Ministerstwo
Cyfryzacji

RODO

WPROWADZENIE W PROBLEMATYKĘ

DNIA 25 MAJA 2018 ROKU WE WSZYSTKICH KRAJACH NALEŻĄCYCH DO UNII EUROPEJSKIEJ ZACZNIE BYĆ STOSOWANE OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH 2016/679 (RODO)

TRZY GŁÓWNE ZAŁOŻENIA UNIJNEJ REFORMY OCHRONY DANYCH

- Stworzenie uniwersalnych ram prawnych zapewniających skuteczną ochronę danych osobowych mimo stałego rozwoju nowych technologii (chmura obliczeniowa, profilowanie, rozwój aplikacji mobilnych itp.);
- Zapewnienie ochrony danych osobowych na każdym etapie projektowania rozwiązania;
- Wprowadzenie efektywnych mechanizmów współpracy w sprawach ochrony danych osobowych

DANE OSOBOWE

Mogą to być informacje takie jak: imię, nazwisko, numer PESEL, płeć, adres e-mail, ale również mniej oczywiste jak numer IP, dane o lokalizacji, kod genetyczny, poglądy polityczne czy historia zakupów.

Wszelkie informacje zbierane na temat osoby, które pozwalają na ustalenie jej tożsamości, są danymi osobowymi, niezależnie od tego, czy są przetwarzane w formie papierowej czy cyfrowej.

ORGANY PUBLICZNE W ROZUMIENIU RODO

Na gruncie projektu ustawy przyjęto, iż w polskim systemie prawnym przez organy publiczne co do zasady będą rozumiane organy administracji publicznej o których mowa w **art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.**

ORGANY OCHRONY DANYCH OSOBOWYCH

- Wzmocnienie organów nadzorczych;
- Gwarancje niezależności organów nadzorczych;
- Większy zakres uprawnień i obowiązków;
- Autonomia proceduralna państw członkowskich UE

ROZPORZĄDZENIE TO AKT PRAWNY KTÓRY MA OBOWIĄZYWAĆ PRZEZ KILKADZIESIĄT LAT. JAKIE INSTRUMENTY ZASTOSOWANO, BY JEGO POSTANOWIENIA BYŁY ZAWSZE AKTUALNE?

NEUTRALNOŚĆ TECHNOLOGICZNA – NA CZYM POLEGA

RODO NIE WYTYCZA SZCZEGÓŁOWYCH INSTRUKCJI TECHNOLOGICZNYCH ZABEZPIECZANIA DANYCH

W każdym obszarze przetwarzania danych, zasady zabezpieczenia danych powinny być więc inne i dostosowane do specyfiki podejmowanych działań. W ocenie Ministra Cyfryzacji zastosowane środki zabezpieczenia danych powinny być jednak powszechnie dostępne, uznane za skuteczne i stabilne technologicznie.

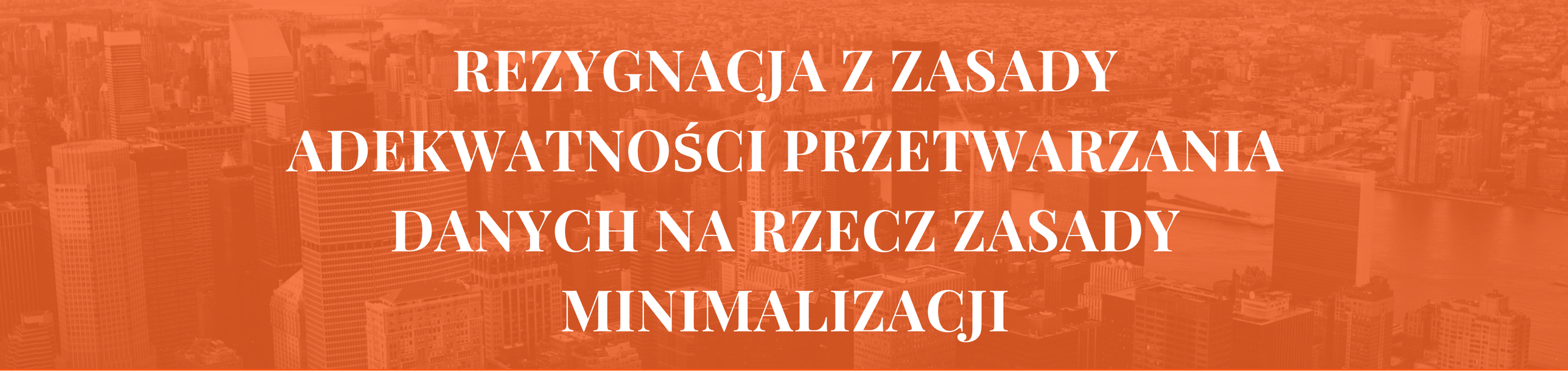
Art. 32

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Art. 25

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak **pseudonimizacja**, zaprojektowane w celu skutecznej realizacji zasad ochrony danych.

- Rozporządzenie ma pozostać aktualne niezależnie od stałego rozwoju nowych technologii
- Brak jest konkretnych technicznych wymogów ochrony danych – o tym jakie środki powinny zastać przyjęte decydować powinny okoliczności stanu faktycznego
- Administrator zobowiązany jest uwzględnić najdalej idące możliwe, uznane za stabilne, skuteczne i powszechnie dostępne techniczne i organizacyjne środki ochrony danych
- W każdym przypadku GIODO oceni, czy poziom ochrony danych jest wystarczający



REZYGNACJA Z ZASADY ADEKWATNOŚCI PRZETWARZANIA DANYCH NA RZECZ ZASADY MINIMALIZACJI

ABY MÓC WYKAZAĆ PRZESTRZEGANIE NINIEJSZEGO ROZPORZĄDZENIA, ADMINISTRATOR POWINIEN PRZYJĄĆ WEWNĘTRZNE POLITYKI I WDROŻYĆ ŚRODKI, KTÓRE SĄ ZGODNE W SZCZEGÓLNOŚCI Z ZASADĄ UWZGLĘDNIANIA OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ Z ZASADĄ DOMYŚLNEJ OCHRONY DANYCH. TAKIE ŚRODKI MOGĄ POLEGAĆ M.IN. NA MINIMALIZACJI PRZETWARZANIA DANYCH OSOBOWYCH (MOTYW 78).

Art. 5 ust. 1 pkt c.
Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”)

ZMIANA MODELU ODPOWIEDZIALNOŚCI

CO DO ZASADY PODMIOTEM ODPOWIEDZIALNYM ZA WYKONYWANIE OBOWIĄZKÓW OCHRONY DANYCH OSOBOWYCH JEST WYŁĄCZNIE ADMINISTRATOR (PODMIOT PRZETWARZAJĄCY). TO ADMINISTRATOR (PODMIOT PRZETWARZAJĄCY) DECYDUJE WIĘC O TYM KTÓRE Z JEGO ZADAŃ WYKONYWAŁ BĘDZIE W PRAKTYCE INSPEKTOR OCHRONY DANYCH (OBECNY ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI).

ZASADA ROZLICZALNOŚCI

ADMINISTRATOR JEST ODPOWIEDZIALNY ZA PRZESTRZEGANIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH I MUSI BYĆ W STANIE WYKAZAĆ ICH PRZESTRZEGANIE („ROZLICZALNOŚĆ”).

NOWE INSTRUMENTY PRAWNE OCHRONY DANYCH OSOBOWYCH

- Ocena skutków
- Wyznaczenie inspektora ochrony danych (były ABI)
- Rejestr Czynności Przetwarzania Danych Osobowych
- Privacy by design
- Privacy by default
- Kary finansowe
- Obowiązek notyfikacji naruszeń

OCENA SKUTKÓW

art. 35

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.

WYZNACZENIE INSPEKTORA OCHRONY DANYCH

Administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych zawsze gdy przetwarzania dokonują organ lub podmiot publiczny z wyjątków sprawowania przez nie wymiaru sprawiedliwości, gdy dane przetwarzane są dużą skalę i dotyczą szczególnych kategorii danych osobowych bądź działania oparte są na monitorowaniu osób.

Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

RODO nakłada na administratorów, w tym podmioty publiczne obowiązek prowadzenia rejestru czynności przetwarzania danych. Od 25 maja 2018 r. każdy podmiot przetwarzający ma obowiązek dokumentować czynności związane z przetwarzaniem danych osobowych.

- Obowiązek administratora
- Prowadzi Inspektor
- Administrator ma obowiązek udostępnić Rejestr na żądanie organu nadzorczego

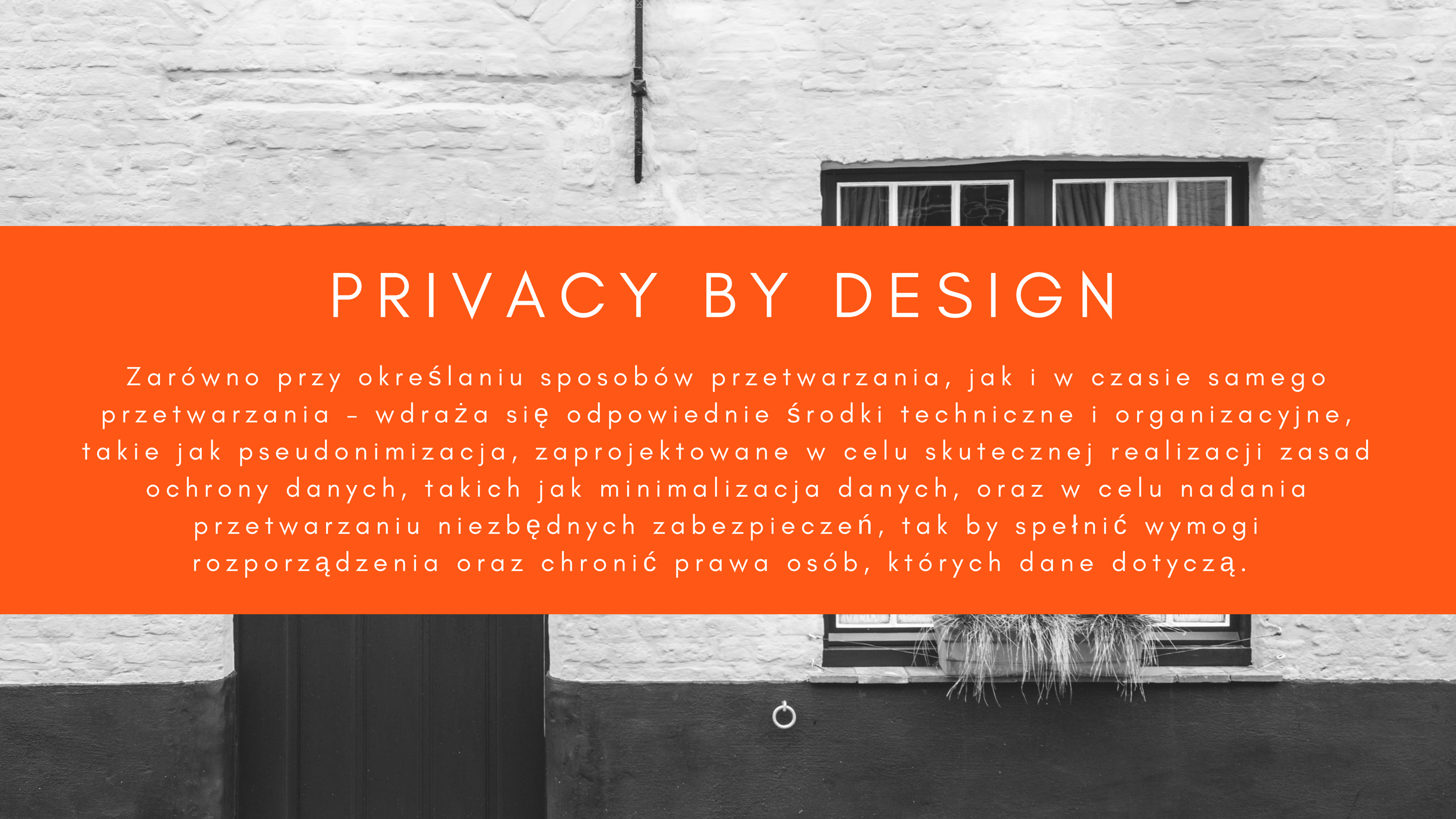
REJESTR POWINIEN ZAWIERAĆ:

- PODSTAWĘ PRAWNĄ PRZETWARZANIA,
- KOMU I KIEDY DANE ZOSTAŁY UDOSTĘPNIONE,
- JAK RAPORTUJE SIĘ INCYDENTY ZWIĄZANE Z NARUSZENIEM OCHRONY DANYCH,
- CZY PRZEPROWADZONO ANALIZĘ W ZAKRESIE OBOWIĄZKU BĄDŹ BRAKU OBOWIĄZKU WYZNACZENIA INSPEKTORA OCHRONY DANYCH I JAKIE WNIOSKI Z NIEJ PŁYNĄ,
- KTÓRY ORGAN NADZORCZY BĘDZIE WIODĄCYM DLA TRANSGRANICZNYCH OPERACJI PRZETWARZANIA, KTÓRE PROWADZISZ.

WYZNACZENIE INSPEKTORA OCHRONY DANYCH

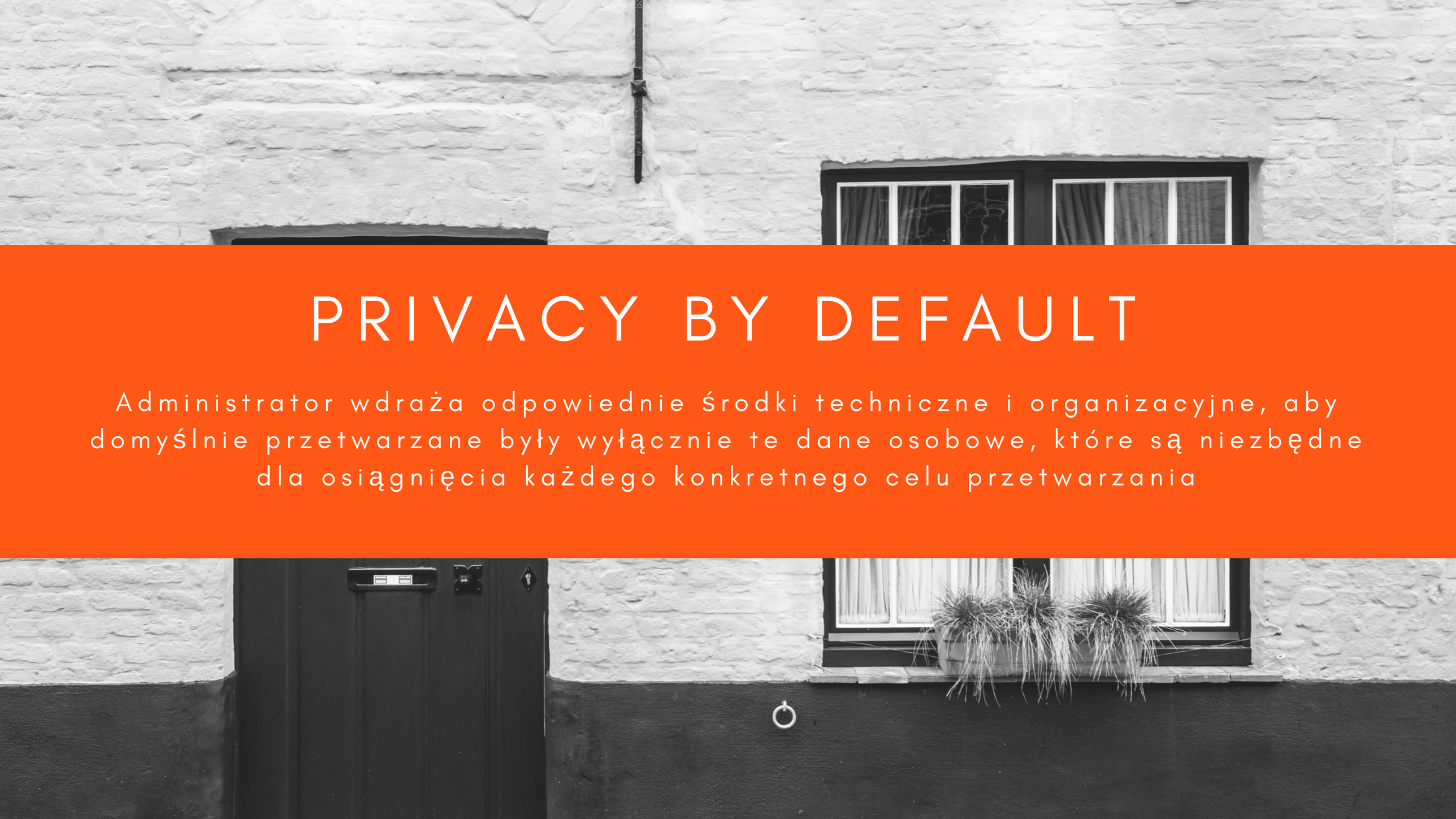
Administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych zawsze gdy przetwarzania dokonują organ lub podmiot publiczny z wyjątków sprawowania przez nie wymiaru sprawiedliwości, gdy dane przetwarzane są dużą skalę i dotyczą szczególnych kategorii danych osobowych bądź działania oparte są na monitorowaniu osób.

Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych.



PRIVACY BY DESIGN

Zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża się odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi rozporządzenia oraz chronić prawa osób, których dane dotyczą.



PRIVACY BY DEFAULT

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania

KARY FINANSOWE

Reforma ochrony danych osobowych nie jest przeprowadzana po to, żeby karać. Jej głównym celem jest zwiększenie poziomu bezpieczeństwa, prywatności i ochrony danych. Kary finansowe powinny być też ostatecznością - wcześniej organ nadzorczy będzie mógł wykorzystać ostrzeżenia, upomnienia czy decyzje nie zawierające kar.

- **100 tys. dla organów publicznych**
- **10 tys zł dla instytucji kultury**

OBOWIĄZEK NOTYFIKACJI NARUSZEŃ

Art. 33

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Czy każde naruszenie należy zgłaszać?

CERTYFIKAT

- NIE TRZEBA, ALE WARTO!
- BUDUJE POZYTYWNY WIZERUNEK ORGANU PUBLICZNEGO W OCZACH OBYWATELI

KODEKS POSTĘPOWANIA

MECHANIZMY POZWALAJĄCE NA ZDEFINIOWANIE LIST DOBRYCH PRAKTYK W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W KONKRETNYM ŚRODOWISKU

JAK WDROŻYĆ 1/2

- STWORZYĆ NAJLEPSZE MOŻLIWE MECHANIZMY **ZABEZPIECZENIA** DANYCH OSOBOWYCH
- ZAWIADOMIĆ PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH O POWOŁANIU **INSPEKTORA OCHRONY DANYCH**, CHYBA ŻE STAŁ SIĘ NIM AUTOMATYCZNIE WCZEŚNIEJSZY ABI
- UTWORZYĆ I SYSTEMATYCZNIE UZUPEŁNIAĆ **REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH**

JAK WDROŻYĆ 2/2

- STWORZYĆ **KODEKS POSTĘPOWANIA** CHARAKTERYSTYCZNY DLA SEKTORA DZIAŁALNOŚCI PODMIOTU I PRZEDŁOŻYĆ GO DO AKCEPTACJI DO URZĘDU OCHRONY DANYCH OSOBOWYCH
- W PRZYPADKU **NARUSZENIA BEZPIECZEŃSTWA DANYCH** OSOBOWYCH ZGŁOSIĆ JE ORGANOWI NADZORCZEMU (URZĘDOWI OCHRONY DANYCH OSOBOWYCH) I OSOBIE/OSOBOM, KTÓRYCH ONO DOTYCZY
- UZYSKAĆ **CERTYFIKAT**

Ministerstwo
Cyfryzacji

DZIĘKUJĘ ZA UWAGĘ

DR MACIEJ KAWECKI