GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Uniwersytet Wrocławski

NOWE ZASADY ZABEZPIECZENIA DANYCH OSOBOWYCH, CZYLI RODO W PRAKTYCE

STATUS I ZAKRES NORM TECHNICZNYCH W MECHANIZMACH CERTYFIKACJI I KODEKSACH POSTĘPOWANIA

Warszawa, 28 marca 2018 r.

Zaczynając od parafrazy …

Art. 4 pkt. 5 RODO

„pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, **bez użycia dodatkowych informacji**, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

W praktyce, dla przykładu, to … (1)

1. stworzenie warunków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych, w szczególności zabezpieczenia danych przed nieuprawnionym dostępem, nielegalnym ujawnieniem lub pozyskaniem (utratą poufności), a także ich modyfikacją, uszkodzeniem, zniszczeniem lub utratą (utratą dostępności i integralności) – **vide art. 9a ust. 2 ustawy o systemie informacji w ochronie zdrowia;**

2. ustanowienie, wdrożenie i eksploatacja, monitorowanie i przeglądanie oraz utrzymywanie i doskonalenie systemu zarzadzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji – **vide §9 ust. 1 rozporządzenia w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostepnienia Zasobów Cyfrowych o Zdarzeniach Medycznych;**

3. uzyskanie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych (podmiotów realizujących zadania publiczne – **vide §20 ust. 2 pkt. 12 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych**

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

W praktyce, dla przykładu, to … (2)

4. zastosowanie metod i środków ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana, systematyczna analiza zagrożeń, stosowanie środków bezpieczeństwa adekwatnych do zagrożeń – **vide §86 ust. 1 i 2 rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania;**

5. **i z całą pewnością …**

wdrożenie odpowiednich środków technicznych i organizacyjnych, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyk naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienie i wadze zagrożenia,

jak i utrzymywanie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania – **vide art. 32 ust. 1 RODO;**

W praktyce …

stanowi trudne do zrealizowania powinności, które wymagają właściwej translacji języka norm prawnych na język procedur operacyjnych. Ta zaś wymaga

użycia dodatkowych informacji

zawierających odniesienie do powszechnych w użyciu dobrych praktyk zawartych w normach technicznych z zakresu zarządzania bezpieczeństwem informacji (sensu largo – np. norm serii 13k, 25k, 27k, 29k), które powinny pozwalać na powrót z języka procedur operacyjnych na język norm prawnych (formułując cele stosowania zabezpieczeń związane z zapewnieniem zgodności – vide A18 ISO/IEC 27001).

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie prawa krajowego …(1)

Postawiona teza odnajduje uzasadnienie w działaniach krajowego prawodawcy o charakterze referencyjnym w stosunku do

norm oraz uznanych w obrocie profesjonalnym standardów i metodyk związanych bezpośrednio i pośrednio z ochroną informacji:

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie prawa krajowego … (2)

§ 15. ust. 1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: **PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2**.

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012.526 ze zm.)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie prawa krajowego … (3)

§20 ust. 3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany **na podstawie Polskiej Normy PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 - w odniesieniu do ustanawiania zabezpieczeń;

2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;

3) PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012.526 ze zm.)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie prawa krajowego … (4)

§ 7. 1. W zakresie warunków organizacyjno-technicznych systemy są zgodne z przepisami wydanymi na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, a w zakresie nieuregulowanym w tych przepisach z następującymi normami, których przedmiotem są zasady gromadzenia i wymiany informacji w ochronie zdrowia:

1) PN-EN ISO 13606-1:2013 Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej,

2) PN-EN 13606:2-4:2009 Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej,

3) PN-EN ISO 13606-5:2010 Informatyka w ochronie zdrowia – Przesyłanie elektronicznej dokumentacji zdrowotnej,

4) PN-EN ISO 10781:2011 Model funkcjonalny systemu elektronicznej dokumentacji zdrowotnej

– albo normami lub wersjami norm je zastępującymi.

Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (Dz.U. 2013.1001).

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie prawa krajowego … (5)

§7 ust. 2. Systemy spełniają warunki organizacyjno-techniczne związane z jakością oprogramowania i oceną produktów programowych odpowiadające wymaganiom norm serii PN-ISO 25000 ustanowionych przez Międzynarodową Organizację Normalizacyjną (ISO), w tym norm:

1) **PN-ISO/IEC 25000:2008** Inżynieria oprogramowania – Wymagania jakości i ocena produktów programowych (SQuaRE) – Przewodnik po SQuaRE,
2) **PN-ISO/IEC 25001:2010** Inżynieria oprogramowania – Wymagania jakości i ocena produktów programowych (SQuaRE) – Planowanie i zarządzanie,
3) **PN-ISO/IEC 25020:2010** Inżynieria oprogramowania – Wymagania jakości i ocena produktów programowych (SQuaRE) – Model odniesienia dla pomiarów i przewodnik,
4) **PN-ISO/IEC 25051:2009** Inżynieria oprogramowania – Wymagania jakości i ocena produktów programowych (SQuaRE) – Wymagania jakości handlowych produktów programowych (COTS) oraz instrukcje ich testowania

– albo norm lub wersji norm je zastępujących.

Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (Dz.U. 2013.1001).

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie prawa krajowego … (6)

§9 ust. 2. System zarzadzania bezpieczeństwem informacji spełnia wymagania określone w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne dla systemu zarządzania bezpieczeństwem informacji oraz uwzględnia w zakresie zarzadzania bezpieczeństwem informacji w ochronie zdrowia następujące normy:

1) **PN-EN 14484:2005** Informatyka medyczna – Międzynarodowy przekaz medycznych danych osobowych objętych dyrektywą UE dotyczącą ochrony danych – Wysoki poziom polityki bezpieczeństwa,
2) **PN-EN 14485:2005** Informatyka medyczna – Wskazania dla operowania medycznymi danymi osobowymi w międzynarodowych aplikacjach z uwzględnieniem dyrektywy UE dotyczącej ochrony danych,
3) **PN-EN ISO 27799:2010** Informatyka w ochronie zdrowia – Zarzadzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002

– albo normy lub wersje norm je zastępujące.

Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (Dz.U. 2013.1001).

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie RODO… (1)

W odniesieniu do norm z zakresu ochrony informacji –
w zasadzie brak …

W odniesieniu do innych regulacji –

wskazanie na mechanizmy certyfikacji, kodeksy postępowania

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Działania referencyjne na gruncie RODO… (2)

Art. 32 RODO

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie **zatwierdzonego kodeksu postępowania**, o którym mowa w art. 40 lub **zatwierdzonego mechanizmu certyfikacji**, o którym mowa w art. 42.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Przywołany mechanizm certyfikacji (1)

Art. 42 RODO

1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – **do ustanawiania mechanizmów certyfikacji** oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające …

2. Certyfikacji przewidzianej w niniejszym artykule dokonują podmioty certyfikujące, o których mowa w art. 43, lub dokonuje jej właściwy organ nadzorczy – **na podstawie kryteriów zatwierdzonych przez niego** zgodnie z art. 58 ust. 3 …

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Źródła kryteriów certyfikacji (2)

Art. 17 Projektu nowej ustawy o ochronie danych osobowych

Prezes Urzędu udostępnia na swojej stronie podmiotowej Biuletynu Informacji Publicznej kryteria certyfikacji, o których mowa w art. 42 ust. 5 rozporządzenia 2016/679.

https://legislacja.rcl.gov.pl/projekt/12302950/katalog/12457690#12457690

[dostęp: 27.03.2018 r.]

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Źródła kryteriów certyfikacji (3)

Należy ich upatrywać w normalizacji …

Działania legislacyjne Unii Europejskiej wynikają z celów określonych w Agendzie Cyfrowej 2020 (filar III: Zaufanie i Bezpieczeństwo) oraz wpisują się w szereg planów działań tam opisanych i dotyczących ochrony cyberprzestrzeni, w tym:

a) Ochrony infrastruktury krytycznej z punktu widzenia ryzyk związanych z cyberbezpieczeństwem,

b) Ochrony usług komunikacji elektronicznej, jako środka wykorzystania cyberprzestrzeni do realizacji potrzeb społecznych, gospodarczych i kulturowych,

c) Zagadnień relacji między bezpieczeństwem a prywatnością, w tym ochrony praw podstawowych.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Źródła kryteriów certyfikacji (4)

Należy ich upatrywać w normalizacji …

W lipcu 2016 przyjęto Dyrektywę 2016/1148/WE3 (zwaną dalej Dyrektywą NIS) regulującą podstawowe zasady cyberbezpieczeństwa w krajach UE. W Dyrektywie NIS podkreślono znaczenie normalizacji międzynarodowej, wskazując na:

- konieczność wdrażania środków technicznych i organizacyjnych w celu zarzadzania ryzykami, na jakie narażone są sieci i systemy informatyczne, przy uwzględnieniu takich elementów, **jak zgodność z normami międzynarodowymi** (art. 16 ust. 1 tejże),

- **stosowanie europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych** jako czynnika zapewniającego spójne wdrażanie zapisów dyrektywy w obszarze określania wymagań bezpieczeństwa i zgłaszania incydentów naruszenia bezpieczeństwa (art. 19 ust. 1 tejże).

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Źródła kryteriów certyfikacji (1)

Jakie źródła dla kryteriów certyfikacji…

wniosek wydaje się być oczywisty …

Komisja przyjmując **akty wykonawcze określające techniczne standardy mechanizmów certyfikacji** oraz znaki jakości i oznaczenia w dziedzinie ochrony danych **weźmie pod uwagę europejskie lub uznane międzynarodowo normy i specyfikacje mające znaczenie dla bezpieczeństwa sieci i systemów informatycznych**.

Vide Art. 43 ust. 9 RODO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Zakres standardów ISO serii 27000 (1)

1. **PN-EN ISO/IEC 27000:2017-06** – wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia (w normie podano przegląd systemów zarządzania bezpieczeństwem informacji, terminy i definicje powszechnie stosowane w rodzinie norm SZBI);
2. **PN-EN ISO/IEC 27001:2017-06** - wersja angielska, 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, obejmuje również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Zakres standardów ISO serii 27000 (2)

1. **PN-EN ISO/IEC 27002:2017-06** - wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji (w normie podano zalecenia dotyczące standardów bezpieczeństwa informacji w organizacjach i praktyk zarządzania bezpieczeństwem informacji, w tym wyboru, wdrażania i zarządzania zabezpieczeniami, z uwzględnieniem środowiska (środowisk) w którym (których) w organizacji występuje (-ą) ryzyko(a) w bezpieczeństwie informacji;
2. **PN-ISO/IEC 27004:2017-07** - wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie bezpieczeństwem informacji -- Monitorowanie, pomiary, analiza i ocena (norma zawiera wytyczne mające pomóc organizacjom w ocenie wyników dotyczących bezpieczeństwa informacji i skuteczności systemu zarządzania bezpieczeństwem informacji w celu spełnienia wymagań normy ISO/IEC 27001: 2017;

Zakres standardów ISO serii 27000 (3)

1. **PN-ISO/IEC 27005:2014-01** - wersja polska, Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji (w normie podano wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji, rozwinięto ogólne koncepcje określone w ISO/IEC 27001, opracowano ją w celu wsparcia wdrożenia podejścia do bezpieczeństwa opartego na zarządzaniu ryzykiem;
2. **PN-ISO/IEC 27006:2016-12** - wersja polska, Technika informatyczna -- Techniki bezpieczeństwa -- Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji (w normie przedstawiono wymagania i podano wytyczne dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji (SZBI) jako uzupełnienie wymagań zamieszczonych w ISO/IEC 17021 i ISO/IEC 27001;

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Zakres standardów ISO serii 27000 (4)

1. **PN-ISO/IEC 27017:2017-07** - wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze (zawiera wytyczne dotyczące zabezpieczenia informacji mających zastosowanie w przypadku świadczenia i korzystania z usług w chmurze a mianowicie: dodatkowe wytyczne wdrażania odpowiednich środków zabezpieczeń określonych w normie ISO/IEC 27002, dodatkowe środki zabezpieczeń z wytycznymi wdrażania, które szczególnie odnoszą się do usług w chmurze;
2. **PN-ISO/IEC 27018:2017-07** - wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady ochrony danych identyfikujących osobę (PII - personally identifiable information) w chmurach publicznych działających jako przetwarzający PII (norma ustanawia powszechnie uznawane cele stosowania zabezpieczeń, zabezpieczenia oraz wytyczne do wdrażania środków ochrony danych identyfikujących osobę (PII - Personally Identifiable Information), zgodnie z pryncypiami zdefiniowanymi w normie **ISO/IEC 29100**, dla środowiska przetwarzania w chmurze.

Zakres standardów ISO serii 29000 (1)

1. **ISO/IEC 29100:2011** – wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- 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;
2. **ISO/IEC 29134** – Privacy Impact Assessment - Methodology/ Metodyka szacowania skutków dla prywatności (w normie przedstawiono wytyczne do: procesu szacowania skutków dla prywatności, oraz struktury i zawartości raportu PIA (Privacy Impact Assessment – vide art. 35 RODO – Ocena skutków dla ochrony danych);

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Zakres standardów ISO serii 29000 (2)

1. **ISO/IEC 29190:2015** - Privacy capability assessmentmodel / Model oceny zdolności do prywatności (norma zawiera ogólne wytyczne do sposobu, w jaki organizacja może ocenić swoją zdolność do zarządzania procesami związanymi z prywatnością, w szczególności opisano w niej kolejne kroki procesu oceny w celu wyznaczenia poziomu zdolności w odniesieniu do prywatności, sformułowano wytyczne co do sposobu wdrożenia procesu oceny, sformułowano wytyczne, w jaki sposób integrować prywatność [w procesach biznesowych].

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski

Zakres standardów ISO serii 29000 (2)

1. **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.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Uniwersytet Wrocławski



DZIĘKUJĘ ZA UWAGĘ

t.radziszewski@prawo.uni.wroc.pl