

RODO – szkolenie.

Radom, 26 marca 2019 roku

Aspekty prawne

Źródła prawa powszechnie obowiązującego

1. Konstytucja

2. Umowy międzynarodowe ratyfikowane za zgodą wyrażoną w ustawie

3. Ustawy

4. Ratyfikowane umowy międzynarodowe

5. Rozporządzenia

6. Akty prawa miejscowego

Przepisy prawa oświatowego

1. Ustawa - Prawo oświatowe

2. Karta Nauczyciela

3. Ustawa o systemie oświaty

4. Ustawa o systemie informacji oświatowej

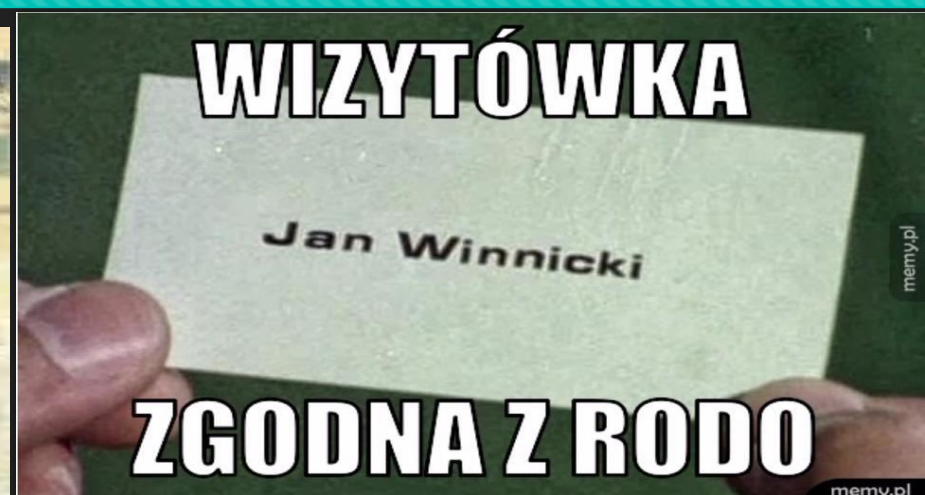
5. Ustawa o finansowaniu zadań oświatowych

6. Rozporządzenia do ww. ustaw

Czym jest RODO?

- Rozporządzenie o ochronie danych osobowych, **RODO** (ang. General Data Protection Regulation, GDPR) – rozporządzenie unijne, zawierające przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.
- Rozporządzenie to weszło w życie we wszystkich krajach członkowskich UE – 25 maja 2018 roku poprzedzone 2-letnim *vacatio legis*, był to czas na implementację, czyli dostosowanie prawa polskiego do dyrektyw UE.
- Wzmocnienie praw osób fizycznych, których dane dotyczą.
- Ujednolicenie przepisów w zakresie ochrony danych osobowych na terenie UE.
- Uatrakcyjnienie rynku UE względem państw trzecich.
- Usprawnienie wymiany informacji i procedur wewnątrzspółnotowych.
- Wyznaczenie standardów bezpieczeństwa adekwatnych do wyzwań XXI wieku.
- Nowe przepisy są stosowane bezpośrednio (zatem będą wiążące dla każdego przedsiębiorcy) i dotyczyć będą każdej firmy, która świadczy swoje produkty lub usługi osobom prywatnym (fizycznym) w całej Unii Europejskiej.

RODO MEMY



Definicja danych osobowych

Dane osobowe - oznaczają 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.

Kategorie danych osobowych

Dane biometryczne

Pozwalają na identyfikację osoby (np. wizerunek twarzy lub dane daktyloskopijne)

Skany siatkówki oka, nagrania głosu, odciski palców

Dane dotyczące zdrowia

Dotyczą zdrowia psychicznego i fizycznego człowieka, informacje o korzystaniu z usług opieki zdrowotnej

Kategorie danych osobowych.

Dane wrażliwe



Główne zasady RODO

I. Zasada legalności, rzetelności i przejrzystości przetwarzania (*lawfulness, fairness and transparency*).

II. Zasada celowości (określenia i ograniczenia celu) (*purpose limitation*).

III. Zasada adekwatności (proporcjonalności) danych (*data minimisation*).

IV. Zasada prawidłowości danych (ścisłości) (*accuracy*).

V. Zasada ograniczenia czasowego (*storage limitation*).

I. Zasada legalności, rzetelności i przejrzystości

- Wymóg, aby dane osobowe były przetwarzane zgodnie z ustawami i rozporządzeniami wydanymi na podstawie ustaw oraz uwzględniały uzasadnione interesy podmiotów danych, a także były przejrzyste dla podmiotu danych.
- Naruszeniem zasady rzetelności jest np. włączenie klauzuli zgody na marketing do pozostałych klauzul, tak aby pozbawić klienta możliwości odmowy zgody, do której jest uprawniony.
- Brytyjski Data Protection Tribunal (Sąd Ochrony Danych Osobowych) w orzeczeniu z 1998 r. w sprawie British Gas Limited vs. Data Protection Registrar (DA983/49/2; 1998 Info. T.L.R. 393) Sąd uznał za naruszenie zasady rzetelności udostępnianie danych osobowych odbiorców gazu – konsumentów, przez firmę British Gas Trading Limited innym podmiotom dla ich celów marketingowych, bez wyraźnej zgody osób, których dane dotyczą, skoro administrator był monopolistą w brytyjskim sektorze gazownictwa.

II. Zasada celowości (określenia i ograniczenia celu)

- Ograniczenie gromadzenia danych do określonych celów oraz zakaz poddawania danych dalszemu przetwarzaniu sprzecznemu z tymi celami.
- Administrator musi sprecyzować cel przetwarzania danych przed rozpoczęciem ich przetwarzania.
- Zasada celowości wiąże zarówno administratora danych, który je pierwotnie zebrał, jak i administratora, któremu dane zostały następnie udostępnione.
- Możemy wyróżnić cele spreczne lub niesprzeczne z pierwotnymi założeniami przetwarzania.
- Np. wykorzystywanie do celów marketingowych produktów administratora wobec jego pracowników. Dane zebrane do celów zatrudnienia nie powinny być wykorzystywane do celów handlowych bez spełnienia odpowiednich warunków, a więc tylko dlatego, że znajdują się w bazie administratora.
- Celami niesprzecznymi z pierwotnym celem przetwarzania są cele: archiwizacyjne, związane z interesem publicznym, badania naukowe i historyczne oraz statystyczne.

III. Zasada adekwatności (proporcjonalności) danych

- Obowiązek zapewnienia, aby zakres przetwarzanych danych był ograniczony, pod względem ilości i treści, do zakresu niezbędnego do osiągnięcia celów ich przetwarzania.
- To czy zakres zbieranych danych i dalej przetwarzanych danych osobowych jest proporcjonalny do celu ich przetwarzania należy ocenić indywidualnie w poszczególnych przypadkach.
- Ilustracja zasady adekwatności to różnicowanie danych zbieranych przez bank, np. w celu przyjęcia lokaty i w celu udzielenia kredytu. Kredytowanie jest uzależnione od zdolności kredytowej wnioskodawcy, której ocena wymaga zebrania i analizy danych osobowych w znacznym zakresie, natomiast przyjęcie lokaty nie wymaga dokonania takiej oceny. Brak różnicowania zakresu przetwarzania danych **byłby sprzeczny** z zasadą adekwatności.
- Realizacja zasady adekwatności art. 33 ust. 2 SysUbSpołU, zgodnie z którym jeżeli osoba ubezpieczona nie ma numeru PESEL, nie podała go lub prawidłowość podanego numeru budzi wątpliwości, konto ubezpieczonego oznacza się numerem NIP, jeżeli nie posiada również tego numeru – serią i numerem dowodu osobistego albo paszportu. Przepis wyklucza więc łączne stosowanie danych osobowych należących do różnych kategorii.

IV. Zasada prawidłowości danych (ścisłości)

- Wymóg zapewnienia zgodności ze stanem rzeczywistym, kompletności i aktualności danych.
- Art. 5 ust 1 RODO nakazuje podjęcie wszelkich uzasadnionych działań dla niezwłocznego usunięcia lub poprawienia danych nieprawidłowych lub niekompletnych, ale nie oznacza to aktywnego, stałego monitorowania prawidłowości i aktualności wszystkich danych w zbiorach z inicjatywy administratora.
- Administrator nie dysponuje środkami, aby monitorować np. zmiany miejsca zamieszkania czy stanu cywilnego lub rodzinnego.
- Przykład: kredytobiorczyni nie może domagać się korygowania w pierwotnej umowie kredytowej nazwiska, które następnie zmieniła po wyjściu za mąż.
- Wyjątek: konieczność monitorowania i aktualizowania danych przez administratora to informacje o zadłużeniu klienta w banku w rejestrach kredytowych (Biuro Informacji Kredytowej S.A., Bankowy Rejestr). Służy to ocenie zdolności i wiarygodności kredytowej klienta.

V. Zasada ograniczenia czasowego

- Zakaz przechowywania danych w formie umożliwiającej identyfikację osób przez czas dłuższy niż niezbędny do celów ich przetwarzania.
- Ściśle powiązana z zasadą celowości.
- Informacje kadrowo-płacowe (dokumentacja pracownicza dotycząca okresów zatrudnienia i wynagrodzenia za pracę, będąca podstawą ustalenia emerytury lub renty) są obligatoryjnie archiwizowane przez kilkadziesiąt lat.
- Inne dane pracowników np. zbierane w ramach monitoringu prowadzonego przez pracodawcę (GPS w samochodach służbowych, historia odwiedzanych stron internetowych) należy przechowywać jedynie przez krótki czas, adekwatny do uzasadnionych zdefiniowanych przez pracodawcę celów.
- Z chwilą spłaty kredytu, zamknięcia rachunku bankowego – osiągnięcia celu przetwarzania danych znika podstawa prawna do przetwarzania danych posiadaczy zamkniętych rachunków.
- Nie zawsze należy dokonać brakowania (niszczenia) dokumentów, aby spełnić wymogi rozporządzenia wystarczy dokonać pseudonimizacji. Dane podlegające usunięciu muszą zostać usunięte bezpowrotnie, bez możliwości ich odzyskania np. za pomocą aplikacji.

Administrator – szkoła reprezentowana przez dyrektora

OBOWIĄZKI:

- zabezpieczenie danych osobowych,
- nadzór nad bezpieczeństwem danych,
- powołanie IOD,
- audyty wewnętrzne (przez IOD),
- umowa przetwarzania (np. w kwestii wycieków),
- rejestr czynności przetwarzania danych osobowych,
- zgłaszanie naruszeń ochrony danych osobowych,
- obowiązek informacyjny.

Obowiązek informacyjny

Na przykładzie zaproszenia na uroczystości i wydarzenia szkolne:

- Warstwowe przekazywanie informacji:
- wskazanie osobie najistotniejszych elementów (np. kto jest administratorem, w jakim celu dane są przetwarzane), odsyłając jednocześnie do pełnej treści obowiązku informacyjnego, np. na konkretnej stronie internetowej.

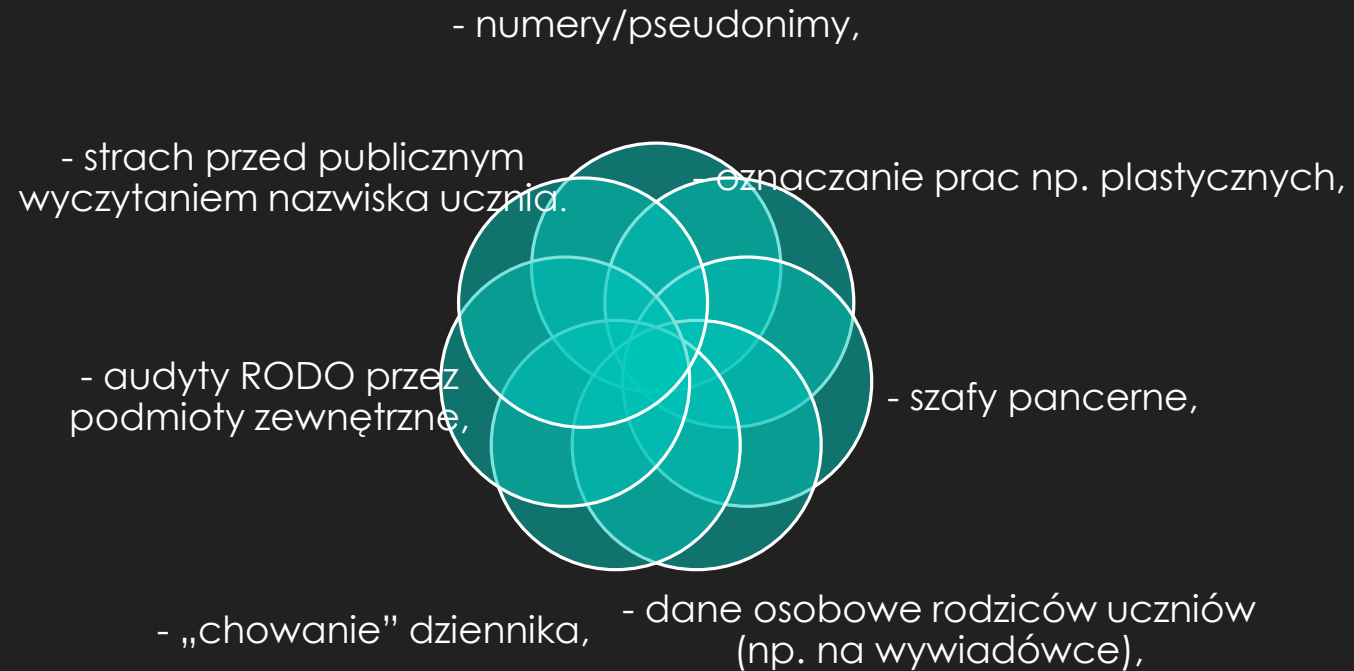
Publikacja list uczniów przyjętych do szkoły

Wynika to wprost z art. 157 ust. 2 pkt 2 i art. 158 ust. 1, 3 i 4 ustawy Prawo oświatowe. Szkoły i placówki zostały więc zobowiązane do podania do publicznej wiadomości poprzez umieszczenie w widocznym miejscu w siedzibie danej placówki. Nie w Internecie!

Udzielanie informacji o uczniu osobom trzecim.

- Omówienie z naciskiem na obligatoryjne wskazanie podstawy prawnej.
- Sytuacje nagłe: art. 9 ust. 2 lit. c RODO: przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

Absurdy RODO



Inspektor Ochrony Danych – IOD

Powołanie Inspektora

- Zgodnie z art. 10 ust. 1 UODO podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. Natomiast stosownie do art. 10 ust. 5 n.u.o.d.o. w przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne każdy z tych podmiotów dokonuje zawiadomienia.
- Zawiadomienie sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Co ważne, niezależnie od obowiązku wskazania danych kontaktowych IOD w klauzuli informacyjnej (art. 13–14 RODO) podmiot, który wyznaczył inspektora, udostępnia jego dane, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Kto może zostać Inspektorem?

- Zgodnie z 37 ust. 5 RODO IOD powinien być wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.
- Kwestię tę precyzuje motyw 97 RODO, zgodnie z którym niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający.
- Kwalifikacje IOD mają zapewnić, aby wypełniał on swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Kwalifikacje IOD

Zgodnie z opinią Grupy Roboczej Art. 29, oceniając wymagany poziom kwalifikacji, należy uwzględnić następujące elementy:

1. znajomość krajowych i europejskich przepisów i praktyk w zakresie ochrony danych;
2. zrozumienie przeprowadzanych operacji przetwarzania;
3. zrozumienie technologii informacyjnych i bezpieczeństwa danych;
4. znajomość kontekstu biznesowego i organizacji administratora (procesora);
5. zdolność promowania kultury ochrony danych w organizacji.

Kwalifikacje IOD c.d.

- IOD może być członkiem personelu administratora lub procesora, może także wykonywać zadania z zewnątrz, na podstawie umowy o świadczenie usług (art. 37 ust. 6 RODO). To ostateczne stwierdzenie należy interpretować w ten sposób, że funkcję IOD można wykonywać m.in. na podstawie umowy o świadczenie usług zawieranej z konkretną osobą fizyczną (przyszły IOD) lub jednostką organizacyjną (wyposażoną w zdolność prawną).
- W tym drugim przypadku jednostka organizacyjna desygnuje konkretną osobę fizyczną do świadczenia usługi IOD u administratora (procesora) 8. Tacy inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny (motyw 97 RODO).

Zadania obligatoryjne IOD

- Zadania obligatoryjne IOD:
- odgrywanie roli punktu kontaktowego dla podmiotów danych (osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO – art. 38 ust. 4 RODO);
- informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów UE lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie; w tym zakresie IOD występuje w potrójnej roli: wskazuje obowiązki, doradza co do sposobu ich wykonania, a następnie ocenia poprawność wykonania tych obowiązków;

Zadania obligatoryjne IOD

- monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Zadania fakultatywne IOD

RODO nie wyklucza realizacji przez IOD szerszego katalogu zadań z zakresu ochrony danych (np. we współpracy z jego zespołem). Ten szerszy zakres zadań może dotyczyć:

zadań nałożonych wprost przepisami na administratora danych lub procesora (np. prowadzenie rejestru czynności przetwarzania danych);

zadań realizowanych przez administratora w ramach zasady rozliczalności (np. prowadzenie rejestru umów powierzenia danych).

Wykluczone zadania fakultatywne

- Chociaż RODO nie wyklucza możliwości polecenia IOD wykonywania innych (niż obligatoryjne zadania) czynności, to wątpliwości mogą dotyczyć następujących zadań:
- przekazywania odpowiedzi na żądanie praw podmiotów danych (np. sporządzenie pisma w imieniu administratora danych);
- zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;
- zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu;
- przeprowadzania oceny skutków dla ochrony danych (a nie tylko konsultowania tej oceny);
- W doktrynie wyrażono pogląd wykluczający wykonywanie przez IOD jakichkolwiek zadań (wymogów) wyraźnie nałożonych na administratora. Jak się wskazuje w doktrynie, na gruncie RODO wyłączona zatem będzie możliwość przeniesienia na IOD ciężaru podejmowania decyzji, który został nałożony wprost na administratora lub procesora. Wydaje się, iż jest to zbyt daleko idący pogląd. Przykładowo, Grupa Robocza Art. 29 przyjmuje dopuszczalność upoważnienia IOD do prowadzenia rejestru czynności przetwarzania (obowiązku administratora danych). Natomiast wykluczyć należy możliwość nałożenia na IOD obowiązków, które mogłyby podważyć jego niezależną pozycję, w tym także poprzez włączenie go w proces decyzyjny – o celach i środkach przetwarzania danych.

Klauzule informacyjne

- Zakresy informacji, które administrator jest obowiązany przekazać podmiotowi danych, gdy zbiera je bezpośrednio od niego, np. podczas obsługi w oddziale czy za pośrednictwem strony internetowej, oraz gdy zebrał je z innego źródła;
- nazwę albo nazwisko oraz dane kontaktowe administratora, a także jego przedstawiciela, jeżeli istnieje;
- dane kontaktowe administratora bezpieczeństwa informacji (inspektora ochrony danych, data protection officer), jeżeli został powołany;
- zakładane cele przetwarzania danych oraz jego podstawę prawną;
- sprecyzowanie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, jeżeli ich realizacja została wskazana jako podstawa przetwarzania; odbiorców lub kategorie odbiorców danych;

Klauzule informacyjne c.d.

- informację o zamiarze transferu danych osobowych do odbiorcy w państwie trzecim lub organizacji międzynarodowej, jeżeli administrator to planuje; również o poziomie ochrony danych po transferze poza UE, a więc czy Komisja Europejska uznała poziom ochrony w państwie docelowym za adekwatny do standardów UE, a jeżeli nie wydała takiej decyzji – m.in. informację o gwarancjach ochrony danych, które zapewnia po transferze sam eksporter (należą do nich m.in. BCR i standardowe klauzule umowne) oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
- okres, przez który dane osobowe będą przechowywane, a gdy jego sprecyzowanie nie jest możliwe – kryteria ustalania tego okresu;
- informację o prawie podmiotu danych do dostępu do nich, korekty, usunięcia, ograniczenia ich przetwarzania, sprzeciwu wobec ich przetwarzania oraz o prawie do przenoszenia danych;
- jeżeli podstawą przetwarzania danych zwykłych lub wrażliwych jest zgoda podmiotu danych – informację o prawie do cofnięcia zgody w dowolnym momencie;
- informację o prawie wniesienia skargi do organu nadzorczego;
- informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla podmiotu danych;

Zgłoszenie naruszenia ochrony danych osobowych

Co to jest naruszenie ochrony danych osobowych?

Do naruszenia ochrony danych osobowych dochodzi, gdy:

- dotyczy danych przesyłanych, przechowywanych lub przetwarzanych przez podmiot, którego dotyczy naruszenie
- jego skutkiem jest zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych
- jest skutkiem złamania zasad bezpieczeństwa danych

Zgłoszenie naruszenia danych osobowych c.d.

Przykłady naruszenia danych osobowych:

- poufności – np. gdy twój pracownik wyśle przypadkowo bazę danych osobowych klientów do osoby postronnej lub niewłaściwego działu firmy,
- dostępności – np. gdy zaginie pendrive z bazą danych klientów,
- integralności – np. gdy pracownik dla żartu zmieni nazwiska,

Kto może powiadomić o naruszeniu ochrony danych osobowych

Zgłoszenia o naruszeniu ochrony danych osobowych dokonuje:

- administrator – przedsiębiorca lub jednostka publiczna przetwarzająca dane osobowe,
- pełnomocnik administratora.

Dane kontaktowe

- Dawid Kostecki, Mateusz Sarnat 792 033 019
adwokat.sarnat@gmail.com

Dziękujemy za uwagę. ☺