Urząd Ochrony Danych Osobowych

NARUSZENIA OCHRONY DANYCH OSOBOWYCH

WYTYCZNE EUROPEJSKIEJ RADY OCHRONY DANYCH

Monika Adamczyk
Zespół Analiz i Strategii
Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

OCHRONA DANYCH OSOBOWYCH

Urząd
Ochrony
Danych
Osobowych

OBOWIĄZKI ADMINISTRATORA

- Dla przetwarzania danych osobowych muszą być zastosowane takie środki techniczne i organizacyjne aby zapewnić :
  - przetwarzanie zgodnie z zasadami RODO
  - bezpieczeństwo danych, w tym ochronę przed naruszeniem poufności, integralności i dostępności danych
  - stwierdzenie tak szybko jak tylko jest to możliwe czy doszło do naruszenia ochrony danych osobowych

ŚRODKI TECHNICZNE I ORGANIZACYJNE

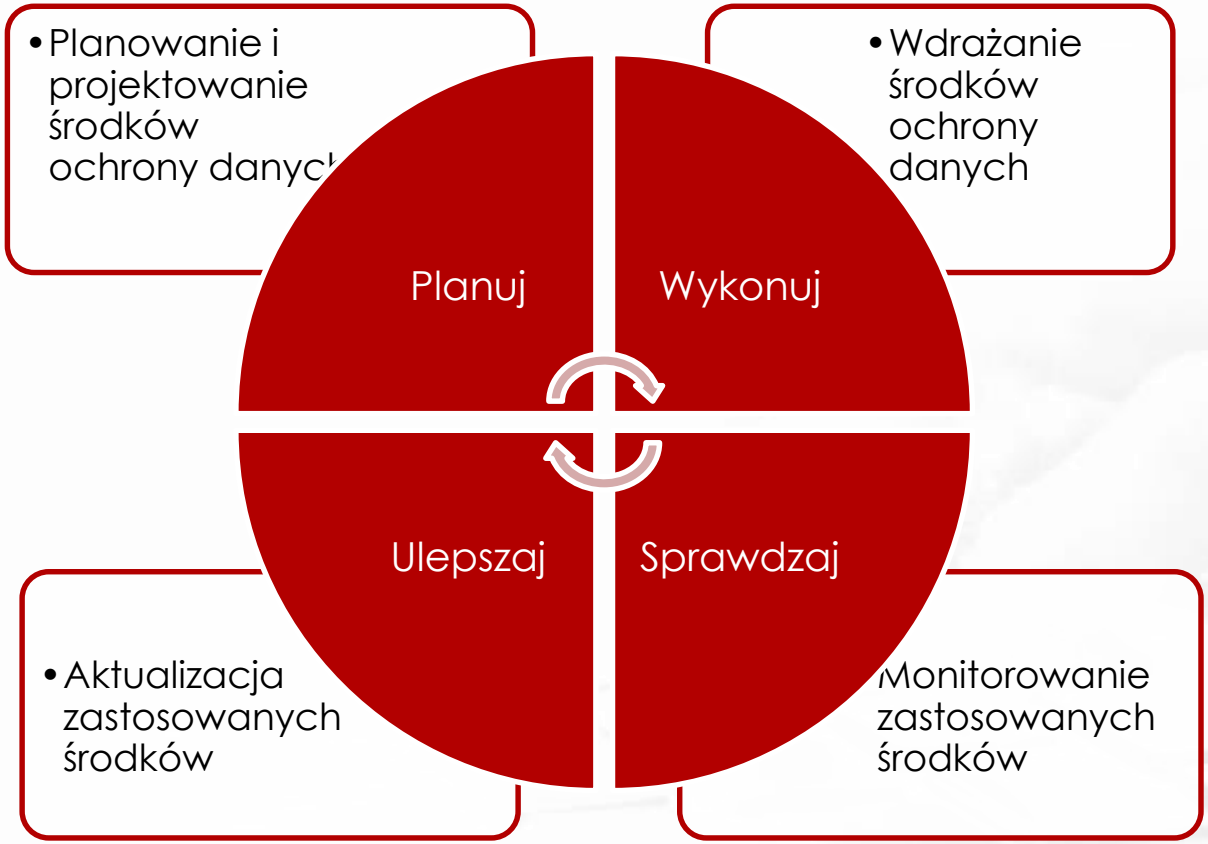
- Polityki i procedury definiujące i regulujące cele i sposoby przetwarzania danych (np. dopuszczalne zasady ich wykorzystywania lub procedury reagowania na incydenty naruszenia)
- Technologiczne (sprzętowe i oprogramowania) rozwiązania wykorzystywane w celu ochrony informacji i systemów informatycznych
- Ludzie świadomi swoich ról i obowiązków oraz przestrzegający przyjęte zasady przetwarzania danych i sposoby zabezpieczeń

BEZPIECZEŃSTWO DANYCH

- Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
- Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu bezpieczeństwa (fizycznego lub technicznego)
- Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

Urząd Ochrony Danych Osobowych

BEZPIECZEŃSTWO DANYCH TO CIĄGŁY PROCESS



Urząd Ochrony Danych Osobowych

NARUSZENIE OCHRONY DANYCH

Urząd
Ochrony
Danych
Osobowych

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

- Incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
- Niemożność zapewnienia zgodności z zasadami dotyczącymi przetwarzania danych osobowych ustanowionymi w RODO

Urząd Ochrony Danych Osobowych

INCYDENT BEZPIECZEŃSTWA

- Losowe zewnętrzne (np. pożar prowadzący do utraty dokumentów papierowych zawierających dane osobowe) lub wewnętrzne (np. zgubienie pendrive, na którym były zapisane dane osobowe).
- O charakterze umyślnym, zarówno zewnętrzne (np. atak, którego skutkiem jest nieuprawniony dostęp do systemów informatycznych) jak i wewnętrzne (np. kradzież dokumentacji z danymi przez pracownika)

RODZAJE NARUSZEŃ

- Naruszenie poufności danych – dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych
- Naruszenie integralności danych - dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych
- Naruszenie dostępności danych – dochodzi do przypadkowej lub nieuprawnionej utraty dostępu do danych osobowych lub zniszczenia danych osobowych

WYSTĄPIENIE NARUSZENIA

Stwierdzenie wystąpienia naruszenia następuje w momencie, w którym administrator uzyskuje wystarczającą dozą pewności, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do naruszenia ochrony danych osobowych

Urząd Ochrony Danych Osobowych

PRZYKŁAD NARUSZENIA OCHRONY DANYCH

Cztery laptopy zostały skradzione ze szpitala. Zawierały one dane dotyczące zdrowia i przyznawanej pomocy finansowej oraz inne dane osobowe dotyczące 2050 dzieci. Dane na laptopach nie były zaszyfrowane.

Urząd Ochrony Danych Osobowych

KONSEKWENCJE NARUSZENIA

- Naruszenie poufności danych

  Rodzice krytycznie chorych dzieci mogą być celem osób, które chcą czerpać korzyści z ich słabości (np. szarlatani)
- Naruszenie integralności danych

  Utracone dane mogą zakłócić leczenie co może doprowadzić do nasilenia się lub nawrotu choroby
- Naruszenie dostępności danych

  Może nastąpić nieuzasadnione opóźnienie przyznania pomocy finansowej lub jej odmowa, mająca negatywne skutki finansowe dla rodzin leczonych dzieci

ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH

Urząd
Ochrony
Danych
Osobowych

ADMINISTRATOR DANYCH

- Obowiązek
  - Zgłoszenia naruszenia danych osobowych właściwemu krajowemu organowi nadzorczemu

    Współadministratorzy uzgadniają, który z nich będzie zajmował się realizacją tych obowiązków

  - Poinformowania o naruszeniu danych osobowych osoby fizyczne

PODMIOT PRZETWARZAJĄCY

- Administrator zawiera porozumienie z podmiotami przetwarzającymi, zobowiązujące ich do zgłaszania zaistniałych u nich naruszeń i określające zasady tych zgłoszeń

- Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych ma obowiązek zgłosić je administratorowi bez zbędnej zwłoki

KIEDY NALEŻY ZGŁOSIĆ NARUSZENIE

- Jeżeli naruszenie danych może spowodować ryzyko naruszenia praw i wolności osób fizycznych – do organu nadzorczego - nie później niż w ciągu 72 godzin od stwierdzenia naruszenia
- Jeżeli naruszenie ochrony może spowodować wysokie ryzyko naruszenia praw lub wolności – poinformowanie osoby fizyczne – tak szybko jak tylko możliwe

Urząd Ochrony Danych Osobowych

CO POWINNO ZAWIERAĆ ZGŁOSZENIE

- Opis naruszenia oraz kategorie osób i ich przybliżoną liczbę oraz kategorie danych osobowych i ich przybliżoną liczbę
- Dane kontaktowe IOD lub punktu kontaktowego od którego można dostać więcej informacji
- Opis możliwych konsekwencji naruszenia
- Opis zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu oraz zminimalizowania jego negatywnych skutków

KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ

- Obejmują różnego rodzaju osoby fizyczne, na których dane osobowe naruszenie wywarło wpływ, np.:
  - dzieci i przedstawiciele innych grup szczególnie wrażliwych
  - osoby niepełnosprawne
  - pracownicy
  - klienci

Urząd Ochrony Danych Osobowych

KATEGORIE WPISÓW DANYCH

- Mogą odnosić się do poszczególnych rodzajów wpisów, które administrator może przetwarzać np.:
  - dane dotyczące zdrowia
  - dane dotyczące wykształcenia
  - informacje z dziedziny opieki społecznej
  - szczegółowe informacje finansowe
  - numery rachunków bankowych
  - numery paszportów

MOŻLIWE KONSEKWENCJE NARUSZENIA OCHRONY DANYCH

- Określnie ryzyka wyrządzenia określonych szkód w rezultacie naruszenia np.:
  - kradzież tożsamości
  - oszustwo
  - strata finansowa
  - ryzyko naruszenia poufności danych chronionych tajemnicą zawodową

Urząd Ochrony Danych Osobowych

SUKCESYWNE DOKONYWANIE ZGŁOSZENIA NARUSZENIA

- Brak dostępu do szczegółowych informacji nie powinien stanowić przeszkody dla terminowego zgłoszenia naruszenia
- Jeśli fakt wystąpienia naruszenia nie wzbudza żadnych wątpliwości, ale jego skala nie jest jeszcze znana, sukcesywne dokonywanie zgłoszenia jest dozwolone
- Różne rodzaje naruszenia mogą wiązać się z koniecznością przekazania dodatkowych informacji, aby w pełni wyjaśnić okoliczności danej sprawy

ZGŁOSZENIE DOKONANE Z OPÓŹNIENIEM

- Administrator nie zawsze może być w stanie zgłosić naruszenie w wyznaczonym terminie
- Dokonanie zgłoszenia z opóźnieniem może być w niektórych przypadkach dopuszczalne
- Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin administrator musi dołączyć wyjaśnienie przyczyn opóźnienia

Urząd Ochrony Danych Osobowych

ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ

Urząd
Ochrony
Danych
Osobowych

INFORMOWANIE OSÓB FIZYCZNYCH

- Zawiadomienie ma na celu przede wszystkim dostarczenie szczegółowych informacji na temat działań zapobiegawczych, które osoby fizyczne powinny podjąć, aby uchronić się przed wszelkimi negatywnymi skutkami naruszenia

KONTAKT Z OSOBAMI FIZYCZNYMI

- Zawiadomienie o naruszeniu musi być jasne i przejrzyste
- Osoby, których dane dotyczą, należy zawiadomić o naruszeniu bezpośrednio
- W przypadku niewspółmiernie dużego wysiłku, dopuszcza się wydanie publicznego komunikatu lub zastosowanie podobnego środka - osoby muszą być poinformowane w równie skuteczny sposób jak bezpośrednio

INFORMACJE, KTÓRYCH NALEŻY UDZIELIĆ OSOBIE FIZYCZNEJ

- Opis naruszenia
- Dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego
- Opis możliwych konsekwencji naruszenia
- Opis zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu oraz zminimalizowania jego ewentualnych negatywnych skutków
- W stosownych przypadkach - szczegółowe zalecenia na temat sposobów ochrony przed potencjalnymi niekorzystnymi skutkami naruszenia

KIEDY ZAWIADOMIENIE NIE JEST KONIECZNE

- Administrator zastosował przed wystąpieniem naruszenia odpowiednie techniczne i organizacyjne środki w celu ochrony danych osobowych, w szczególności środki uniemożliwiające odczyt danych osobom, które nie są uprawnione do dostępu do tych danych
- Natychmiast po wystąpieniu naruszenia administrator podjął działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej
- Skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku

OCENA RYZYKA I WYSOKIEGO RYZYKA

Urząd
Ochrony
Danych
Osobowych

RYZYKO JAKO POWÓD ZGŁOSZENIA

- Oszacowanie ryzyka jest konieczne aby móc:
  - ustalić, czy w danym przypadku zastosowanie ma wymóg zgłoszenia naruszenia do organu nadzorczego
  - ustalić, czy wymagane jest zawiadomienie osoby fizyczne o naruszeniu (tylko w przypadku wysokiego ryzyko naruszenia praw i wolności tych osób)
  - określić działania, które należy podjąć, aby zaradzić naruszeniu i zminimalizować jego konsekwencje

CZYNIKI, MAJĄCE WPŁYW NA ANALIZĘ RYZYKA

- Rodzaj naruszenia
- Rodzaj danych osobowych
- Łatwość zidentyfikowania, kim są osoby, których dane dotyczą
- Liczba osób fizycznych, na które naruszenie wywiera wpływ
- Jakie są możliwe konsekwencje i ich waga dla osób, których dane dotyczą
- Cechy szczególne osób fizycznych
- Cechy szczególne administratora danych

NARUSZENIA O CHARAKTERZE TRANSGRANICZNYM

Urząd
Ochrony
Danych
Osobowych

NARUSZENIA O CHARAKTERZE TRANSGRANICZNYM

- Naruszenie może wywierać wpływ na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim
- Administrator powinien zgłosić je właściwemu organowi nadzorczemu
  - Organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy

NARUSZENIA W JEDNOSTKACH ORGANIZACYJNYCH SPOZA UE

- Czynności przetwarzania wiążą się z:
  - oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty
  - monitorowaniem zachowania osób, o ile do zachowania tego dochodzi w Unii
- Jednostka organizacyjna jest w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego

Urząd Ochrony Danych Osobowych

ROZLICZALNOŚĆ I PROWADZENIE DOKUMENTACJI

Urząd
Ochrony
Danych
Osobowych

ROZLICZALNOŚĆ ADMINSTRATORA

- Administrator musi być w stanie wykazać przestrzeganie przepisów ochrony danych i zaistniałych naruszeń
- Dokumentacja prowadzona w tym celu musi umożliwić organowi nadzorczemu weryfikację przestrzegania przepisów o ochronie danych oraz konkretnych działań podjętych przez administratora podczas naruszeń

JAK PRZYGOTOWAĆ SIĘ DO ZGŁOSZEŃ

- Przygotowanie planu reagowania na naruszenia danych oraz procedur powiadamiania / informowania o naruszeniach
- Identyfikacja osób odpowiedzialnych za zarządzanie naruszeniami ochrony danych i przydzielenie im odpowiednich ról i obowiązków
- Przygotowanie procedur postępowania w celu ustalenia czy doszło do naruszenia
- Ustalenie struktury dokumentacji naruszeń danych
- Szkolenia i budowanie świadomości

Urząd Ochrony Danych Osobowych

DOKUMENTOWANIE NARUSZEŃ

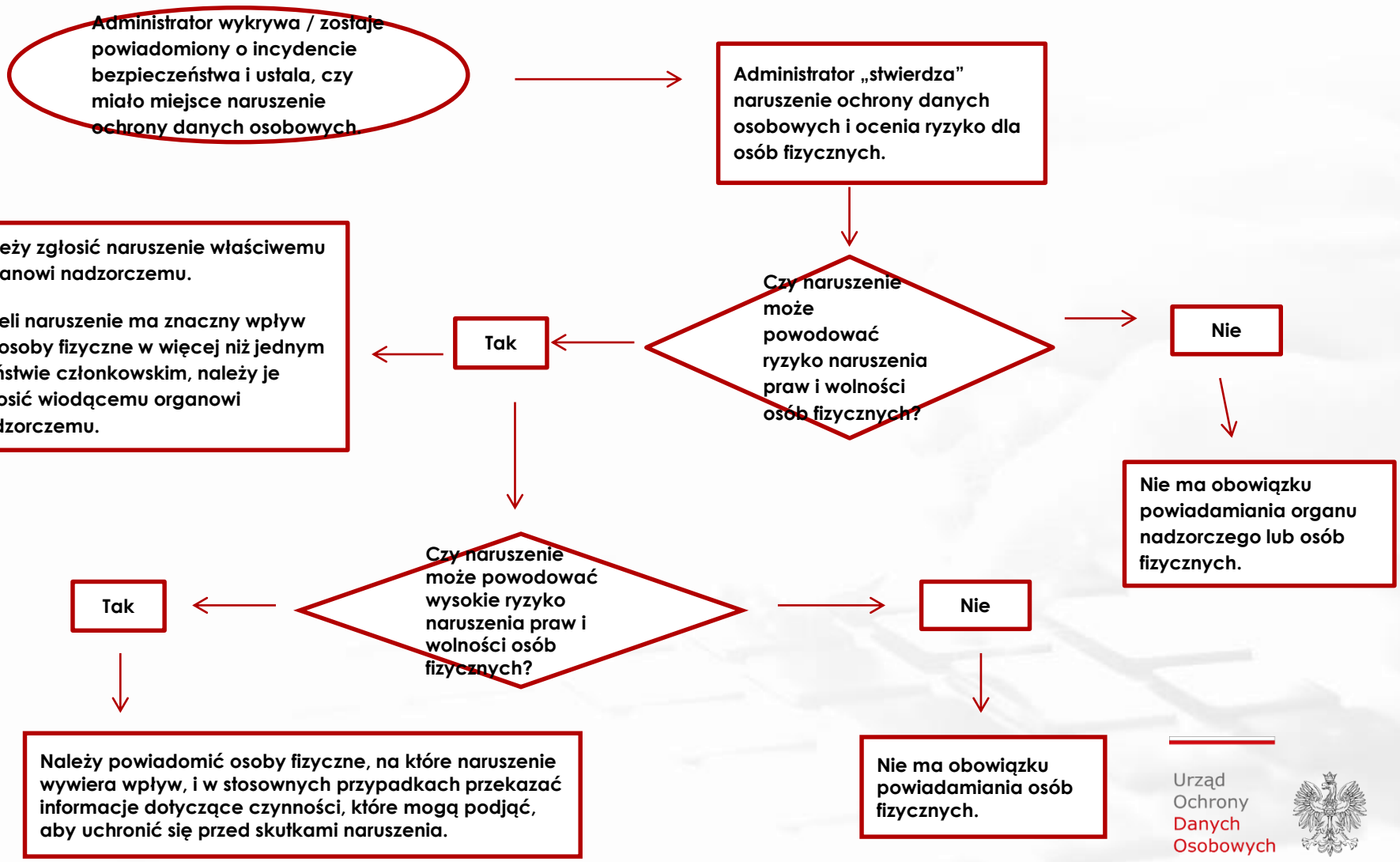
- Wewnętrzny rejestr naruszeń musi być prowadzony bez względu na to, czy muszą być one zgłoszone i musi zawierać
  - okoliczności naruszenia ochrony danych osobowych
  - przyczyny zgłoszenia opóźnienia (jeśli jest to stosowne)
  - potencjalne skutki naruszenia dla osób fizycznych
  - podjęte działania zaradcze
  - uzasadnienia podjętych decyzji
  - informacje przekazane osobom fizycznym

ROLA INSPEKTORA DANYCH

- Przekazuje zalecenia oraz wskazówki dotyczące wykrywania i raportowania naruszeń ochrony danych
- Wspiera w przygotowaniu struktury dokumentacji naruszeń oraz ewentualnie zarządza nią
- Monitoruje przestrzeganie przyjętych zasad i procedur
- Przekazuje zalecenia w zakresie przeprowadzania analizy ryzyka i oceny skutków
- Jest punktem kontaktowym dla organu nadzorczego oraz osób, których dane dotyczą

Urząd Ochrony Danych Osobowych

PODSUMOWANIE



Urząd Ochrony Danych Osobowych

źródło: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679

PRZYDATNE MATERIAŁY

- Europejska Rady Ochrony Danych, Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (dostępne też w wersji polskiej)

  https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
- ENISA, Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych (po angielsku)

  https://www.enisa.europa.eu/publications/dbn-severity
- Obowiązki związane z naruszeniami ochrony danych osobowych (materiały na stronie UODO)

  https://uodo.gov.pl/pl/134

Urząd Ochrony Danych Osobowych

Urząd
Ochrony
Danych
Osobowych

DZIĘKUJĘ ZA UWAGĘ

PYTANIA?

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl