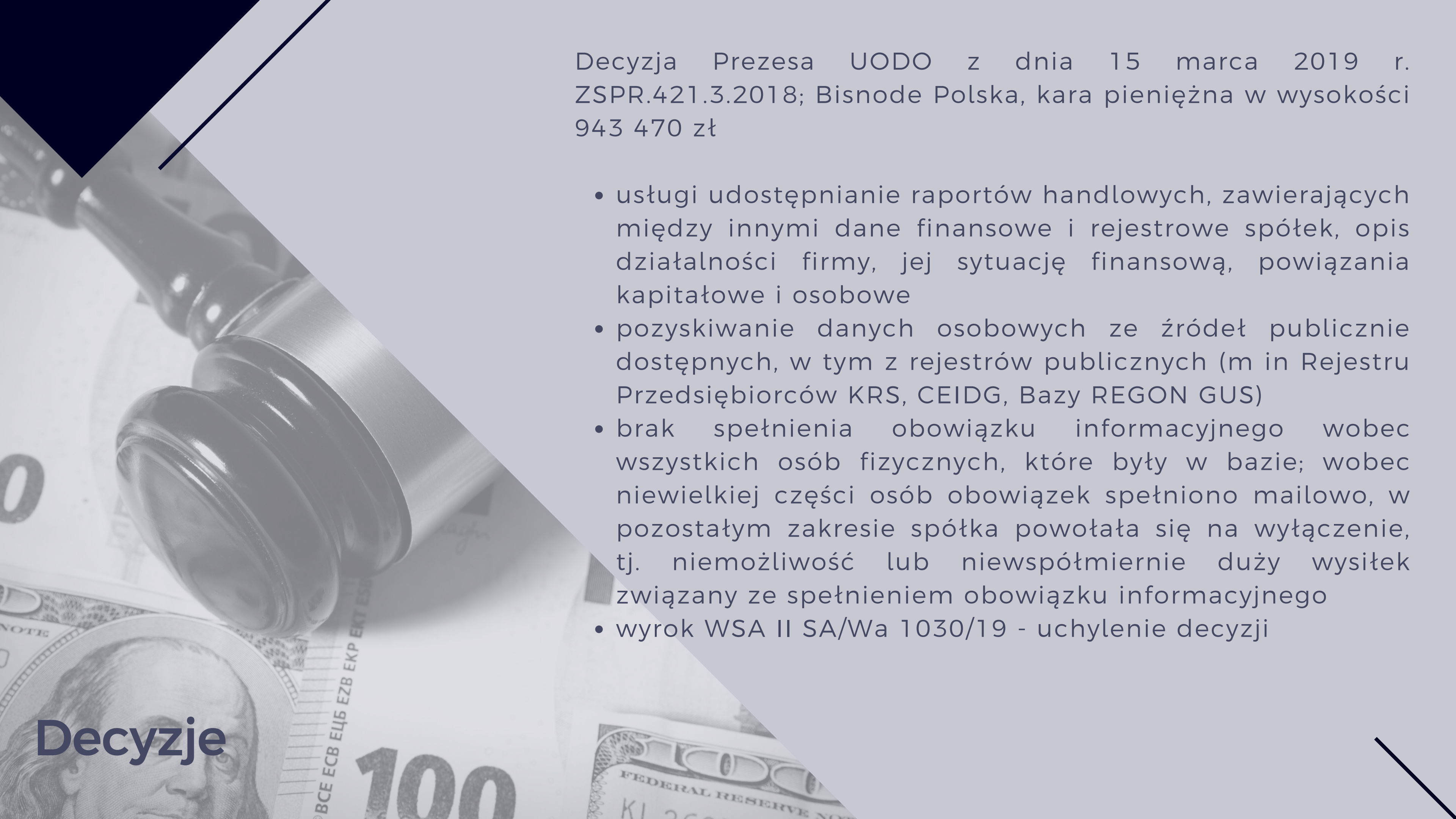
REALIZACJA OBOWIĄZKU INFORMACYJNEGO

Klauzula
informacyjna w treści
umowy lub jako
załącznik do umowy

Polityka prywatności
na stronie
internetowej

Stopka mailowa,
informacja pod
formularzem
kontaktowym lub
podobnym z
odesłaniem do
Polityki prywatności
(wytyczne GR art. 29
dotyczące
przejrzystości WP260
rev.01).

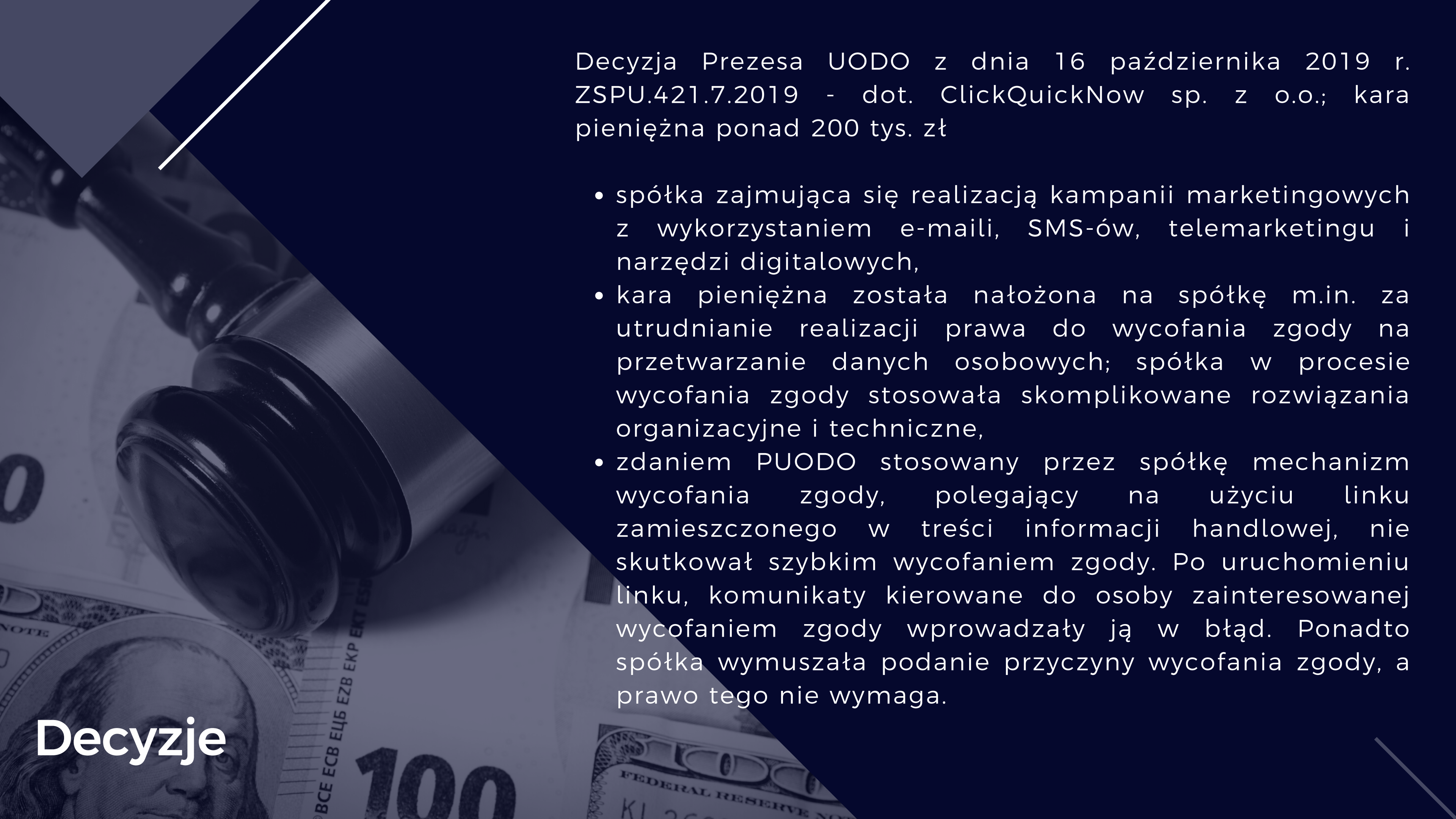
Sekcja "prywatność"
lub "informacje" w
profilu w mediach
społecznościowych.



Decyzja Prezesa UODO z dnia 15 marca 2019 r.
ZSPR.421.3.2018; Bisnode Polska, kara pieniężna w wysokości
943 470 zł

- usługi udostępnianie raportów handlowych, zawierających między innymi dane finansowe i rejestrowe spółek, opis działalności firmy, jej sytuację finansową, powiązania kapitałowe i osobowe
- pozyskiwanie danych osobowych ze źródeł publicznie dostępnych, w tym z rejestrów publicznych (m.in. Rejestru Przedsiębiorców KRS, CEIDG, Bazy REGON GUS)
- brak spełnienia obowiązku informacyjnego wobec wszystkich osób fizycznych, które były w bazie; wobec niewielkiej części osób obowiązek spełniono mailowo, w pozostałym zakresie spółka powołała się na wyłączenie, tj. niemożliwość lub niewspółmiernie duży wysiłek związany ze spełnieniem obowiązku informacyjnego
- wyrok WSA II SA/Wa 1030/19 - uchylenie decyzji

Decyzje



Decyzja Prezesa UODO z dnia 16 października 2019 r.
ZSPU.421.7.2019 - dot. ClickQuickNow sp. z o.o.; kara
pieniężna ponad 200 tys. zł

- spółka zajmująca się realizacją kampanii marketingowych z wykorzystaniem e-maili, SMS-ów, telemarketingu i narzędzi digitalowych,
- kara pieniężna została nałożona na spółkę m.in. za utrudnianie realizacji prawa do wycofania zgody na przetwarzanie danych osobowych; spółka w procesie wycofania zgody stosowała skomplikowane rozwiązania organizacyjne i techniczne,
- zdaniem PUODO stosowany przez spółkę mechanizm wycofania zgody, polegający na użyciu linku zamieszczonego w treści informacji handlowej, nie skutkował szybkim wycofaniem zgody. Po uruchomieniu linku, komunikaty kierowane do osoby zainteresowanej wycofaniem zgody wprowadzały ją w błąd. Ponadto spółka wymuszała podanie przyczyny wycofania zgody, a prawo tego nie wymaga.

Decyzje

Decyzja Prezesa UODO z dnia 18 lutego 2020 r.
ZSZS.440.768.2018 - Szkoła Podstawowa nr 2 w Gdańsku; kara
20 tys. zł

- sprawa dotyczyła przetwarzania danych biometrycznych dzieci podczas korzystania przez nie ze szkolnej stołówki,
- szkoła pozyskiwała te dane i przetwarzała je na podstawie pisemnej zgody rodziców lub opiekunów prawnych,
- organ nadzorczy uznał, że przetwarzanie danych biometrycznych nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu; szkoła może przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka,
- PUODO wskazał, że szczególnej ochrony danych osobowych wymagają dzieci. Dane biometryczne zaś, mają wyjątkowy charakter w świetle podstawowych praw i wolności, dlatego również też wymagają wyjątkowej ochrony. Ewentualny ich wyciek może skutkować dużym ryzykiem naruszenia praw i wolności osób fizycznych.
- II SA/Wa 809/20 - WSA uchylił decyzję PUODO - wyrażenie zgody przewidzianej w art. 9 ust. 1 lit. a RODO legalizuje przetwarzanie danych biometrycznych dzieci. Skarga kasacyjna poparta przez RPD.

Decyzje

Decyzja Prezesa UODO z dnia 24 sierpnia 2020 r. DKN.5112.13.2020; Główny Geodeta Kraju; kara 100 tys.

- PUODO uznał, że GGK naruszył zasadę zgodności z prawem przetwarzania danych osobowych oraz udostępniał w sposób umyślny bez podstawy prawnej na portalu GEOPORTAL2 danych osobowych w postaci numerów ksiąg wieczystych pozyskanych z ewidencji gruntów i budynków,
- GGK w trakcie przeprowadzonego postępowania nie wskazał przepisu prawa, który stanowiłby podstawę prawną jego działania. Prezes UODO stwierdził również, że żaden z przepisów regulujących kwestie związane z działalnością Głównego Geodety Kraju nie pozwala na udostępnianie przez niego w ramach GEOPORTAL2 danych pozyskanych ze starostw,
- WSA przyznał rację PUODO w wyr. II Sa/Wa 2222/20

Decyzje

Zapraszam do kontaktu

ADW. AGNIESZKA RAPCEWICZ

<https://www.linkedin.com/in/agnieszka-rapcewicz/>

ADRES E-MAIL

agnieszka@rodowskaz.pl

TELEFON

+48 668 264 604