WIERCIŃSKI KWIECIŃSKI BAEHR

NOWE PRZEPISY DOTYCZĄCE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Agnieszka Wiercińska-Krużewska, adwokat, senior partner

21 września 2017 r.

PODSTAWOWE POJĘCIA Z ZAKRESU DANYCH OSOBOWYCH

PRZEPISY PRAWA I PRZYDATNE INFORMACJE

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych → zostanie uchylona
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
- Rozporządzenie Ogólne o Ochronie Danych nr 2016/679 z dnia 27 kwietnia 2016 r. **(w zastosowaniu od dnia 25 maja 2018 r.)**
- **Projekt nowej ustawy o ochronie danych osobowych**
- Strona eduGIODO: **https://edugiodo.giodo.gov.pl/**
- Strona GIODO – odpowiedzi na pytania: **http://www.giodo.gov.pl/266/**
- Prace nad reformą polskich przepisów: **https://mc.gov.pl/aktualnosci/rewolucja-w-systemie-ochrony-danych-osobowych**

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

DEFINICJE

Dane osobowe

- Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Osoba możliwa do zidentyfikowania

- Osoba możliwa do zidentyfikowania to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, nr identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną kulturową społeczną tożsamość osoby fizycznej.

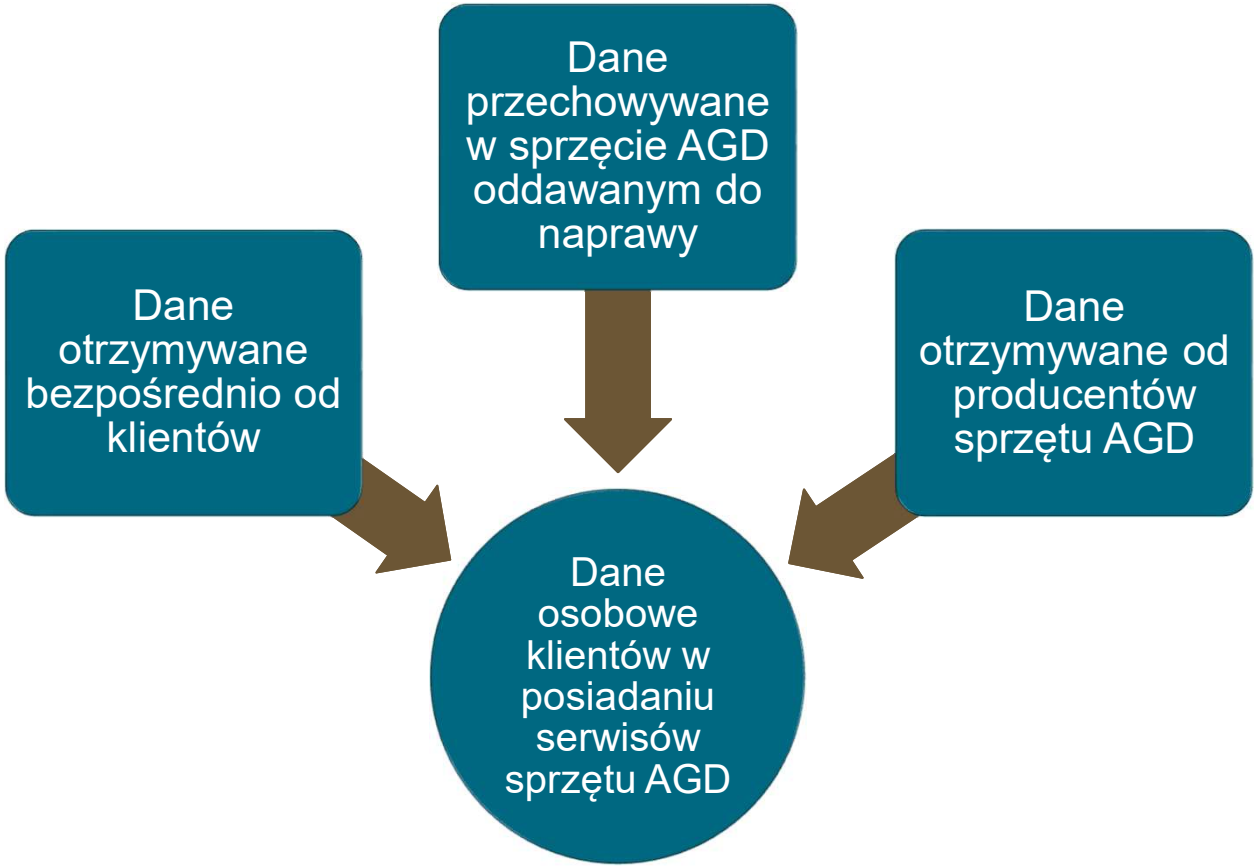
Przetwarzanie danych

- Jakiekolwiek operacje wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, przechowywanie, modyfikowanie, przeglądanie, udostępnianie, usuwanie lub niszczenie.

Administrator danych

- Podmiot decydujący o celach i środkach przetwarzania danych.

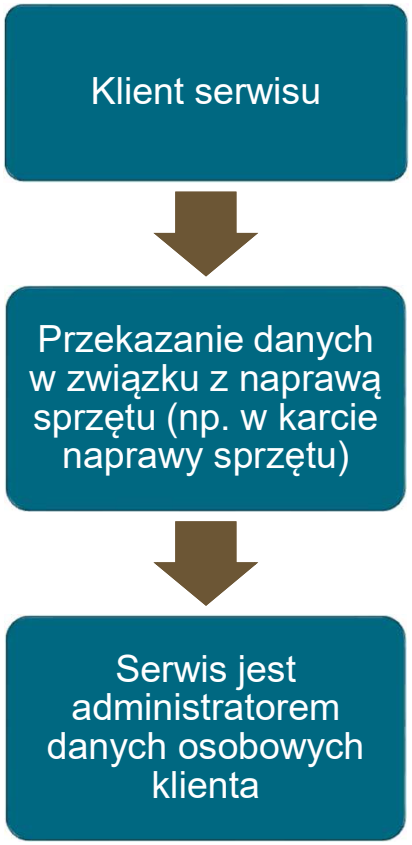
PRZYKŁADY DANYCH OSOBOWYCH



WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

DANE OSOBOWE KLIENTÓW W SERWISACH SPRZĘTU

Zbieranie danych osobowych

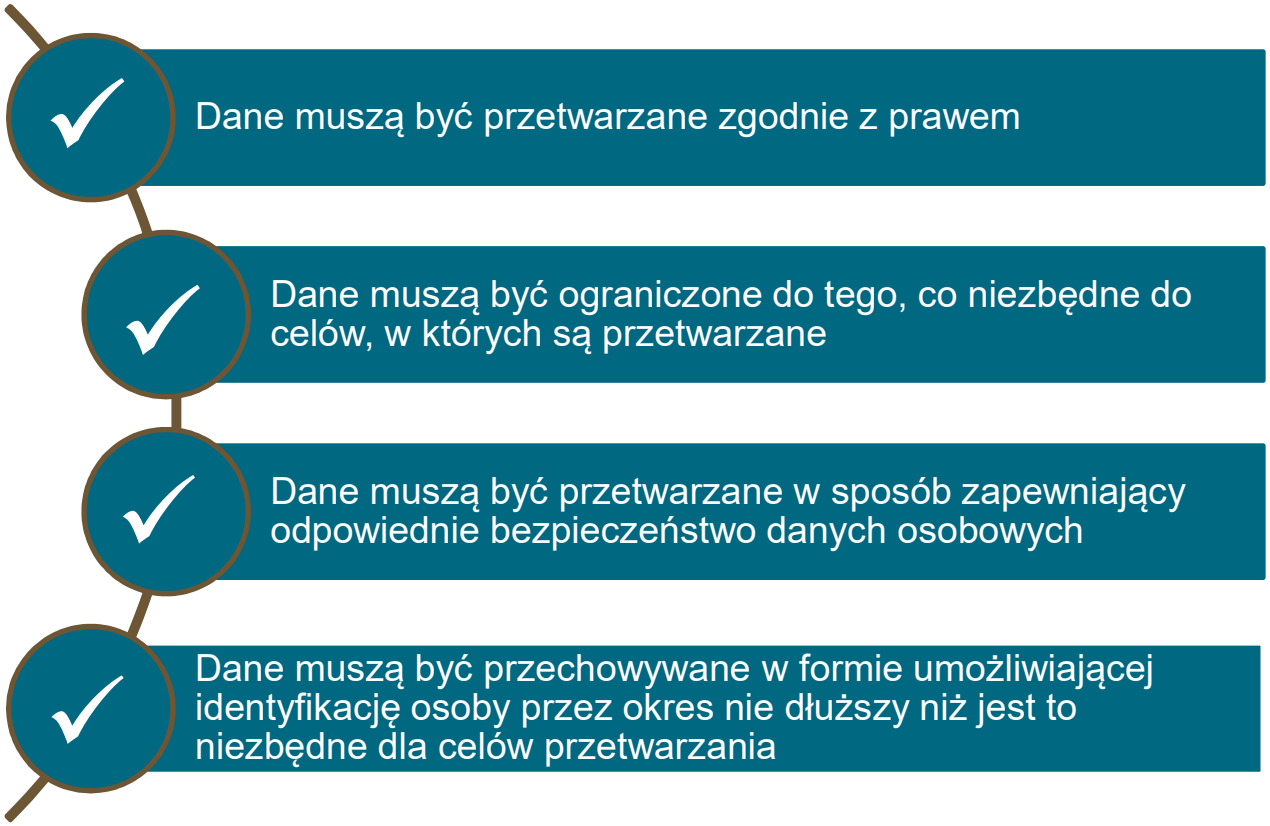


Powierzenie przetwarzania danych

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Z punktu widzenia serwisantów AGD



WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

Kiedy mogę przetwarzać dane?

- 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.
- 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.

Dla świadczenia usługi serwisowej

Np. instalacja monitoringu w firmie

- Podstawę do przetwarzania może również stanowić **zgoda** na przetwarzanie danych osobowych w jednym lub większej liczbie określonych celów, np. do reklamowania partnerów biznesowych.
- Nie jest potrzebna zgoda do **marketingu usług własnych**.

Zgoda na otrzymywanie maili – czy zostanie utrzymana?

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

ZAKRES PRZEDMIOTOWY
Kiedy RODO ma zastosowanie?

- RODO **ma zastosowanie** zarówno do przetwarzania danych klientów **w formie papierowej, jak i elektronicznej**.

- RODO **nie ma zastosowania** do przetwarzania danych w ramach działalności **osobistej lub domowej**.

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

NOWE PRZEPISY RODO:
(REWOLUCYJNA) ZMIANA PODEJŚCIA DO OCHRONY DANYCH OSOBOWYCH

(REWOLUCYJNA) ZMIANA PODEJŚCIA DO OCHRONY DANYCH

- Zgodnie z RODO żądać i przetwarzać można tylko te dane, które są **konieczne do danego celu**.
- Oznacza to, że administrator **nie można żądać danych osoby fizycznej, jeśli nie są one niezbędne do świadczenia usługi**.
- Np. nie ma uzasadnienia dla wymagania podania adresu zamieszkania, jeśli klient dostarcza i odbiera sprzęt osobiście w punkcie serwisowym.
- Dla wykonania usługi serwisowej **zbędne będzie też np. żądanie podania numeru PESEL lub wykonanie kserokopii dowodu**.
- Po wykonaniu usługi można przechowywać dane przez okres obowiązywania rękojmi (czy gwarancji) w odniesieniu do tej naprawy. Po tym czasie niezbędne jest **usunięcie danych**.

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

(REWOLUCYJNA) ZMIANA PODEJŚCIA DO OCHRONY DANYCH

Planując nową usługę, produkt lub aplikację, konieczne jest uwzględnienie ochrony danych już **w fazie projektowania**.
Np. wprowadzenie nowej aplikacji na telefon komórkowy, informującej o postępach w wykonaniu usługi, musi brać pod uwagę prywatność użytkownika – nie zbierać zbyt wielu danych, uwzględniać konieczność ich usunięcia po określonym czasie itd.

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

KONIECZNOŚĆ ZAPEWNIENIA BEZPIECZEŃSTWA DANYCH

Administrator danych odpowiada samodzielnie za wdrożenie środków bezpieczeństwa danych

Przykłady odpowiednich środków technicznych i organizacyjnych:

- Polityka bezpieczeństwa (dokument regulujący zasady zapewnienia bezpieczeństwa danych w firmie)
- Przygotowanie upoważnień do przetwarzania danych dla pracowników
- Pseudonimizacja i szyfrowanie danych
- Odpowiednie zabezpieczenie danych przechowywanych w formie papierowej (zamykanie szuflad, szaf, pomieszczeń)
- Odpowiednie zabezpieczenie systemów informatycznych (programy antywirusowe, zabezpieczenie dostępu hasłem)
- Odpowiednie zabezpieczenie sprzętu elektronicznego
- Przeszkolenie pracowników

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

ZASADY PRZETWARZANIA DANYCH: UWAGI PRAKTYCZNE

ROZWINIĘTY OBOWIĄZEK INFORMACYJNY

Co należy przekazać klientowi, uzyskując jego dane osobowe?

Konieczność zwięzłego i przejrzystego poinformowania o:

- tożsamości i danych kontaktowych administratora;
- gdy ma to zastosowanie – **danych kontaktowych inspektora ochrony danych**;
- celach przetwarzania danych osobowych i podstawie prawnej przetwarzania;
- jeśli ma to zastosowanie – prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią;
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie – **o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;**
- **okres, przez który dane osobowe będą przechowywane**, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- **uprawnieniach (w tym nowych) osoby**, której dane dotyczą;
- tym, **czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy** oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- oraz dodatkowo, jeśli dane nie są zbierane od osoby, której dotyczą: o kategoriach danych oraz o źródle pochodzenia danych.

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

NOWY OBOWIĄZEK – ZGŁASZANIE NARUSZEŃ

W przypadku naruszenia ochrony danych osobowych, np. wycieku danych w wyniku ataku na system informatyczny:

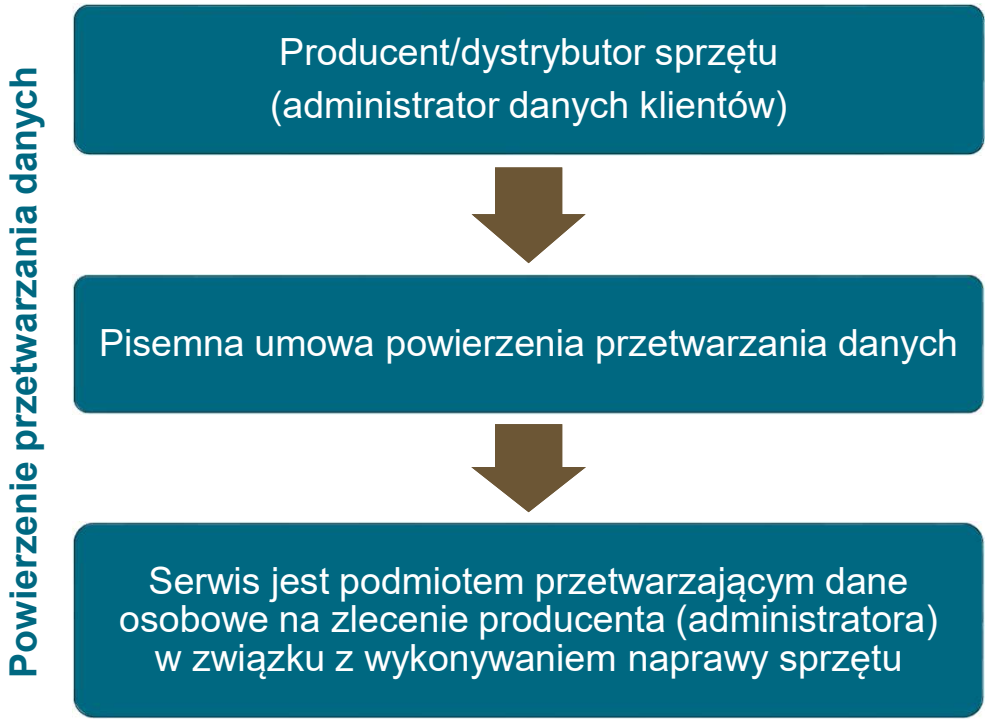
- administrator jest zobowiązany do zgłoszenia bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia – organowi nadzorczemu;
- podmiotu przetwarzający jest zobowiązany do zgłoszenia bez zbędnej zwłoki administratorowi;
- w określonych przypadkach, obowiązek zawiadomienia osób, których dane dotyczą.

Uwaga: obowiązek należy spełnić tylko, gdy naruszenie powoduje ryzyko naruszenia praw lub wolności osób np. możliwość sfałszowania tożsamości, wywołanie szkody majątkowej.

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

PODMIOT PRZETWARZAJĄCY DANE OSOBOWE (PROCESOR)

→ przetwarza dane osobowe na zlecenie administratora, na podstawie umowy, wyłącznie w celach wskazanych w tej umowie.



WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

PODMIOT PRZETWARZAJĄCY DANE OSOBOWE (PROCESOR)
Umowa powierzenia

Obligatoryjne elementy umowy

- ✓ Rodzaj powierzonych danych i kategorie osób, których dane dotyczą
- ✓ Cel przetwarzania
- ✓ Czas przetwarzania
- ✓ Warunki współpracy administratora z procesorem
- ✓ Warunki dotyczące zakończenia współpracy
- ✓ Klauzula poufności

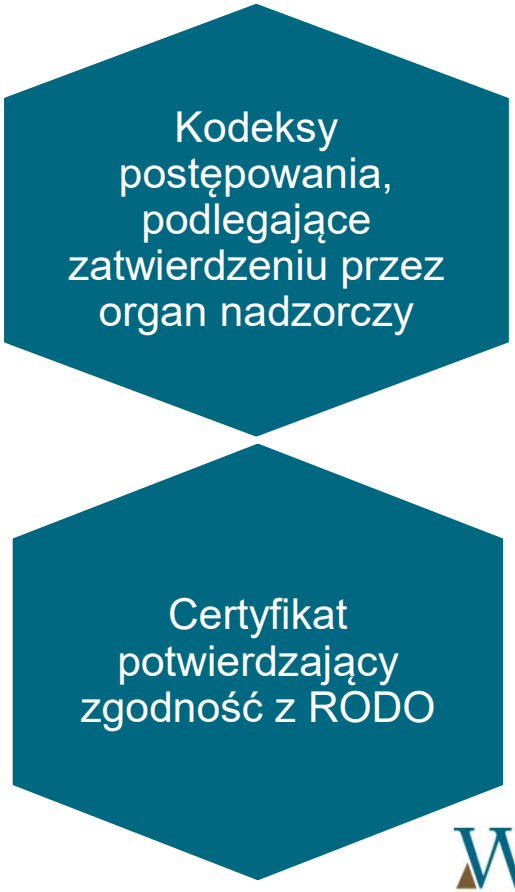
Fakultatywne elementy umowy

- Zobowiązanie procesora do zapewnienia odpowiedniego poziomu zabezpieczenia danych osobowych
- Wskazanie, czy procesor jest (i na jakich warunkach) upoważniony do dalszego powierzania przetwarzania
- Forma przekazania danych

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

NOWY MECHANIZM CERTYFIKACJI I KODEKSY POSTĘPOWANIA

- Możliwość **wykazania wywiązania się z obowiązku zapewnienia bezpieczeństwa** poprzez stosowanie zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji.
- RODO zachęca do **zrzeszania się podmiotów** w celu opracowania kodeksów.
- Kodeksy postępowania mogą **ułatwić** podmiotom z danej branży spełnienie wymagań wynikających z RODO.
- Ich opracowanie może także być **sygnałem dla klientów**, że branża uwzględnia kwestię ochrony danych w swojej działalności.
- Przedsiębiorca może uzyskać **certyfikat**, który będzie dowodem, że spełnia wymagania RODO.



WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

EGZEKWOWANIE PRZESTRZEGANIA PRZEPISÓW

NIEZALEŻNY ORGAN OCHRONY DANYCH OSOBOWYCH (ORGAN NADZORCZY)

- → ~~**Generalny Inspektor Ochrony Danych Osobowych**~~ → **Prezes Urzędu Ochrony Danych Osobowych** (prawdopodobnie, zgodnie z projektem ustawy).
- → Prezes Urzędu odpowiada za monitorowanie stosowania RODO.
- → Prezes Urzędu ma kompetencje kontrolne oraz **możliwość nakładania obowiązków i kar administracyjnych.**
- → Kara w wysokości **do 20 mln euro**, a w przypadku przedsiębiorstwa do **4%** całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (zastosowanie ma wyższa kwota).
- → Wysokość kar będzie zależała od np.
  - ✓ wagi i czasu trwania naruszenia,
  - ✓ liczby poszkodowanych,
  - ✓ umyślności naruszenia,
  - ✓ działań podjętych w celu zminimalizowania szkody,
  - ✓ poprzednich naruszeń prawa ochrony danych,
  - ✓ kategorii danych, których dotyczyło naruszenie.

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

PRZYKŁADY NARUSZEŃ

Kara do 10 mln EUR lub 2% światowego obrotu

- Niewywiązanie się z obowiązków procesora
- Niezapewnienie bezpieczeństwa przetwarzania
- Niewyznaczenie inspektora ochrony danych mimo takiego obowiązku

Kara do 20 mln EUR lub 4% światowego obrotu

- Naruszenie obowiązków informacyjnych
- Przetwarzanie danych bez podstawy prawnej
- Nieudzielenie organowi nadzoru dostępu do pomieszczeń

WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

AGNIESZKA WIERCIŃSKA-KRUŻEWSKA, LL.M.
adwokat, senior partner

agnieszka.wiercinska@wkb.pl
+48 22 201 00 00

WKB Wierciński, Kwieciński, Baehr sp. k.

ul. Polna 11
00-633 Warszawa
Tel. +48 22 201 00 00

ul. Paderewskiego 7
61-770 Poznań
Tel: +48 61 855 32 20

biuro@wkb.pl
www.wkb.pl