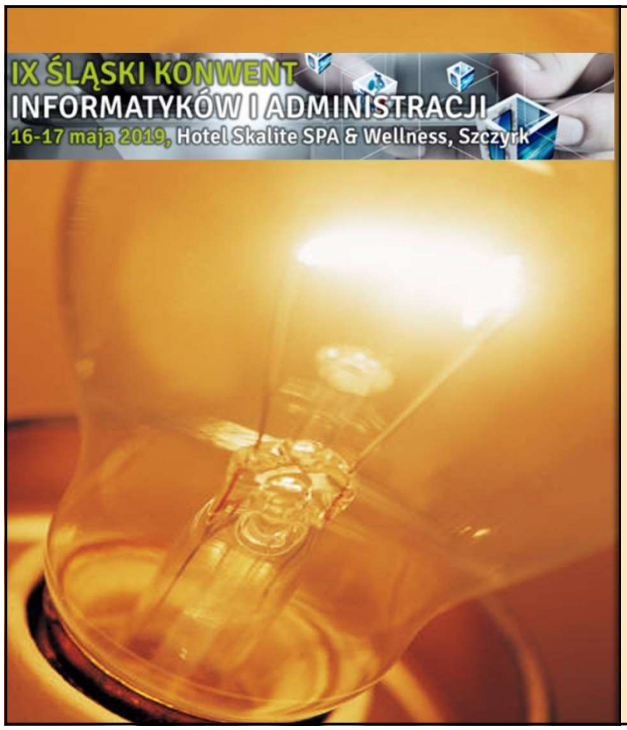


Odpowiedzialność i wymagania dla
działu IT
w świetle nowych wymagań prawnych w trakcie audytu i kontroli

Janusz Czauderna
Tel. 505 328 100
jczauderna@volvox.pl

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

- W bieżącej obsłudze informatycznej to obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.
- W trakcie kontroli lub audytu opisanie i udowodnienie **zasad rozliczalności** w dostępie do danych osobowych w systemach informacyjnych

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

Obowiązki te oznaczają konieczność zapewnienia na każdym etapie przetwarzania danych co najmniej:

a) **legalności przetwarzania** - rozumianej jako zgodność nie tylko zRODO/ UODO (zwłaszcza istnienie tzw. podstawy przetwarzania), lecz też z przepisami szczególnymi;

b) **celowości przetwarzania** - dane mogą być przetwarzane tylko do oznaczonych, zgodnych z prawem celów. Administrator danych osobowych jest związany wskazanym celem, a dane osobowe, co do zasady, nie powinny być przetwarzane niezgodnie z celem ich zebrania;

c) **adekwatności przetwarzania** - zakres danych powinien być adekwatny do celu ich przetwarzania, w szczególności nie może być szerszy, niż jest to niezbędne do realizacji tego celu;

d) **ograniczenia czasu przetwarzania** - dane mogą być przetwarzane przez czas niezbędny do osiągnięcia celu przetwarzania (po upływie tego okresu muszą zostać usunięte);

e) **bezpieczeństwa przetwarzania** - dane muszą pozostać poufne, a administrator musi zapewnić, że nie zostaną ujawnione nieautoryzowanym podmiotom;

f) **rozliczalności przetwarzania** - rozumianej jako zapewnienie możliwości przypisania określonych działań/operacji na danych konkretnemu podmiotowi,

g) **merytorycznej poprawności danych** - dane muszą być prawdziwe i aktualne;

h) **integralności danych** - rozumianej jako zapewnienie, że dane nie zostały zmienione lub zniszczone bez odpowiedniego upoważnienia.

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

- **Privacy by design** - wszelkie ustawienia domyślne muszą co do zasady sprzyjać prywatności z obowiązkiem administratora danych osobowych jest wdrażanie odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie dane osobowe niezbędne do osiągnięcia każdego konkretnego celu przetwarzania w zakresie ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

Zapewnienie przenoszalności danych (data portability)

Jest to potencjalnie jedno z podstawowych wyzwań z punktu widzenia technologicznego , gdyż w praktyce większość danych osobowych jest przetwarzana w dedykowanych systemach zamkniętych.

Przenoszalność jest jednak ograniczona do systemów gdzie przetwarzanie odbywa się w sposób zautomatyzowany a jego podstawą jest zgoda osoby, której dane dotyczą, lub 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).

Prawa tego - ze względu na jego charakter wg tezy 68 preambuły RODO - nie powinno się natomiast wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych.

Dlatego nie powinno ono mieć zastosowania, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

Zapewnienie adekwatnego poziomu bezpieczeństwa danych poprzez **monitorowanie podatności** dla m.in..:

- Stosowanych mechanizmów uwierzytelniania
- Wdrożonych systemów kontroli parametrów środowiskowych (temperatury, zasilania, itp.)
- Wymaganych poprawek bezpieczeństwa dla aplikacji i sprzętu
- Stosowanych mechanizmów szyfrowania transmisji danych
- Zasad i mechanizmów backupu i archiwizacji

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

Zapewnienie adekwatnego poziomu posiadanych **zapisów i udokumentowanej informacji** dla udowodnienia realizowanego poziomu bezpieczeństwa danych zawartych w obowiązującej w organizacji dokumentacji SZBI oraz RODO/UODO poprzez:

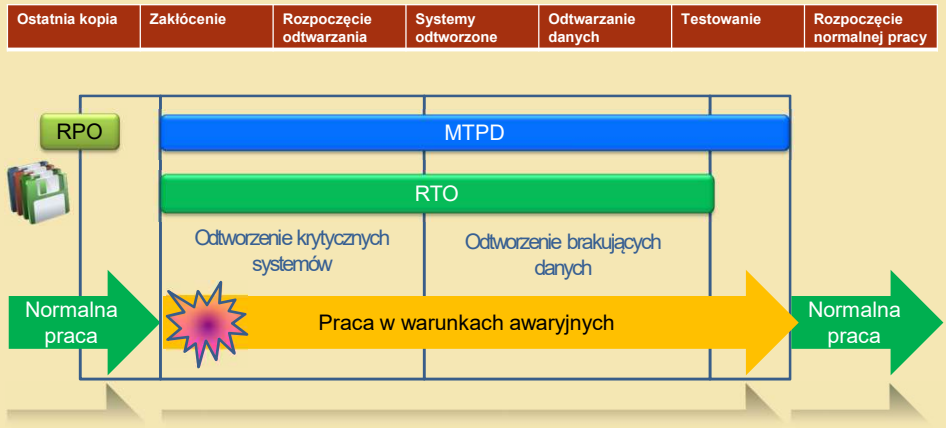
- Opisy i dowody na dopuszczalność przetwarzania - czy istnieją podstawy, które pozwalają na przetwarzanie konkretnych danych w określonym celu
- Opisy i dowody na prawidłowość i zgodność stosowanych sposobów przetwarzania danych z prawem , zasadami przetwarzania, udostępniania danych osobowych z systemowymi i organizacyjnymi standardami, np. bezpieczeństwa danych obowiązującymi w organizacji
- Rejestry i raporty
- Testy penetracyjne
- Audyty bezpieczeństwa

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

- Kontrola wymagań umów SLA z dostawcami zewnętrznymi
- Kontrola stosowania minimalnych zapisów dla wymagań bezpieczeństwa w umowach serwisowych i dla dostaw
- Monitoring zmienności wymagań prawnych w obszarze dysponowania, gromadzenia i przetwarzania danych
- Monitoring poziomu bezpieczeństwa dla usług i zadań outsourcingowych
- Kontrola poziomu zabezpieczeń dla e-usług i portali informacyjnych

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

- Zapewnienie ciągłości działania i dostępu do danych



Straty, kary, odszkodowania

RTO<= MTPD

Zakres zadań i odpowiedzialności działu IT w ochronie danych osobowych

- Zapewnienie ciągłości działania i dostępu do danych

Ile czasu możemy funkcjonować bez nieodwracalnych konsekwencji?

MTPD – (Maximum Tolerable Period of Disruption) maksymalny tolerowany czas trwania zakłócenia

MAO – (Maximum Acceptable Outage) maksymalny czas przerwy

RTO (Recovery Time Objective) czas, po którym działalność musi zostać wznowiona

Jakie dane i z kiedy są dostępne?

RPO (Recovery Point Objective) wyznacza punkt w czasie, wskazujący na akceptowalny poziom utraty danych gwarantowany czasu odzyskania danych

Na jakim poziomie możemy odtworzyć działalność?

MBCO (Minimum Business Continuity Objective) wyznacza minimalny poziom usług/produktów, który jest dla organizacji akceptowalny, realizujący jej cele biznesowe w czasie zakłócenia

Rozliczalność – najważniejsza odpowiedzialność IT

Jeden z najważniejszych czynników obrony w przypadku kontroli
wystąpienia incydentu
lub
naruszenia ochrońmy danych

Rozliczalność w RODO

Określa ją art. 5 ust. 2 RODO, który stanowi, że **administrator danych** jest odpowiedzialny za przestrzeganie przepisów RODO wskazanych w art.5 ust. 1 RODO i musi być w stanie wykazać ich przestrzeganie.

Rozliczalność na gruncie RODO dotyczy zapewnienia zgodności ze wszystkimi zasadami przetwarzania, bez względu na sposób, w jaki dane są przetwarzane

czyli nie tylko w kwestiach związanych z przetwarzaniem danych w systemie informatycznym czy zapewnieniem bezpieczeństwa danych, jak to było na gruncie tradycyjnej definicji rozliczalności

Rozliczalność w RODO

Rozliczalność na gruncie RODO składa z dwóch elementów, które muszą zostać spełnione łącznie, aby zasada ta została zrealizowana:

- odpowiedzialność administratora za przestrzeganie przepisów,
- wykazywanie ich przestrzegania.

Nie wystarczy zatem, aby administrator przestrzegał przepisów RODO, **ale powinien także w należyty sposób to dokumentować,** gdyż już samo niewykazanie ich przestrzegania może wiązać się z poniesieniem przez administratora odpowiedzialności (tak jak za ich nieprzestrzeganie).

Znaczenie rozliczalności

Zasadzie tej przypisano w RODO istotną rolę związaną z przerzuceniem na administratora obowiązku wykazania zgodności z RODO.

Przykładowo, w przypadku kontroli to na **administratorze danych będzie ciążył obowiązek wykazania zgodnego z prawem przetwarzania danych** (a nie na organie nadzorczym wykazania niezgodności administratora).

Jak się wskazuje, na gruncie RODO **zasada rozliczalności** jako mająca zapewnić większą skuteczność zasad przetwarzania ma **charakter instrumentalny** wobec pozostałych zasad, które w praktyce mogą zostać wdrożone dopiero wówczas, gdy zostaną zoperacjonalizowane w ramach działań organizacyjnych .

Zakres rozliczalności

Na gruncie zasady rozliczalności administrator danych będzie zatem odpowiedzialny za zapewnienie i wykazanie spełnienia następujących zasad (wskazanych w art. 5 ust. 1 RODO):

- zgodności z prawem, rzetelności i przejrzystości,
- ograniczenia celu,
- minimalizacji danych,
- prawidłowości,
- ograniczenia przechowywania,
- integralności i poufności.

Biorąc pod uwagę choćby zasadę legalności, która ma szeroki zakres przedmiotowy, obejmujący nie tylko konieczność spełnienia przesłanek legalności przetwarzania wskazanych w art. 6 i 9 RODO, lecz także zapewnienia zgodności z pozostałymi przepisami o ochronie danych osobowych czy nawet zgodności z całokształtem przepisów regulujących działalność administratora danych , należy wskazać, że zasada rozliczalności dotyczy zatem w praktyce wszystkich wymogów wynikających z RODO.

Realizacja zasady rozliczalności

art. 5 ust. 2 RODO nie konkretyzuje, co w praktyce miałoby oznaczać zapewnienie odpowiedzialności za przestrzeganie przepisów RODO i wykazywanie ich przestrzegania, z pomocą przychodzi art. 24 ust. 1 RODO, który stanowiąc doprecyzowanie **zasady rozliczalności,** stanowi, że administrator ma obowiązek **wdrożyć odpowiednie środki techniczne i organizacyjne**, aby przetwarzanie odbywało się zgodnie z RODO i **aby móc to wykazać.**

W tym celu administrator danych ma obowiązek uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia

Oznacza to, że zasadą podejścia opartego na ryzyku (*risk based aproach)* objęty został także wymóg zapewnienia rozliczalności, a sama zasada ma być realizowana przez wdrożenie odpowiednich środków technicznych i organizacyjnych.

Realizacja zasady rozliczalności

Zgodne z opinią w sprawie zasady rozliczalności , w której zaproponowano, aby przy tworzeniu przepisów dotyczących rozliczalności zasadą tą objąć dwa elementy:

- wymaganie podjęcia przez administratora właściwych i skutecznych środków do wdrożenia zasad ochrony danych,
- wymaganie wykazania na żądanie, że właściwe i skuteczne środki bezpieczeństwa zostały podjęte.
- Administrator danych musi przedstawić dowody w związku z powyższym pkt – a wiec będzie to wymaganie skierowane m.in. do działu IT

Dokumentowanie w ramach rozliczalności i obsługi naruszenia/incydentu

Zgodnie z RODO administrator danych w dziale IT :

- dokumentuje wszelkie naruszenia ochrony danych osobowych, **w tym okoliczności naruszenia ochrony danych osobowych**, jego skutki oraz podjęte działania zaradcze; dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania art. 33 RODO (Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu) :
- **należy stosować odpowiednie standardy i normy ISO**

Pozostałe dokumenty i zapisy

- dokumentują polecenie przetwarzania danych podmiotowi przetwarzającemu;
- zawiera umowę powierzenia danych do przetwarzania w formie pisemnej, w tym elektronicznej;
- wyraża pisemną zgodę na skorzystanie z dalszego podmiotu przetwarzającego;
- prowadzi rejestr czynności przetwarzania w formie pisemnej, w tym elektronicznej;
- w przypadku przekazań do państwa trzeciego, o których mowa w art. 49 ust. 1 ak. 2 RODO, dokumentuje ocenę oraz stosowanie odpowiednich zabezpieczeń;
- wyznacza przedstawiciela za pomocą pisemnego upoważnienia do podejmowania działań w jego imieniu w odniesieniu do obowiązków wynikających z rozporządzenia;
- udziela na piśmie lub w inny sposób, w tym w stosownych przypadkach elektronicznie, informacji podmiotom danych w ramach wykonywania ich praw.

Zabezpieczenia techniczne

Uwzględniając
stan wiedzy technicznej,
koszt wdrażania
charakter, zakres, kontekst i cele przetwarzania
ryzyko naruszenia praw lub wolności osób fizycznych

o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, AD i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi:

- pseudonimizację
- szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania poprzez odpowiedni zestaw technikaliów i wymagań formalnych

Zabezpieczenia organizacyjne i techniczne

- **Udokumentowaną** i monitorowaną zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

- **Udokumentowaną i monitorowaną procedurę** regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

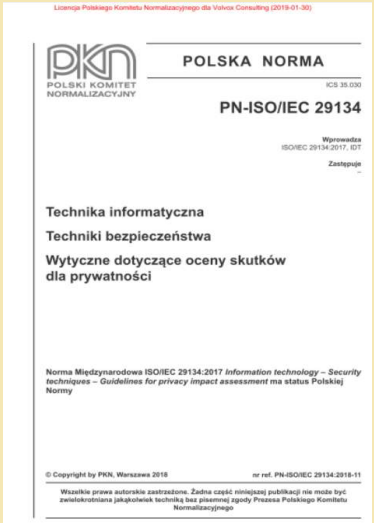
Kontrola, postępowanie administracyjne – metody i narzędzia obrony

Numer normy	Opis
PN ISO/IEC 27000:2014-11	Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia
PN ISO/IEC 27001:2014-12	Systemy zarządzania bezpieczeństwem informacji -- Wymagania
PN ISO/IEC 27002:2014-12	Praktyczne zasady zabezpieczania informacji
PN ISO/IEC 27005:2014-12	Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji
PN-ISO/IEC 27013	Wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000-1
PN-EN ISO /IEC 27018	Praktyczne zasady ochrony danych identyfikujących OSOBĘ (PII) w chmurach publicznych działających jako przetwarzający PII
PN-EN ISO /IEC 2737:2016-12	Wytyczne dotyczące identyfikowania, gromadzenia i przechowywania cyfrowego materiału dowodowego
PN-EN ISO /IEC 2738:2016-12	Specyfikacja metod cyfrowych trwałego usuwania
PN – ISO 31000	Zarzadzanie ryzykiem zasady i wytyczne
PN-ISO/IEC 20000-1	Technika informatyczna. Zarządzanie usługami. Część 1: Wymagania dla systemu zarządzania
PN-ISO/IEC 20000-2	Technika informatyczna. Zarządzanie usługami. Część 2: Reguły postępowania
PN-EN ISO 22301:2014-18	Bezpieczeństwo powszechne -- Systemy zarządzania ciągłością działania -- Wymagania.
PN-EN ISO/IEC 27040: 2016-12	Techniki bezpieczeństwa – Bezpieczeństwo pamięci masowych
PN-EN ISO/IEC 27041:2016-12	Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem
PN-EN ISO/IEC 27042:2016-12	Wytyczne do analizy i interpretacji cyfrowego śladu dowodowego
PN-EN ISO/IEC 27043:2016-12	Pryncypia i procesy w dochodzeniach związanych z incydentami
PN-EN ISO /IEC 24762	Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie (dobra praktyka)
PN-EN ISO/IEC 30121:2016-12	Nadzór nad strukturą ryzyka związanego z informatyką śledczą

Norma PN-ISO/IEC 29134

Technika informatyczna, Technika bezpieczeństwa, Wytyczne dotyczące oceny skutków dla prywatności

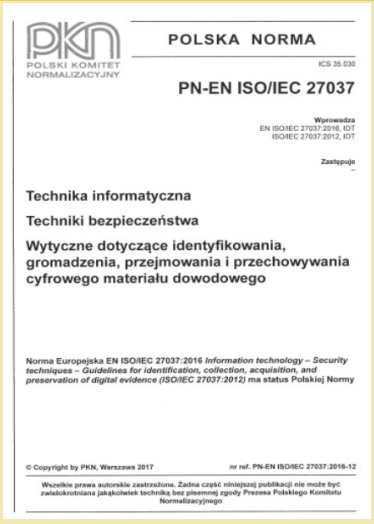
W normie określono ramy zarządzania uzasadnioną pewnością uwierzytelnienia podmiotu w określonym kontekście. W szczególności, norma ta:
— określa cztery poziomy uzasadnionej pewności uwierzytelnienia podmiotu;
— określa kryteria i wytyczne do osiągnięcia każdego z czterech poziomów uzasadnionej pewności uwierzytelnienia podmiotu;
— zapewnia wytyczne do odwzorowania innych schematów uzasadnionej pewności uwierzytelnienia na cztery zdefiniowane poziomy;
— zapewnia wytyczne do wymiany wyników uwierzytelnienia, które wykorzystują koncepcję czterech poziomów;
— zapewnia wytyczne w odniesieniu do zabezpieczeń, które są zalecane w celu zmniejszenia zagrożeń związanych z uwierzytelnianiem.



Norma PN-ISO/IEC 27037

Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego

Norma zawiera wytyczne do specyficznych działań w ramach postępowania z cyfrowym materiałem dowodowym; do tych działań należą: identyfikacja, gromadzenie, pozyskiwanie i zachowywanie cyfrowego materiału dowodowego, który może mieć wartość dowodową.
Norma zawiera wskazówki dla osób fizycznych w odniesieniu do typowych sytuacjach spotykanych w całym procesie postępowania z cyfrowym materiałem dowodowym i pomaga organizacjom w ich procedurach dyscyplinarnych i w ułatwianiu wymiany potencjalnego cyfrowego materiału dowodowego pomiędzy różnymi systemami prawnymi.


POLSKA NORMA

ICS 35.030

PN-EN ISO/IEC 27037

Wprowadza
EN ISO/IEC 27037:2016, IDT
ISO/IEC 27037:2012, IDT

Zastępuje
–

Technika informatyczna

Techniki bezpieczeństwa

Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego

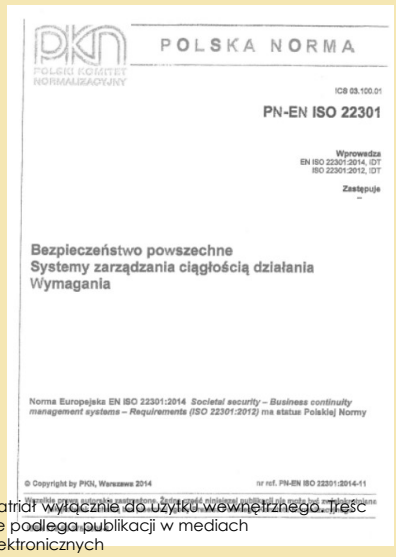
Norma Europejska EN ISO/IEC 27037:2016 *Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence (ISO/IEC 27037:2012)* ma status Polskiej Normy

nr ref. PN-EN ISO/IEC 27037:2016-12

Norma PN - ISO/IEC 22301

Bezpieczeństwo powszechne – Systemy zarządzania ciągłością działania - Wymagania

Wymagania dotyczące planowania, ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i ciągłego doskonalenia udokumentowanego systemu zarządzania, aby zmniejszyć prawdopodobieństwo wystąpienia uciążliwych incydentów, przygotować się na ich wystąpienia, odpowiedzieć na ich działanie i wyjść z kryzysu gdy się pojawiają.


POLSKA NORMA

ICS 03.100.01

PN-EN ISO 22301

Wprowadza
EN ISO 22301:2014, IDT
ISO 22301:2012, IDT

Zastępuje
–

Bezpieczeństwo powszechne
Systemy zarządzania ciągłością działania
Wymagania

Norma Europejska EN ISO 22301:2014 *Societal security – Business continuity management systems – Requirements (ISO 22301:2012)* ma status Polskiej Normy

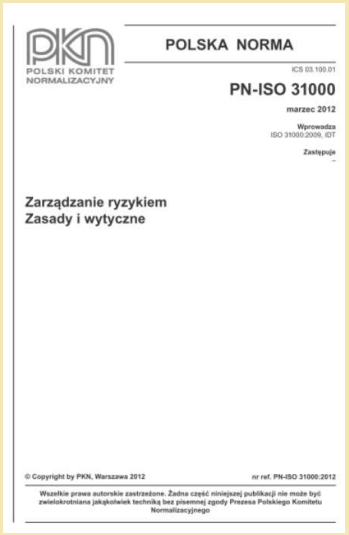
nr ref. PN-EN ISO 22301:2014-11

Norma PN - ISO 31000

Zarządzanie ryzykiem - Zasady i wytyczne

Wytyczne dotyczące zarządzania ryzykiem, na które narażone są organizacje.

Zastosowanie tych wytycznych można dostosować do każdej organizacji i jej kontekstu.
Ppodano wspólne podejście do zarządzania każdym rodzajem ryzyka i nie jest ono ograniczone do specyficznej branży lub sektora.
Norma może być wykorzystywany przez całe życie organizacji i można go stosować do każdej działalności, w tym podejmowania decyzji na wszystkich poziomach


POLSKA NORMA

ICS 03.100.01

PN-ISO 31000

marzec 2012

Wprowadza
ISO 31000:2009, IDT

Zastępuje

Zarządzanie ryzykiem
Zasady i wytyczne

nr ref. PN-ISO 31000:2012

Norma PN – ISO/IEC 27001

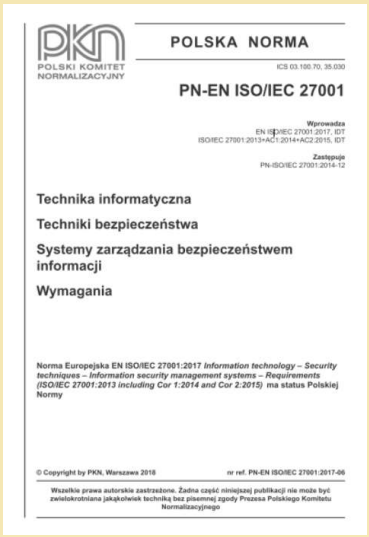
Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania

Norma określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji.

Norma obejmuje również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji.

Wymogi określone w Normie Międzynarodowej są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru.

Wyłączenie któregokolwiek z wymagań określonych w Rozdziałach 4 do 10 jest nieakceptowalne, w wypadku gdy organizacja deklaruje zgodność Normą


POLSKA NORMA

ICS 03.100.70, 35.030

PN-EN ISO/IEC 27001

Wprowadza
EN ISO/IEC 27001:2017, IDT
ISO/IEC 27001:2013+AC1:2014+AC2:2015, IDT

Zastępuje
PN-ISO/IEC 27001:2014-12

Technika informatyczna

Techniki bezpieczeństwa

Systemy zarządzania bezpieczeństwem informacji

Wymagania

Norma Europejska EN ISO/IEC 27001:2017 *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)* ma status Polskiej Normy

nr ref. PN-EN ISO/IEC 27001:2017-06

Norma ISO/IEC 29100:2011

Privacy framework/ Ramy prywatności

W normie określono ramy prywatności, które obejmują:

— określenie wspólnej terminologii dotyczącej prywatności;
— zdefiniowanie aktorów i ich ról w przetwarzaniu danych
— opis uwarunkowań dotyczących zabezpieczeń prywatności;
— zapewnienie technologiom informatycznym odniesień do znanych pryncypiów prywatności

Norma ma zastosowanie **do osób fizycznych oraz organizacji** uczestniczących w definiowaniu, zamawianiu, projektowaniu, opracowywaniu, testowaniu, utrzymaniu, administrowaniu i eksploatowaniu systemów teleinformatycznych lub usług, które wymagają zabezpieczeń prywatności przy przetwarzaniu PII.

Norma ISO/IEC 29115:2013

Entity authentication assurance framework / Ramy uzasadnionej pewności poziomów uwierzytalnienia

W normie określono ramy zarządzania uzasadnioną pewnością uwierzytelnienia podmiotu w określonym kontekście.

W szczególności, norma ta:
wytyczne do odwzorowania innych schematów uzasadnionej pewności uwierzytelnienia na cztery zdefiniowane poziomy;
— zapewnia wytyczne do wymiany wyników uwierzytelnienia, które wykorzystują koncepcję czterech poziomów
— zapewnia wytyczne w odniesieniu do zabezpieczeń, które są zalecane w celu zmniejszenia zagrożeń związanych z uwierzytelnianiem.

Norma ISO/IEC 29101: 2013

Privacy architecture frame-work/ Ramy architektury prywatności

W normie określono ramy architektury prywatności, które:
— odnoszą się do zagadnień systemów teleinformatycznych przetwarzających PII;
— wskazują komponenty do wdrożenia takich systemów;
— opisują widoki architektury zapewniających osadzenie w kontekście tych komponentów.

Norma ma zastosowanie u podmiotów uczestniczących w definiowaniu, zamawianiu, projektowaniu, opracowywaniu, testowaniu, utrzymaniu, administrowaniu i eksploatowaniu systemów teleinformatycznych przetwarzających PII.

W pierwszym rzędzie norma koncentruje się na systemach zapewniających interakcję z właścicielem PII.

Norma ISO/IEC 29151

Code of practice for PII protection/ Praktyczne zasady ochrony PII

W normie ustanowiono cele stosowania zabezpieczeń, zabezpieczenia i wytyczne do wdrażania zabezpieczeń, tak aby spełnić wymagania zidentyfikowane w wyniku przeprowadzenia szacowania ryzyka oraz skutków w odniesieniu do ochrony danych identyfikujących osobę (Personally Identifiable Information (PII)).

W szczególności, norma określa wytyczne na podstawie ISO/IEC 27002, biorąc pod uwagę wymagania wynikające z przetwarzania PII, które mogą mieć zastosowanie w kontekście ryzyka związanego z bezpieczeństwem informacji.

Norma ma zastosowanie do organizacji wszystkich typów i wielkości, działających(zgodnie z dfinicją zawartą w ISO/IEC 29100) jako podmioty kontrolujące PII, przetwarzając PII.

Pojęcie naruszenia przepisów o ochronie danych osobowych

Zgodnie z art. 4 pkt 12 RODO:

„naruszenie ochrony danych osobowych» oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem *zniszczenia, utracenia, zmodyfikowaniania nieuprawnionego ujawnienia lub nieuprawnionego dostępu dodanych osobowych przesyłanych,* przechowywanych lub w inny sposób przetwarzanych".

Dział IT - Pojęcie naruszenia przepisów o ochronie danych osobowych

Pojęcie naruszenia ochrony danych osobowych jest węższe od pojęcia naruszenia przepisów o ochronie danych osobowych (mieści się w nim).

Pojęcie naruszenia ochrony danych osobowych dotyczy wyłącznie aspektu bezpieczeństwa:

poufności;
integralności;
dostępności.

Dzial IT - Podział danych osobowych objętych kontrolą

Rodzaj	Dane dotyczące zidentyfikowanej osoby	Łatwa identyfikacja	Art. 11 (deidentyfikacja)	Dane anonimowe
Bezpośrednio połączone z danymi identyfikującymi	Tak	Nie	Nie	Nie
Znany jest sposób *(sytematic way)* na (ponowną) identyfikacje	Tak	Tak	Nie	Nie
Dane odnoszące się do konkretnej osoby	Tak	Tak	Tak	Nie

Źródło: M. Hintze, Viewing the GDPR through a De-Identification Lens: A Tool*f*or Cornpliance, Clarzfication, and Consistency, „International Data Protection Law" 2018f1, s.

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

- Zgodnie z art. 78 ust. 1 n.u.o.d.o. Prezes UODO przeprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych.
- weryfikacja przestrzegania przepisów o ochronie danych osobowych, tj. RODO oraz przepisów wdrażających
- weryfikacja stanu istniejącego ze stanem postulowanym, wynikającym z obowiązujących norm

Zakres Kontroli lub audytu w ochronie danych osobowych

Na liście kontrolnej organu nadzorczego znajdują się między innymi 40 następujących kwestii:

1. zgodność z prawem, rzetelność, przejrzystość,
2. ograniczenie celu,
3. minimalizacja danych,
4. **prawidłowość,**
5. **ograniczenie przechowywania,**
6. **integralność i poufność,**
7. **rozliczalność,**
8. przetwarzanie szczególnych kategorii danych,
9. warunki wyrażenia zgody i jej wycofania,
10. warunki wyrażenia zgody przez dziecko dla potrzeb usług społeczeństwa informacyjnego,
11. obowiązki informacyjne,
12. prawo dostępu do danych,
13. sprostowanie danych,
14. usunięcie danych (prawo do bycia zapomnianym),
15. prawo do ograniczenia przetwarzania,
16. obowiązek powiadamiania o sprostowaniu lub usunięciu danych lub ograniczeniu przetwarzania,
17. prawo do przenoszenia danych,
18. prawo do sprzeciwu,
19. zautomatyzowane podejmowanie decyzji
20. profilowanie,

Zakres Kontroli lub audytu w ochronie danych osobowych

Na liście kontrolnej organu nadzorczego znajdują się między innymi 40 następujących kwestii:

21. **faza projektowania,**
22. **domyślna ochrona danych,**
23. **bezpieczeństwo przetwarzania,**
24. **rejestrowanie czynności przetwarzania,**
25. **zgłaszanie organowi nadzorczemu naruszeń ochrony danych,**
26. zawiadamianie osoby, której dane dotyczą, o naruszeniu,
27. ocena skutków dla ochrony danych,
28. inspektor ochrony danych,
29. umowne powierzenie przetwarzania (podmiot przetwarzający),
30. przekazywanie danych do państw trzecich lub organizacji międzynarodowych: (i) z zastrzeżeniem odpowiednich zabezpieczeń; (ii) wiążące reguły korporacyjne – proces zatwierdzania,
31. wspólne kontrole
32. rejestr czynności przetwarzania danych i rejestr kategorii czynności przetwarzania
33. wytyczne dotyczące klasyfikacji naruszeń
34. procedura zgłaszania naruszeń ochrony danych do organu nadzorczego
35. procedurę informowania osób, których dane dotyczą, w razie naruszenia mogącego powodować wysokie ryzyko naruszenia ich praw lub wolności osób, w tym o działaniach jakie powinni wykonać, aby ryzyko to ograniczyć
36. procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych
37. raport z ogólnej analizy ryzyka
38. raport z ocen skutków dla ochrony danych
39. **procedury związane z pseudonimizacją i szyfrowaniem**
40. **plan ciągłości działania**
41. **procedury odtwarzania systemu po awarii, oraz ich testowania.**
42. polityki ochrony danych
43. **dokumentacja technicznych i organizacyjnych środków ochrony danych**

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

Postępowanie kontrolne - ustawa określa dwa tryby kontroli:

- **zwykły -** celem jest zweryfikowanie, czy mogło dojść do naruszenia przepisów o ochronie danych osobowych;
- **uzupełniający -** ten typ kontroli jest także regulowany przepisami rozdziału 9 n.u.o.d.o., niemniej w tym przypadku celem kontroli jest uzupełnienie materiału dowodowego w ramach (wszczętego już) postępowania administracyjnego w sprawie naruszenia prze pisów o ochronie danych osobowych.

zgodnie z art. 90 n.u.o.d.o. jeżeli na podstawie informacji zgromadzonych w postępowaniu kontrolnym Prezes UODO uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania, o którym mowa w art. 60 n.u.o.d.o. (postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych).

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

Celem kontroli jest zwłaszcza wszczynanej przed rozpoczęciem postępowania administracyjnego - jest weryfikacja, czy mogło dojść do naruszenia przepisów o ochronie danych osobowych, i w konsekwencji, czy należy wszcząć postępowanie administracyjne w tym zakresie (które może zakończyć się np. nałożeniem administracyjnej kary pieniężnej).

Cel kontroli - uprawdopodobnienie naruszenia, ponieważ kontrola nie rozstrzyga o prawach i obowiązkach kontrolowanego. W przypadku kontroli toczącej się równolegle do postępowania administracyjnego celem będzie uzupełnienie materiału dowodowego.

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

Cel postępowania, o którym mowa w art. 60 n.u.o.d.o. (postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych), jest ostateczne rozstrzygnięcie tej sprawy administracyjnej w formie przewidzianej przepisami tej ustawy i Kodeksu postępowania administracyjnego (decyzja administracyjna).

Zgodnie z art. 60 n.u.o.d.o. postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych jest prowadzone przez Prezesa Urzędu.

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

- kontrola służy przede wszystkim ustaleniu, czy mogło dojść do naruszenia przepisów o ochronie danych
- kontrola zwykle poprzedza postępowanie administracyjne, ale taka kolejność nie jest obligatoryjna, np. fakt naruszenia może być uprawdopodobniony, a jednocześnie może istnieć potrzeba szybkiej reakcji w ramach postanowienia, o którym mowa w art. 70 n.u.o.d.o. (tj. środek tymczasowy), które jest wydawane w toku postępowania administracyjnego.
- W toku kontroli taki środek nie może zostać zastosowany;

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

art. 70 ust. 1 n.u.o.d.o.:

Jeżeli w toku postępowania **zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy** o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, Prezes Urzędu, w celu zapobieżenia tym skutkom, może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do **ograniczenia przetwarzania** danych osobowych, wskazując dopuszczalny zakres tego przetwarzania.

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych – zależności

Wariant A

kontrola bez postępowania administracyjnego w sprawie naruszenia przepisów o ochronie danych osobowych (gdy w toku kontroli nie uprawdopodobniono naruszenia)

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

Wariant B

kontrola i następstwo kontroli, tj. postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

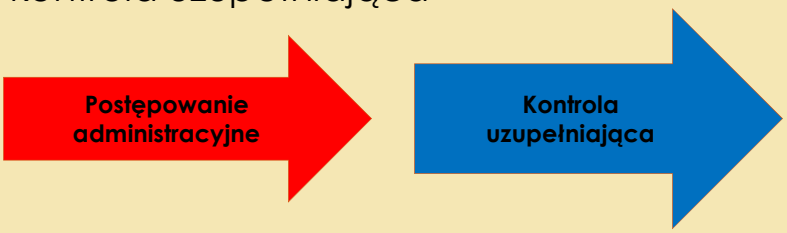
Wariant C

kontrola i następstwo kontroli, tj. postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych, w czasie którego prowadzona jest kontrola uzupełniająca

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

Wariant D

postępowanie administracyjne (bez wcześniejszej kontroli) w sprawie naruszenia przepisów o ochronie danych osobowych, w czasie którego prowadzona jest kontrola uzupełniająca



Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

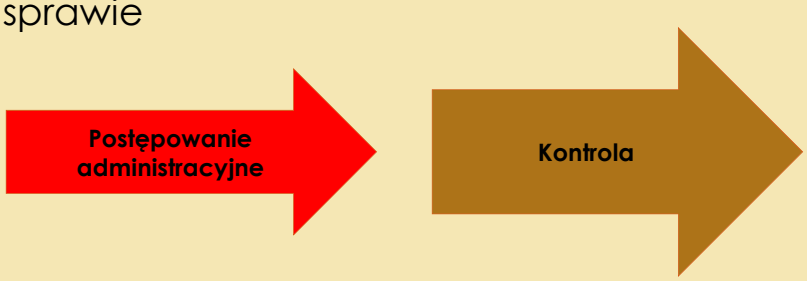
Wariant E

samodzielne postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych

Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

Wariant F

postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych, w następstwie którego prowadzona jest kontrola w innej sprawie



Kontrola a postępowanie administracyjne vs naruszenia przepisów o ochronie danych osobowych

Postępowanie kontrolne, uregulowane rozdziałem 9 n.u.o.d.o., poprzedzające postępowanie właściwe, prowadzone w trybie rozdziału 7 n.u.o.d.o., **nie ma charakteru postępowania administracyjnego.**

W przypadku kontroli uzupełniającej znajdą zastosowanie przepisy rozdziału 7 n.u.o.d.o. oraz przepisy Kodeksu postępowania administracyjnego, tj. przepisy o postępowaniu administracyjnym, natomiast przepisy rozdziału 9 n.u.o.d.o., tj. przepisy o kontroli, tylko w zakresie nienaruszającym tych wcześniejszych unormowań_

P. Gorzko [wz] Ustawa o ochronie danych osobowych. Komentarz, red. M. Gumularz, K. Kozieł, P. Kozik, Warszawa 2018, s. 347.

Jak przygotować się do kontroli - obowiązki

Skorelowane obowiązki kontrolowanego

Oznaczenie uprawnienia kontrolującego (lub odpowiednio obowiązku kontrolowanego	Podstawa prawna	Wyjaśnienie
Kontrolowany ma obowiązek zapewnić kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach, o których mowa w art. 84 ust. 1 pkt 3 n.u.o.d.o.	Art. 84 ust. 2 n.u.o.d.o.	Uprawnienia kontrolującego zostały skorelowane z obowiązkami podmiotu kontrolowanego do zapewnienia warunków i środków niezbędnych do sprawnego przeprowadzenia kontroli. Powyższy obowiązek obejmuje m.in. sporządzenie we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach informatycznych lub telein-formatycznych służących do przetwarzania danych.
Kontrolowany ma obowiązek dokonać potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w art. 84 ust. 2 n.u.o.d.o. W przypadku odmowy potwierdzenia za zgodność z oryginałem kontrolujący czyni o tym wzmiankę w protokole kontroli	Art. 84 ust. 3 n.u.o.d.o.	Kontrolowany ma prawny obowiązek samodzielnego sporządzania kopii wszystkich materiałów zgromadzonych na takich nośnikach, w urządzeniach bądź systemach informatycznych czy też kopii całości serwera danych. Użycie sformułowania „w szczególności" oznacza, że kontrolowany ma rów-nież obowiązek sporządzenia kopii innych dokumentów i informacji, np. przechowywanych w formie papierowej, jeżeli jest to niezbędne do sprawnego przeprowadzenia kontroli. Jednocześnie przygotowane kopie lub wydruki powinny być potwierdzone przez kontrolowanego za zgodność z oryginałem. Odmowa potwierdzenia za zgodność z oryginałem powinna zostać udokumentowana przez kontrolującego w formie wzmianki w protokole kontroli

(P. Gołko [w:] Ustawa... red. M. Gumularz, K. Kozieł, P. Kozik, art. 84).

Kontrole sektorowe 2019 - udostępnianie danych w Biuletynie Informacji Publicznej oraz sposób wysyłania korespondencji zawierającej dane osobowe

Przykład

Obszar kontroli dotyczy dwóch zagadnień:

1) udostępniania danych w Biuletynie Informacji Publicznej,

2) sposobu wysyłania korespondencji zawierającej dane osobowe

Przykład

Kontrole sektorowe 2019 - udostępnianie danych w Biuletynie Informacji Publicznej oraz sposób wysyłania korespondencji zawierającej dane osobowe

Kluczowe wymogi	Podstawa prawna	Przykładowe środki wdrożenia wymogów
Weryfikacja, czy dane są przetwarzane w sposób prawidłowy	Art. 5 ust. 1 lit. d RODO	Zastosowanie prawidłowej metody anonimizacji
Weryfikacja wymogów zmiany celu przetwarzania w ujawniania danych poprzez BIP	Art. 6 ust. 4	Pseudonimizacja, stosowanie środków technicznych uniemożliwiających masowe pobieranie danych
Weryfikacja, czy nie dochodzi do ujawniania zbyt szerokiego katalogu informacji o osobach pełniących funkcje publiczne	Art. 5 ust. 1 lit. c	Procedura oceny procesów przetwarzania pod kątem minimalizacji danych, wskazanie dopuszczalnego zakresu zbieranych danych w procedurze udostępniania danych w Biuletynie Informacji Publicznej, rejestr czynności przetwarzania, sprawdzenia dokonywane przez inspektora ochrony danych
Weryfikacja, czy nie dochodzi do ujawniania w BIP informacji dotyczących innych kategorii osób niż osoby pełniące funkcje publiczne	Art. 5 ust. 1 lit. a i c	Wskazanie kategorii osób w procedurze udostępniania danych w Biuletynie Informacji Publicznej, sprawdzenia dokonywane przez inspektora ochrony danych
Weryfikacja, czy dane są przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane	Art. 5 ust. 1 lit. e	Procedura retencji danych, systemowy mechanizm usuwania/anonimizowania danych po upływie okresów przechowywania

Przykład

Kontrole sektorowe 2019 - udostępnianie danych w Biuletynie Informacji Publicznej oraz sposób wysyłania korespondencji zawierającej dane osobowe

Przykładowe zachowania, które mogą być kwalifikowane jako naruszenia

- możliwość szczątkowej identyfikacji (de-anonimizacja);
- możliwość identyfikacji wskutek łączenia danych pochodzących z różnych źródeł (de-anonimizacja);
- błędna ocena co do statystycznego charakteru danych;
- błędna ocena możliwości przypisania informacji do osoby fizycznej (np. błędna kwalifikacja potrzebnych środków i nakładów na identyfikację – zob. motyw 26 RODO);
- błędna kwalifikacja, iż rejestr jest objęty motywem 14 RODO;
- błędna ocena, że w rejestrze nie występują dane wrażliwe;
- de-anonimizacja (możliwość szczątkowej identyfikacji / możliwość identyfikacji wskutek łączenia danych pochodzących z różnych źródeł);
- możliwość szerszego wykorzystywania danych osobowych niż cele udostępniania.

Gumularz Mirosław, Kozik Patrycja, Kontrole sektorowe 2019

Jak przygotować dział IT do kontroli/audytu

Przygotować :

1. Dokumentacja SZBI/ KRI
2. Dokumentacji ciągłości działania
3. Dokumentacje procedury identyfikacji naruszenia/ incydentu i gromadzenia materiału dowodowego
4. Rejestr incydentów
5. Procedury funkcjonowania serwera logów
6. Procedury nadawania/odbierania uprawnień do zgodności z opisem stanowiska lub czynności pracownika
7. Wykaz usług działu IT, portali informacyjnych,
8. Procedury backupu i archiwizacji
9. Dokumentację audytów bezpieczeństwa w dziale IT wewnętrznych i zewnętrznych
10. Analiza ryzyka
11. Wykazy/rejestry baz danych, aplikacji i systemów przetwarzających dane osobowe

Powyższa lista jest listą przykładową i minimalną – może ulec zmianie w zależności od kontekstu badania kontrolnego lub audytowego

Dziękuję za uwagę