RODO i CYBERBEZPIECZEŃSTWO W ADMINISTRACJI

r. pr. Paweł Gruszecki

Partner, **Szef Praktyki Nowych Technologii i Telekomunikacji**.

Szczyrk, 01.06.2017r.

BusinessLawFirm

kochański zięba i partnerzy

KALENDARIUM

NIS	RODO
Data opublikowania w Dzienniku Urzędowym Unii Europejskiej – **19 lipiec 2016 r.**	Data opublikowania w Dzienniku Urzędowym Unii Europejskiej **– 4 maj 2016 r.**
Przyjęcie i publikacja przepisów w państwach członkowskich – **do 9 maja 2018 r.**	Stosowanie rozporządzenia - **od 25 maja 2018 r.**
Stosowanie przepisów – **od 10 maja 2018 r.**	Uchylenie Dyrektywy 95/46/WE ze skutkiem od dnia **25 maja 2018 r.**
Przewidywany czas opracowania projektu przepisów polskich – **?**	W marcu 2017r. został przedstawiony projekt ustawy uzupełniającej/dopełniającej RODO.
	Pomiędzy kwietniem 2017r., a czerwcem 2017r. ma zostać przedstawiony tzw. „pakiet legislacyjny" obejmujący zmiany w ustawach sektorowych, w tym Ustawie o działalności ubezpieczeniowej i reasekuracyjnej/ Ustawie Prawo bankowe.

9 maja 2017 r. została podpisana uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.

Przepisy uzupełniające RODO w zakresie działania administracji

Jeżeli chodzi o przetwarzanie danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, **państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące stosowanie przepisów niniejszego rozporządzenia.**

Co może regulować nowa ustawa dopełniająca ?

Funkcjonowanie **organu nadzorczego**

Zabezpieczenia proceduralne do nakładania **administracyjnych kar pieniężnych**

Możliwość przyznania przyszłemu organowi ochrony danych osobowych **uprawnienia** do opracowywania **dobrych praktyk dotyczących technicznych i organizacyjnych standardów**, zapewniających zgodne z prawem przetwarzanie danych osobowych - wykazy dobrych praktyk powinny w takim przypadku podlegać **okresowej aktualizacji** i być sporządzane z uwzględnieniem specyfiki działań różnego rodzaju przedsiębiorców.

Czy każdy administrator bezpieczeństwa informacji zarejestrowany do 25 maja 2018 r. **z mocy prawa staje się inspektorem ochrony danych** (projekt GIODO) ?

Możliwa sprzeczność z art. 37 RODO, w myśl którego IOD ma zostać wyznaczony.

Poszukiwania kompromisu: przez okres przejściowy administratorzy bezpieczeństwa informacji pełnią funkcję inspektora ochrony danych **do momentu zgłoszenia** ich danych kontaktowych do organu ochrony danych przez wyznaczającego ich administratora.

Jaka jest forma i termin notyfikacji IOD przez ADMINISTRATORA/PROCESORA ?

Czy powyższe informacje podlegają aktualizacji ?

Jeżeli tak – to w jakim zakresie ?

KRAJOWE RAMY POLITYKI CYBERBEZPIECZEŃSTWA - PLANOWANE DZIAŁANIA (I)

- przegląd istniejących przepisów prawa (w tym regulacji sektorowych) w celu ich harmonizacji, zwiększenia efektywności działania i poprawy przepływu informacji pomiędzy wszystkimi interesariuszami zaangażowanymi w aktywne budowanie krajowego systemu cyberbezpieczeństwa;

- wdrożenie Dyrektywy NIS;

WŁĄCZENIE

- zapewnienie skuteczności krajowego systemu cyberbezpieczeństwa wymaga **włączenia do niego sektora publicznego oraz telekomunikacyjnego**, a także **uwzględnienia kwestii związanych z usługami zaufania i usługami publicznym**i świadczonymi przez sektor prywatny.

CEL:

- wysoki poziom odporności: (A) krajowych systemów teleinformatycznych, (2) operatorów usług kluczowych, (3) operatorów infrastruktury krytycznej, (4) dostawców usług cyfrowych oraz (5) **administracji publicznej**.

KRAJOWE RAMY POLITYKI CYBERBEZPIECZEŃSTWA - PLANOWANE DZIAŁANIA (II)

- ustanowienie **Narodowego Centrum Cyberbezpieczeństwa (NCC),** CSIRT Narodowego, sektorowych zespołów reagowania na incydenty (CSIRT sektorowe), centrów wymiany i analizy informacji;

- doprecyzowanie **wzajemnych powiązań** pomiędzy poszczególnymi interesariuszami krajowego systemu cyberbezpieczeństwa, w tym organów odpowiedzialnych za bezpieczeństwo narodowe, działania antyterrorystyczne, bezpieczeństwo wewnętrzne oraz porządek publiczny, prokuraturę oraz sądownictwo;

KLASTRY BEZPIECZEŃSTWA

- rząd w ramach współpracy administracji rządowej z administracją samorządową będzie **rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie tworzenia klastrów bezpieczeństwa dla tej administracji (bezpieczne sieci typu intranet, oferujące połączenia wewnątrz sieci, usługi bezpieczeństwa oraz bezpieczny dostęp do sieci Internet).**

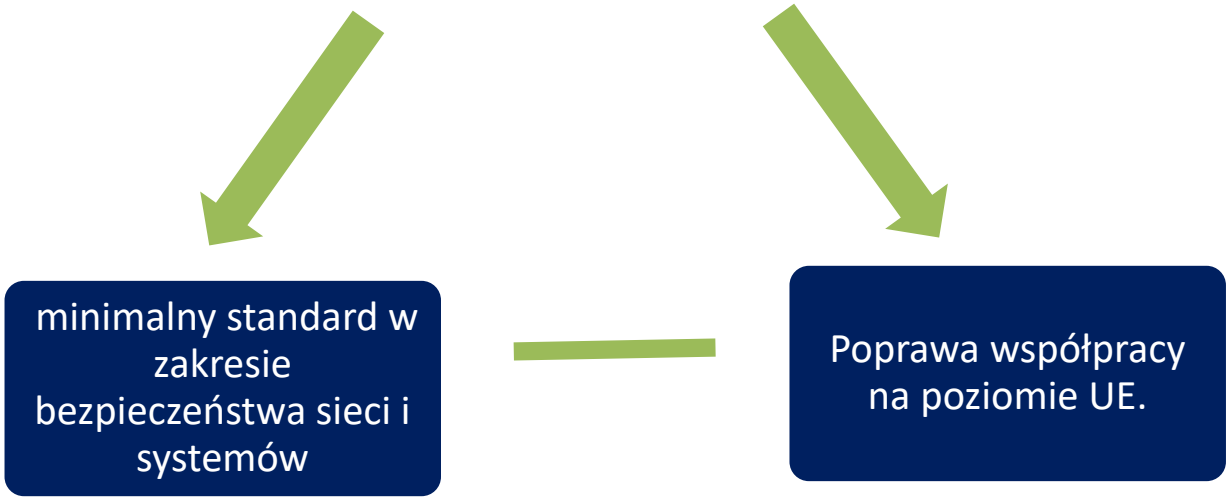
KRAJOWE RAMY POLITYKI CYBERBEZPIECZEŃSTWA - PLANOWANE DZIAŁANIA (III)

Na wszystkich etapach życia systemu teleinformatycznego, w odniesieniu do zapewnienia bezpieczeństwa tych systemów, zastosowanie powinny mieć **Polskie Normy, normy międzynarodowe**, powszechnie uznawane standardy, a także tak zwane dobre praktyki;

Na potrzeby zarządzania bezpieczeństwem państwa w cyberprzestrzeni opracowana zostanie **spójna metodyka szacowania ryzyka**, uwzględniająca specyfikę poszczególnych sektorów;

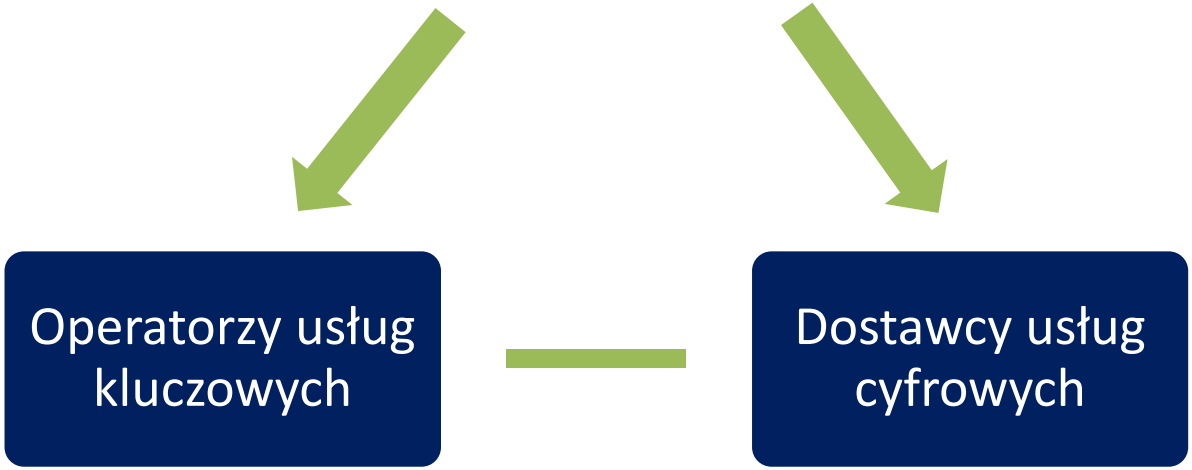
Partnerstwo publiczno-prywatne.

Przedmiot regulacji NIS



odporność sieci i systemów informatycznych na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne.

Kategorie podmiotów objętych regulacją



Wystarczy, że dostawca oferuje usługi w UE.

Nie dotyczy mikroprzedsiębiorstw (do 10/ do 2 mln EURO) oraz małych przedsiębiorstw (do 50/ do 10 mln EURO).

Dostawca usługi cyfrowej czyli (...)

1
- Osoba prawna
- Świadczy usługi cyfrowe

2
- Usługi cyfrowe to usługi świadczone za wynagrodzeniem, na odległość drogą elektroniczną, na ind. żądanie odbiorcy .

3
- Usługi należą do kategorii: wyszukiwarka, internetowa platforma handlowa, usługa przetwarzania w chmurze.

Internetowa platforma handlowa czyli (...)

- Umożliwianie zawarcia umów online B2B i/lub B2C (umów online sprzedaży oraz o świadczenie usług).

Booking.com

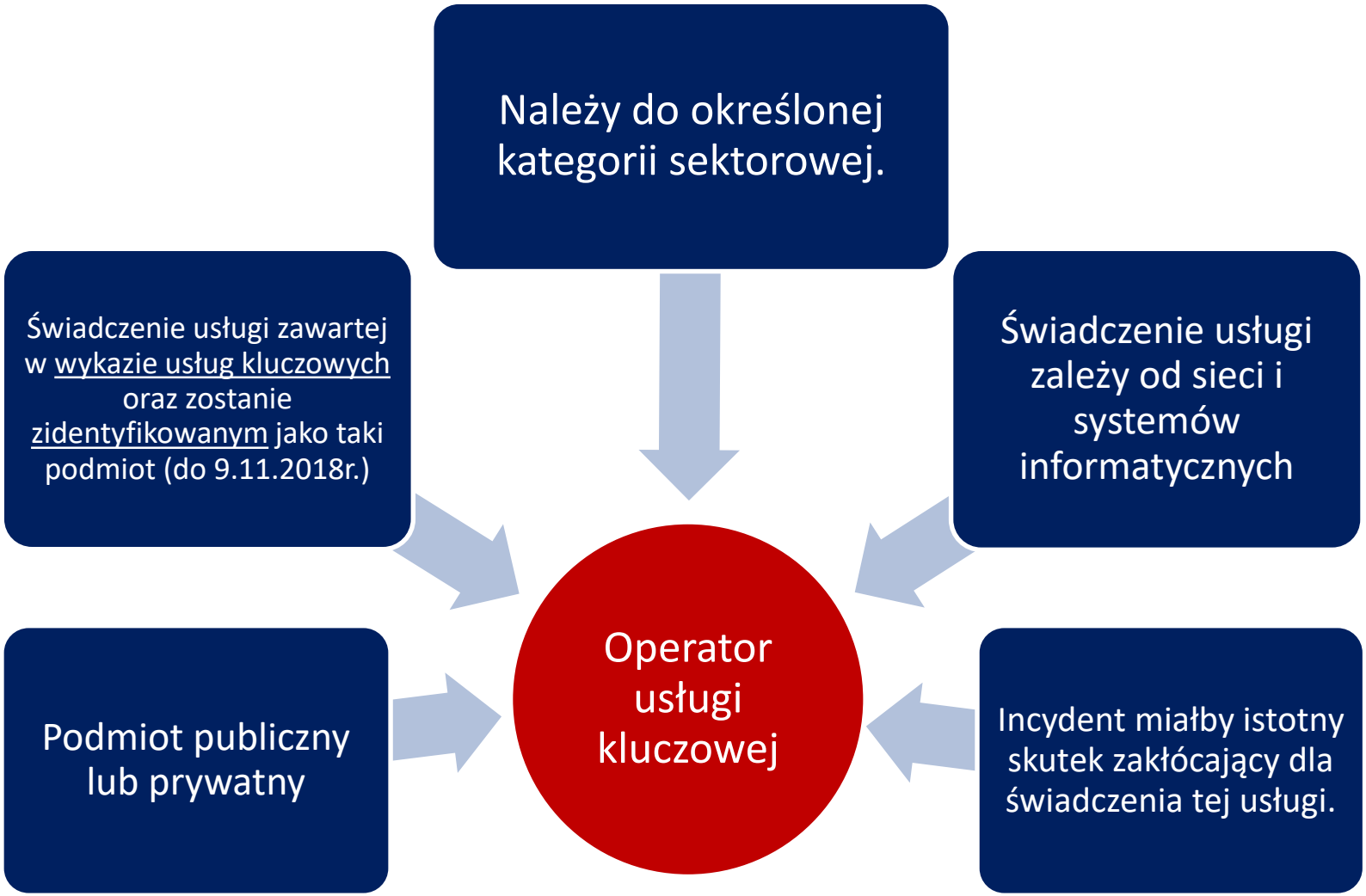
Google Play

Alibaba.com

UBER

Usługa przetwarzania w chmurze czyli (...)

usługa cyfrowa umożliwiająca dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania.


Należy do określonej kategorii sektorowej.
Świadczenie usługi zawartej w wykazie usług kluczowych oraz zostanie zidentyfikowanym jako taki podmiot (do 9.11.2018r.)
Świadczenie usługi zależy od sieci i systemów informatycznych
Operator usługi kluczowej
Podmiot publiczny lub prywatny
Incydent miałby istotny skutek zakłócający dla świadczenia tej usługi.

Sektory objęte regulacją:

Energetyka

Transport

- lotniczy: przewoźnicy lotniczy, zarządzający portem lotniczym, jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych, operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC).
- kolejowy: zarządcy infrastruktury kolejowej, przedsiębiorstwa kolejowe.
- wodny: armatorzy śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów, organy zarządzające portami, jednostki wykonujące prace i operujące sprzętem znajdującym się w tych portach, operatorzy systemów ruchu statków.
- drogowy: organy zarządzające ruchem drogowym, operatorzy ITS.

Instytucje kredytowe

Infrastruktura rynków finansowych

Służba zdrowia (szpitale i prywatne kliniki)

Zaopatrzenie w wodę pitną i jej dystrybucja

Infrastruktura cyfrowa (IXP, dostawcy usług DNS, rejestry nazw TLD).

Obowiązki operatorów usług kluczowych	Obowiązki dostawców usług cyfrowych
Podejmowanie odpowiednich i proporcjonalnych środków w celu zarządzania ryzykami. Środki te muszą zapewniać poziom bezpieczeństwa odpowiedni do istniejącego ryzyka.	**Określanie** i podejmowanie odpowiednich i proporcjonalnych środków w celu zarządzania ryzykami. Środki te muszą zapewniać poziom bezpieczeństwa odpowiedni do istniejącego ryzyka **oraz uwzględniać następujące elementy:** **a) bezpieczeństwo systemów i obiektów;** **b) postępowanie w przypadku incydentu;** **c) zarządzanie ciągłością działania;** **d) monitorowanie, audyt i testowanie;** **e) zgodność z normami międzynarodowymi.**

Obowiązki operatorów usług kluczowych	Obowiązki dostawców usług cyfrowych
Podejmowanie odpowiednich środków zapobiegających i minimalizujących wpływ incydentów z myślą o zapewnieniu ciągłości usług.	Podejmowanie środków zapobiegających i minimalizujących wpływ incydentów z myślą o zapewnieniu ciągłości usług.
Niezwłoczne zgłaszanie właściwemu organowi lub CSIRT incydentów **mających istotny wpływ na ciągłość** świadczonych przez nich usług kluczowych. Zgłoszenia muszą zawierać informacje umożliwiające określenie transgranicznego wpływu incydentu. Zgłoszenie nie może narażać strony zgłaszającej na zwiększoną odpowiedzialność.	Zgłaszanie bez zbędnej zwłoki właściwemu organowi lub CSIRT wszelkich incydentów mających istotny wpływ na świadczenie usługi, o której mowa w załączniku III. Zgłoszenia muszą zawierać informacje umożliwiające określenie istotności wpływu transgranicznego. Zgłoszenie nie może narażać strony zgłaszającej na zwiększoną odpowiedzialność

Obowiązki operatorów usług kluczowych	Obowiązki dostawców usług cyfrowych
Istotność wpływu danego incydentu, zależy od: a) liczby użytkowników, których dotyczy zakłócenie usługi kluczowej; b) czas trwania incydentu; c) zasięg geograficzny związany z obszarem, którego dotyczy incydent.	Istotność wpływu danego incydentu zależy od: a) liczby użytkowników, których dotyczy incydent, **w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług;** b) czas trwania incydentu; c) zasięg geograficzny, którego dotyczy incydent; **d) zasięg zakłócenia funkcjonowania usługi;** **e) zasięg wpływu na działalność gospodarczą i społeczną.** **Obowiązek zgłoszenia incydentu ma zastosowanie wyłącznie wówczas, gdy dostawca usług cyfrowych ma dostęp do informacji niezbędnych do oceny wpływu incydentu względem parametrów, o których mowa w akapicie pierwszym.**

Obowiązki operatorów usług kluczowych	Obowiązki dostawców usług cyfrowych
	Zgłoszenie operatorowi usług kluczowych, zależnemu od dostawcy usług cyfrowych w zakresie usługi, która ma istotne znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, wszelkiego istotnego wpływu na ciągłość usług kluczowych związanego z incydentem, który dotyczy dostawcy usług cyfrowych.

Ogólne rozporządzenie o ochronie danych osobowych – wybrane aspekty prawne.

r. pr. Paweł Gruszecki

Partner, **Szef Praktyki Nowych Technologii i Telekomunikacji**.

Szczyrk, 01.06.2017r.

Żądanie ujawnienia danych osobowych przez organ.

Organy publiczne, **którym ujawnia się dane osobowe** w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), **nie powinny być traktowane jako odbiorcy,** jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. **Żądanie ujawnienia danych osobowych,** z którym występują takie organy publiczne, powinno zawsze mieć **formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.**

BusinessLawFirm

kochański zięba i partnerzy

System zarządzania ryzykiem prawnym w zakresie ochrony danych osobowych.

BusinessLawFirm

kochański zięba i partnerzy

Rewizja umów/nowe polityki/ szablony/schematy oceny skutków/rejestr czynności przetwarzania/nowe klauzule zgody

Brak rejestracji zbiorów.

Wybór środków technicznych i organizacyjnych odpowiednich do ryzyka.

Ocena skutków przetwarzania

Np. Prywatność na etapie projektowania/regulacja profilowania .

Powołanie IOD/przedstawiciela.

PRZYPISANIE RÓL	Artykuł RODO
Wyznaczenie **przedstawiciela (dotyczy podmiotu mającego siedzibę poza UE).**	27
Wyznaczenie **inspektora ochrony danych** (IOD) do pełnienia niezależnego nadzoru	37, 38
Posiadanie **ról i obowiązków** dla podmiotów odpowiedzialnych za bezpieczeństwo danych osobowych (np. opisy stanowisk)	39
Regularna komunikacja pomiędzy osobami zajmującymi się prywatnością, prywatnością sieci oraz innymi osobami odpowiedzialnymi za prywatność danych osobowych	38

Podstawy przetwarzania

Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
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;
Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze
Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorów
przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Obowiązki prawodawcy

Prawo Unii lub prawo państwa członkowskiego powinno określać także **cel przetwarzania**. Ponadto prawo to może **doprecyzowywać A. ogólne warunki określone w niniejszym rozporządzeniu dotyczące zgodności przetwarzania z prawem, B. określać sposoby wskazywania administratora, C. rodzaj danych osobowych podlegających przetwarzaniu, D. osoby, których dane dotyczą, E. podmioty, którym można ujawniać dane osobowe, F. ograniczenia celu, G.okres przechowywania oraz I. inne środki zapewniające zgodność z prawem i rzetelność przetwarzania.** Prawo Unii lub prawo państwa członkowskiego powinno określać także, **czy administratorem** wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, na przykład zrzeszenie zawodowe, jeżeli uzasadnia to interes publiczny, w tym cele zdrowotne, takie jak zdrowie publiczne, ochrona socjalna oraz zarządzanie usługami opieki zdrowotnej.

Nowe zasady ochrony danych – prywatność na etapie projektowania

Konieczność uwzględnienia ochrony danych osobowych na etapie **tworzenia i komponowania danej usługi/procesu**.

Wdrożenie **odpowiednich do zagrożeń** środków technicznych i organizacyjnych (np. **pseudonimizacja na możliwie najwcześniejszym etapie procesu**, szyfrowanie, zapewnienie poufności, integralności, dostępności i odporności systemów).

Zdaniem ENISA do środków organizacyjnych należy:

- minimalizacja zbieranych danych;
- ukrywanie danych oraz zależności pomiędzy nimi dla osób posiadających dostęp;
- separowanie danych (przetwarzane dane są rozdzielone – rozproszone);
- agregacja – dane są przetwarzane w możliwie najwyższym stopniu zagregowania i z możliwie najmniejszą liczbą szczegółów (przy jakiej są wciąż użyteczne).

Obowiązek ma charakter uprzedni i ciągły

Uwzględnienie stanu wiedzy technicznej, kosztów wdrażania, celu przetwarzania, ryzyka naruszenia praw i wolności, wagi zagrożenia – w przypadku większej wagi stosujemy **więcej środków lub środki bardziej zaawansowane** co może dotyczyć np. **profilowania**, danych biometrycznych, przetwarzania danych dzieci.

Dane osobowe

Imię (*):

Nazwisko:

Płeć (*): Mężczyzna Kobieta

Email (*):

Data urodzenia: (rrrr.mm.dd)

ul.: nr /

Kod pocztowy:

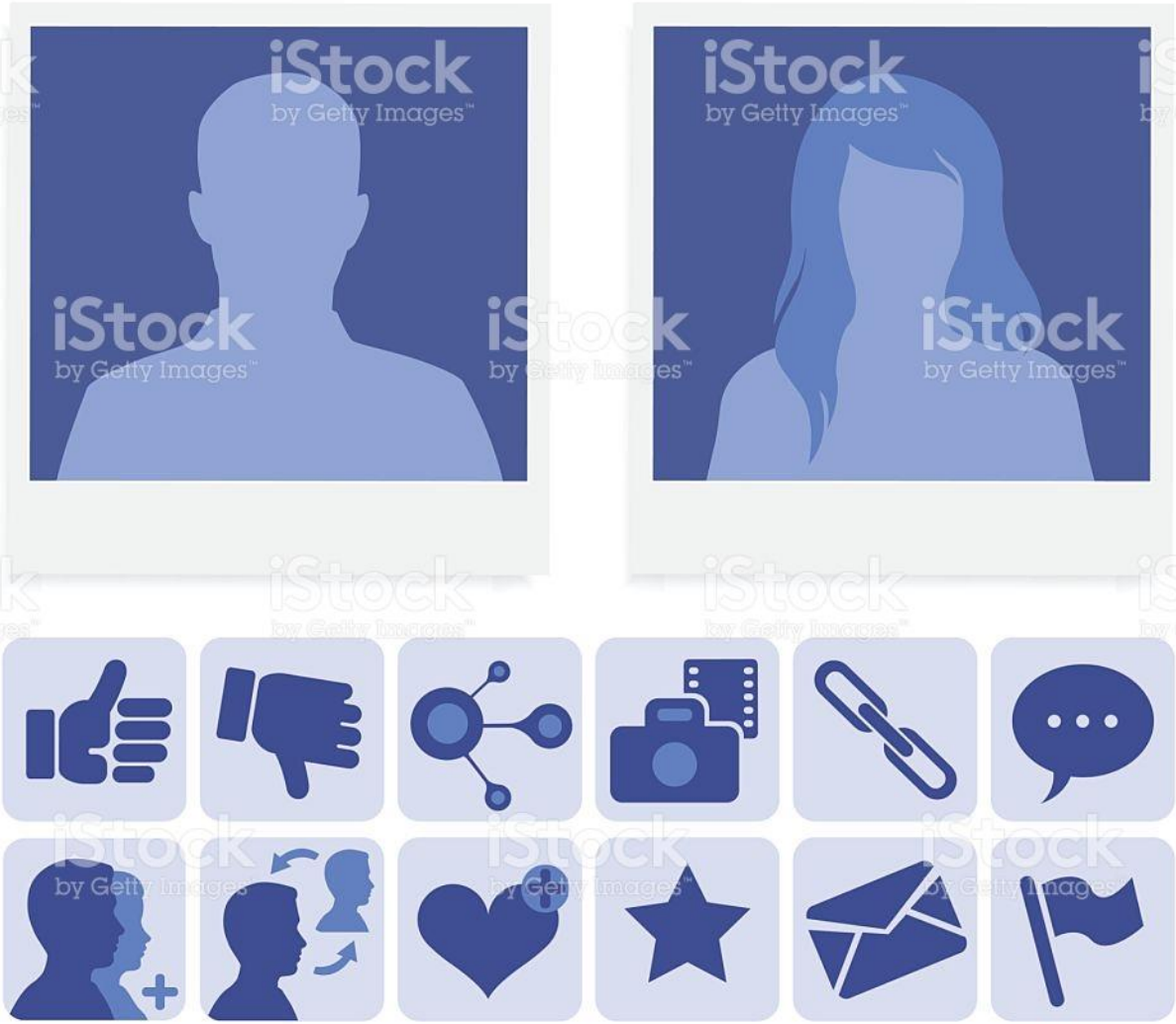
Miasto:

Województwo (*): ---------

Uwagi:

Zainteresowania: Sport Muzyka Turystyka Literatura

Wyślij Wyczyść


iStock
by Getty Images

Nowe zasady ochrony danych – prywatność na etapie projektowania

Podejście proaktywne
Prywatność jako ustawienie domyślne
Prywatność włączona w projekt
Pełna funkcjonalność
Ochrona prywatności od początku do końca cyklu życia informacji
Transparentność i przejrzystość
Poszanowanie dla prywatności użytkowników.

Przetargi publiczne

Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych.

Przetwarzanie danych dziecka

Jeżeli dziecko nie ukończyło 16 lat, przetwarzanie na podstawie zgody jest dopuszczalne wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

W takich przypadkach administrator, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

BusinessLawFirm

Brak zakazu profilowania – tylko ograniczenie podstaw prawnych.

kochański zięba i partnerzy

Nowe zasady ochrony danych – profilowanie.

ZASADA:

Prawo podmiotu danych do **niepodlegania decyzji**, która: (1) opiera się *wyłącznie* na **zautomatyzowanym przetwarzaniu** (w tym profilowaniu) oraz która to decyzja (2) wywołuje wobec osoby, której dane dotyczą **skutki prawne** lub w **inny podobny sposób na nią wpływa**.

WYJĄTKI:

1. Decyzja jest **niezbędna do zawarcia lub wykonania umowy** pomiędzy osobą, której dane dotyczą, a administratorem danych;
2. Jest ona **dozwolona prawem** UE lub też prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony.
3. Decyzja opiera się na **wyraźnej zgodzie** podmiotu.

Dotyczy **tylko** podejmowania decyzji na podstawie profili.
Tworzenie profili – **szerszy katalog podstaw**

Nowe zasady ochrony danych – profilowanie.

Obowiązek informacyjny:

- Fakt podejmowania decyzji w sposób zautomatyzowany;
- Zasady podejmowania decyzji;
- Znaczenie i przewidywane konsekwencje przetwarzania.

Nie dokonuje jej IOD. IOD jedynie konsultuje, udziela zaleceń, monitoruje oraz jest punktem kontaktowym.

OCENA SKUTKÓW

Dotyczy nie przetwarzania samego w sobie ale **poszczególnych operacji** na danych związanych z wprowadzeniem nowej usługi, aplikacji lub wdrożeniem nowego systemu IT **jeżeli dochodzi do zmiany warunków przetwarzania;**

Przewidywanie niekorzystnych skutków operacji dla podmiotów danych;

Obowiązkowa w przypadku **wysokiego ryzyka** (samodzielna ocena), w tym m.in..:

- prowadzenia **systematycznej, kompleksowej oceny** czynników osobowych dot. osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu i jest podstawą decyzji wywołującej skutki prawne dla osoby fizycznej lub w podobny sposób znacząco wpływającej na nią;
- przetwarzania **na dużą skalę szczególnych** kategorii danych osobowych w celu zidentyfikowania osoby fizycznej;
- przetwarzania **objętego wykazem** ustalonym przez organ nadzorczy.

Co zawiera OCENA SKUTKÓW ?

Systematyczny opis planowanych operacji i celów przetwarzania;
Ocena tego czy operacje są niezbędne oraz adekwatne;
Ocena ryzyka naruszenia praw i wolności (ryzyko zwykłe lub wysokie)
Środki planowane w celu zaradzenia ryzyku.

Obowiązek przeprowadzenia **konsultacji** z organem nadzorczym, który ma 8 tygodni na reakcję tj. (1) ostrzeżenie, (2) nakazanie dostosowania operacji, (3) wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania, (4) nałożenie kary pieniężnej, (5) udzielenie porady.

Przetwarzanie na dużą skalę szczególnych kategorii danych np. danych o zdrowiu.

OBOWIĄZKI IOD (personel ADM/PROC albo umowa o świadczenie usług).

informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

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;**

współpraca z organem nadzorczym;

pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

udzielanie na żądanie **zaleceń co do oceny skutków** dla ochrony danych oraz monitorowanie jej wykonania.

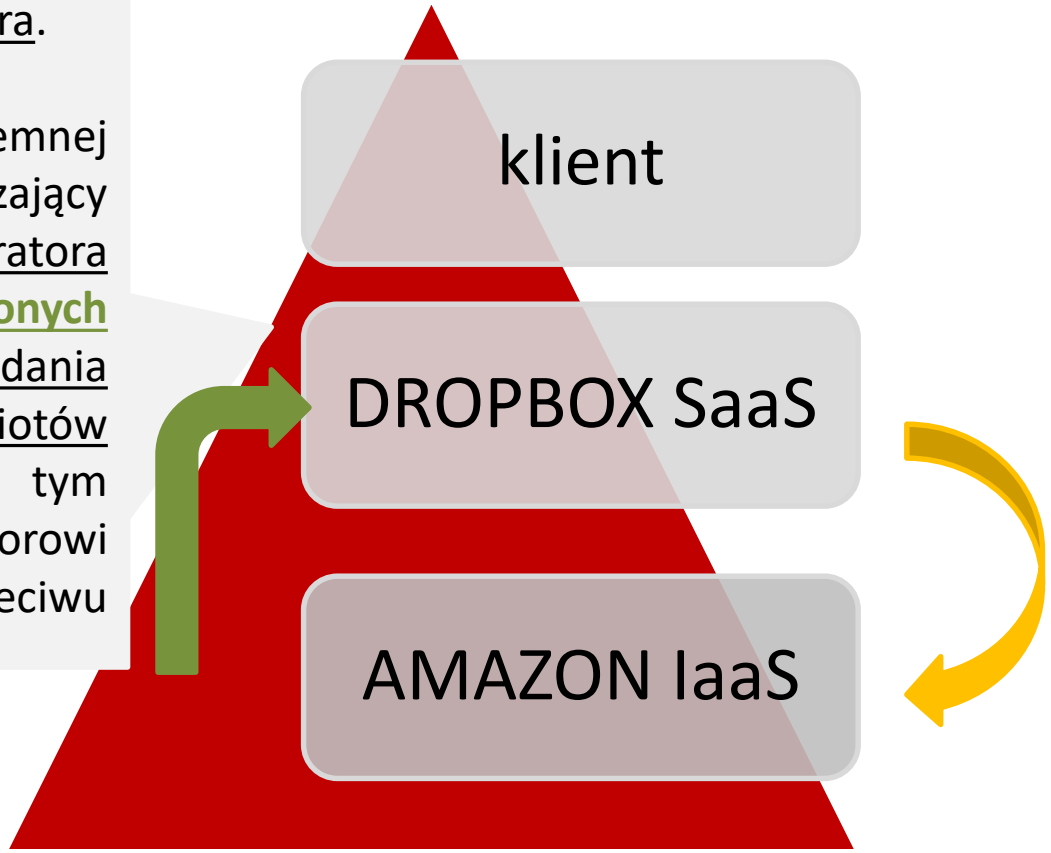
WYBRANE PROCEDURY (I)	Artykuł RODO
Procedury dot. zbierania i wykorzystania wrażliwych danych osobowych (w tym biometrycznych)	9,10
Procedury dot. zbierania oraz wykorzystywania danych osobowych dzieci oraz nieletnich	8, 12
Procedury dla utrzymania jakości danych (zasady dot. przetwarzania danych)	5
Posiadanie procedury dot. pseudonimizacji danych osobowych (np. dla celów statystycznych).	89
Procedury ponownego wykorzystania danych osobowych	6, 13

WYBRANE PROCEDURY (II)	Artykuł RODO
Procedury odpowiedzi na **żądanie dostępu do danych osobowych**	15
Procedura **odpowiedzi na żądanie i/lub dostarczenie sposobu indywidualnego aktualizowania oraz poprawiania swoich danych osobowych**	16, 19
Procedura **odpowiedzi na żądanie zaprzestania, ograniczenia przetwarzania lub zgłoszenia zastrzeżenia do przetwarzania**	7, 18, 19, 21
Procedura odpowiedzi na żądanie przenoszenia danych	20
Procedura odpowiedzi na żądanie realizacji prawa do bycia zapomnianym lub usunięcia danych.	17, 19

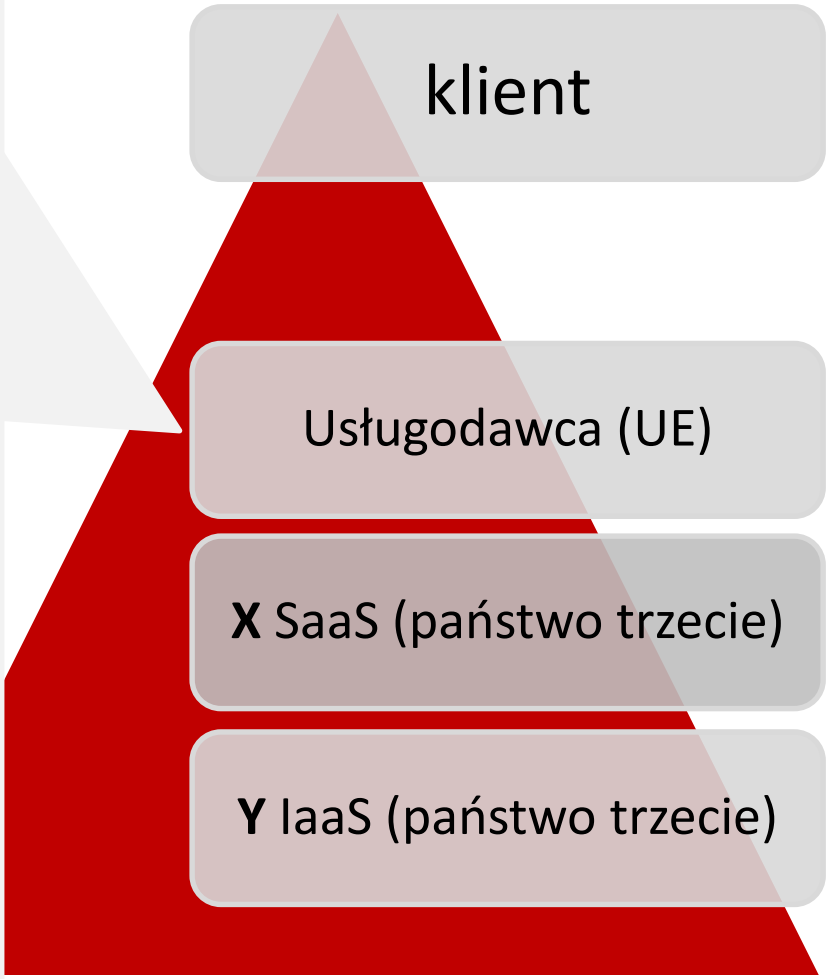
WYBRANE PROCEDURY (III)	Artykuł RODO
Plan reagowania na incydenty/naruszenia prywatności danych osobowych	33, 34
Schemat powiadamiania o naruszeniu **podmiotów danych** oraz zgłaszania naruszenia **do organów nadzorczych**.	12, 33, 34
Rejestr śledzenia incydentów naruszenia prywatności danych (dokumentacja)	33

Podmiot przetwarzający **nie korzysta** z usług innego podmiotu przetwarzającego bez **uprzedniej szczegółowej** lub **ogólnej** pisemnej zgody administratora.

W przypadku ogólnej pisemnej zgody podmiot przetwarzający **informuje** administratora o wszelkich **zamierzonych zmianach** dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

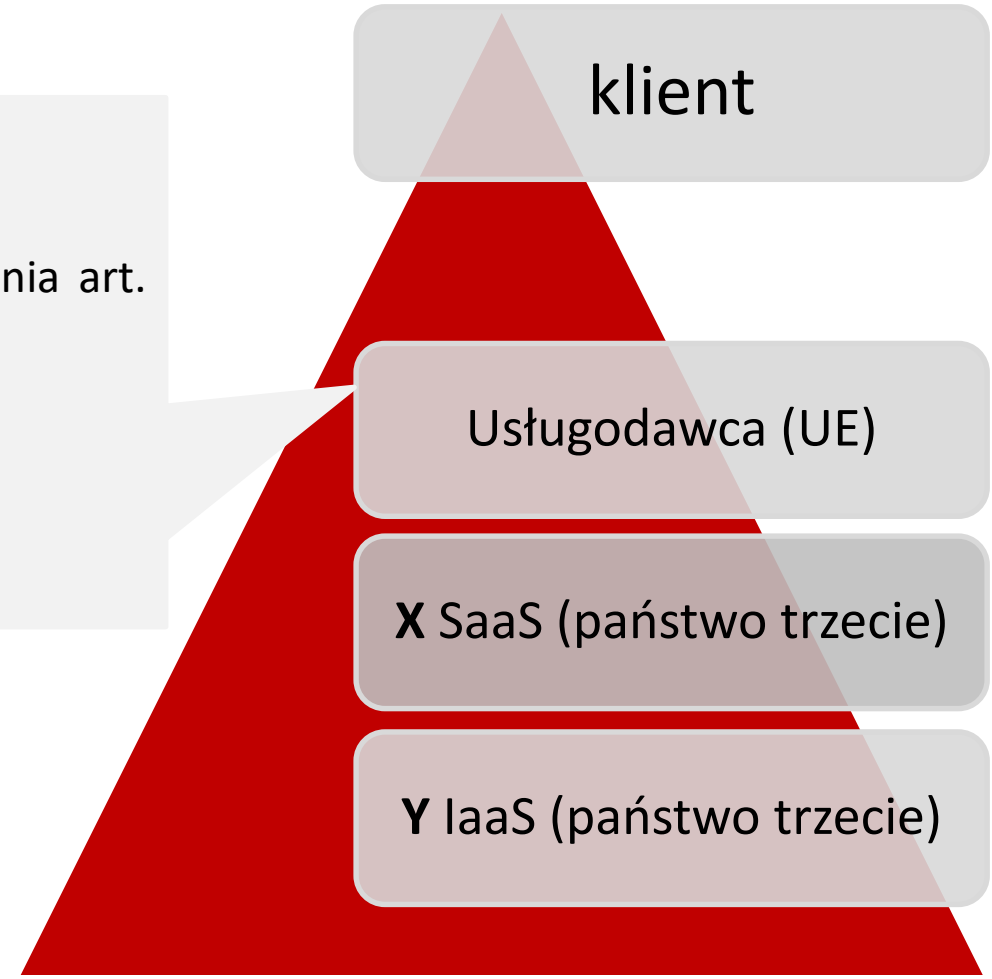


Korzysta wyłącznie z usług takich podmiotów przetwarzających, które **zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia** i chroniło prawa osób, których dane dotyczą.



Zróżnicowane poziomy ochrony poszczególnych danych.

Czy stosujemy postanowienia art. 28 RODO wobec X oraz Y ?



NOWA DOKUMENTACJA - UMOWA POWIERZENIA PRZETWARZANIA DANYCH

UODO	RODO
- powierzenie przetwarzania na podstawie **pisemnej umowy**; - przetwarzanie możliwe tylko **w zakresie i celu** przewidzianym w umowie; - obowiązek podjęcia środków zabezpieczających przez rozpoczęciem przetwarzania; - w zakresie przepisów dot. środków zabezpieczających podmiot przetwarzający ponosi **odpowiedzialność jak administrator danych**. - odpowiedzialność za przestrzeganie przepisów dot. przetwarzania ponosi administrator. Jednak nie wyłącza to odpowiedzialności podmiotu przetwarzającego za przetwarzanie niezgodne z umową; - Możliwe jest podpowierzenie przetwarzania, na tych samych zasadach co powierzenie pierwotne;	- powierzenie przetwarzania na podstawie **umowy** lub innego instrumentu prawnego obowiązujących w danym państwie członkowskim; dla umowy RODO przewiduje **formę pisemną**, w tym elektroniczną; - **umowa ma określać**: • przedmiot i czas trwania przetwarzania, • charakter i cel przetwarzania, • rodzaj danych osobowych, • kategorie osób których dane dotyczą, • prawa i obowiązki administratora. - ponadto umowa ma stanowić, że podmiot przetwarzający: • **przetwarza dane wyłącznie na udokumentowane polecenie administratora,** • zapewnia zachowanie tajemnicy, • **pomaga w spełnieniu obowiązku realizacji praw osób, których dane są przetwarzane,**

NOWA DOKUMENTACJA - UMOWA POWIERZENIA PRZETWARZANIA DANYCH

UODO	RODO
	• **<u>po zakończeniu usług przetwarzania usuwa lub zwraca dane i/lub ich kopie</u>,** • wdraża odpowiednie środki techniczne i organizacyjne , • pomaga administratorowi wywiązywać się z obowiązków zapewnienia bezpieczeństwa danych. • **<u>niezwłocznie informuje o incydencie.</u>** - podmiot przetwarzający ma gwarantować wdrożenie odpowiednich środków technicznych i organizacyjnych; - możliwe jest podpowierzenie przetwarzana danych, wtedy na wskazany podmiot nałożone zostają te same obowiązki jakie obowiązują procesora pierwotnego. Odpowiedzialność za podpowierzenie spoczywa na podmiocie który ustanowił to podpowierzenie **(FLOW – DOWN);** - gwarancje wdrożenia odpowiednych środków technicznych i organizacyjnych można wykazać poprzez stosowanie zatwierdzonego **kodeksu postępowania** (art. 40) lub zatwierdzonego **mechanizmu certyfikacji** (art. 42); - umowa lub inny akt prawny powierzenia przetwarzania danych może się opierać (w całości lub części) na standardowych klauzulach umownych (BCR, art. 28 ust. 7, 8);

Jak zrealizować to w praktyce ? - NIS

- ENISA, we współpracy z państwami członkowskimi, opracowuje **porady i wytyczne** dotyczące kwestii technicznych, które powinny zostać wzięte pod uwagę **a także dotyczące już istniejących norm**, w tym krajowych norm państw członkowskich.

„Technical Guidelines for the implementation of minimum security measures for Digital Service Providers" – 17.02.2017r.

- przyjęcie jednego z **3 standardów bezpieczeństwa** (podstawowy, sektorowy oraz najwyższy).

- **27 celów bezpieczeństwa** do spełnienia.

- każdemu celowi służą poszczególne **środki bezpieczeństwa**

- Najczęściej przywoływane normy: ISO 27001 / CCS / OCF / BSI C5

Przyjęcie polityki bezpieczeństwa	Monitorowanie usług
Zarządzanie ryzykiem (lista ryzyk, uświadomienie ryzyk, metodologia, podział ról i obowiązków, procedury, przewodnik dla pracowników, przegląd metodologii).	Raportowanie o incydentach
Ustanowienie konkretnych stanowisk	Ciągłość działania (business continuity).
Standardy bezpieczeństwa w zakresie umów z dostawcami i klientami.	Przywrócenie usługi w razie katastrofy (disaster recovery).
Sprawdzanie zatrudnianych pracowników (screening)	Testowanie systemów
Zapewnienie wiedzy o bezpieczeństwie	Procedury oceny bezpieczeństwa
Bezpieczeństwo w trakcie zmiany/opuszczania stanowisk pracy.	Polityka sprawdzania i wprowadzania zgodności z przepisami obowiązującymi na terytorium UE , danego kraju, a także najlepszymi praktykami i standardami.
Bezpieczeństwo fizyczne	Bezpieczeństwo przechowywanych danych.
Bezpieczeństwo infrastruktury towarzyszącej	Bezpieczeństwo interfejsów.
Kontrola dostępu do sieci oraz systemów	Bezpieczeństwo oprogramowania.
Integralność elementów sieci oraz systemów	**Interoperacyjność i przenośność (np. procedura fall –back).**
Procedury operacyjne	Zapewnienie klientowi prawa do monitorowania usługi
Zarządzanie zmianą	Zarządzanie assetami.
Wykrywanie incydentów i zarządzanie nimi	

Jak zrealizować to w praktyce ? - RODO

Zamiast rozporządzenia technicznego

W ramach samodzielnej oceny:

- Pomocnicze stosowanie np. **Normy** PN-ISO 27001 (podczas wdrażania analiza ryzyka opisana w Normie ISO 27005).
- Pomocnicze stosowanie zaleceń **Raportów ENISA** np. *„Prywatność i ochrona danych w fazie projektowania – od polityki do inżynierii”*.
- Pomocnicze stosowanie **zatwierdzonych** kodeksów postępowania (fakultatywnych).
- Pomocnicze stosowanie **akredytowanych** mechanizmów certyfikowania/znaków jakości (wydawanych przez organizacje nie tylko PL).
- Stosowanie wytycznych i zaleceń Europejskiej Rady Ochrony Danych Osobowych

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES[17]
SO1 Information Security Policy	●	●	●		●	●	●	●	
SO2 Risk management	●	●	●		●	●	●	●	
SO3 Security roles	●	●	●		●	●	●	●	
SO 04 Security in supplier relationships	●	●	●		●	●	●	●	
SO 05 Background checks	●	●	●		●	●	●	●	
SO 06 Security knowledge and training	●	●	●	●	●	●	●	●	
SO 07 Personnel changes	●	●	●		●	●	●	●	
SO 08 Physical and environmental security	●	●	●		●	●	●	●	
SO 09 Security of supporting utilities	●		●		●	●			
SO 10 Access control to network and information systems	●	●	●	●	●	●	●	●	●
SO 11 Integrity of network and information systems	●		●		●	●	●	●	●
SO 12 Operating procedures	●				●	●			●
SO 13 Change management	●	●	●	●	●	●	●	●	●
SO 14 Asset management	●	●	●	●	●	●	●	●	●
SO 15 Security incident detection & response	●	●	●	●	●	●	●	●	
SO 16 Security incident reporting	●	●	●	●	●	●	●	●	
SO 17 Business continuity	●	●	●		●	●	●	●	

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES[17]
SO 18 Disaster recovery capabilities	●	●	●	●	●	●	●	●	
SO 19 Monitoring and logging policies	●	●	●		●	●	●	●	●
SO 20 System tests	●		●		●	●	●	●	●
SO 21 Security assessments	●	●	●		●	●		●	●
SO 22 Compliance	●	●	●		●	●			
SO 23 Security of data at rest	●	●	●	●	●	●	●	●	●
SO 24 Interface security		●	●		●	●		●	●
SO 25 - Software security		●	●		●	●	●	●	
SO 26 Interoperability and portability		●	●		●	●			
SO 27 Customer monitoring and log access	●	●	●	●	●	●	●	●	●

Stosowanie norm w zakresie cyberbezpieczeństwa.

- państwa członkowskie, nie narzucając ani nie faworyzując wykorzystywania określonego rodzaju technologii, **powinny zachęcać** do stosowania **europejskich lub uznanych międzynarodowo norm i specyfikacji** mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych (opis: *„Normy jako podstawa do opracowywania i wdrażania standardów bezpieczeństwa teleinformatycznego w projektach realizowanych przez MC w ramach POPC.”* z dnia 30.03.2017r.).

- zagadnieniami normalizacji w obszarze cyberbezpieczeństwa zajmuje się specjalnie powołana połączona grupa koordynacyjna CEN-CENELEC Focus Group on Cybersecurity. Efektem jej działań w 2016 roku było uznanie **8 norm międzynarodowych ISO/IEC z obszaru informatyki śledczej jako norm europejskich (EN)**. Ponadto, w planie normalizacji na 2017 rok znajduje się przyjęcie kolejnych 3 norm międzynarodowych jako norm europejskich

Cyberbezpieczeństwo w zakresie energetyki

Energy Expert Cyber Security Platform (EECSP), grupa ekspercka Komisji Europejskiej, opracowała obszerny raport dotyczący cyberbezpieczeństwa w sektorze energetycznym. Celem raportu jest ocena regulacji w kontekście usług energetycznych oraz wskazanie działań, jakie powinny zostać podjęte dla podniesienia poziomu bezpieczeństwa.

EECSP zidentyfikowała **10 kluczowych obszarów** z zakresu cyberbezpieczeństwa w energetyce, w ramach których wskazała na istnienie **39 luk prawnych, które powinny zostać uzupełnione w celu zapewnienia odpowiedniego poziomu bezpieczeństwa**.

Luki dotyczą m.in. zagadnień zarządzania ryzykiem, metod reagowania na zagrożenia i naruszenia bezpieczeństwa oraz współpracy międzynarodowej (zob. Str. 59-63 raportu). Raport EECSP zawiera rekomendacje działań, których podjęcie doprowadzi do zniwelowania wskazanych luk (zob. Str. 64-69 raportu).

BusinessLawFirm

kochański zięba i partnerzy

Kontakt

e-mail: biuro@kochanski.pl
tel.: +48 22 326 9600
fax.: +48 22 326 9601
Metropolitan
Plac Piłsudskiego 1
00-078 Warszawa

www.kochanski.pl