

Ochrona danych osobowych oraz danych medycznych –zmiany w prawie oraz rola Administratora Bezpieczeństwa Informacji

Wrocław 2017-09-06



„GDPR”, zwane także „RODO” lub „Ogólnym Rozporządzeniem o Ochronie Danych” to Rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE1.



Od kiedy GDPR zacznie obowiązywać?

Rozporządzenie weszło w życie 17 maja 2016 r.

Zacznie ono obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r.

Należy pamiętać, że przepisy RODO weszły już w życie, ale stosować mamy je od 25 maja 2018 roku.



Okres (dokładnie 9 miesięcy) , który pozostało o rozpoczęcia ich stosowania to czas dla krajowego ustawodawcy, który powinien być wykorzystany na rewizję przepisów krajowych.

To czas dla administratorów danych i podmiotów przetwarzających dane do wykonywania nowych obowiązków.



**25 maja 2018 roku administratorzy danych muszą
wykazać się pełną zgodnością
z przepisami rozporządzenia ogólnego.**

**Dlatego tak ważne jest, żeby przygotowania do
stosowania przepisów rozpocząć już dziś.**



Przepisy RODO zastąpią ustawę o ochronie danych osobowych, a w raz z nią przestaną obowiązywać rozporządzenia wykonawcze wydane na jej podstawie.



**28 marca 2017 r. Ministerstwo Cyfryzacji opublikowało
Projekt ustawy o ochronie danych osobowych**

<https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych>

Przepisy nowej ustawy o ochronie danych osobowych, mają zapewnić skuteczne stosowanie w polskim porządku prawnym rozporządzenia ogólnego o ochronie danych.



Udostępnieniu przez Ministra Cyfryzacji podlega projekt części przepisów regulujących:

- zagadnienia ogólne (niektóre przepisy),
- zagadnienia związane z postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych,
- europejską współpracą administracyjną,
- zagadnienia związane z postępowaniem kontrolnym,
- zagadnienia związane z administracyjnymi karami pieniężnymi, odpowiedzialnością cywilną
- regulacje w zakresie inspektorów ochrony danych.



Czekamy na projekty ostateczny projekt ustawy krajowej oraz na projekt zmian w przepisach branżowych w tym w przepisach w zakresie ochrony zdrowia.

Tam gdzie przepis krajowy nie będzie wprowadzał odmiennych regulacji tam wprost stosowane są zapisy Rozporządzenia



Rozporządzenie zachowuje znany dotychczas model zaostrzenia rygoru przetwarzania danych wrażliwych (szczególnych kategorii danych).

Zasadą jest zakaz przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby lub danych dotyczących zdrowia lub seksualności i orientacji seksualnej, a także danych o wyrokach skazujących i o przestępstwach.



Rozporządzenie precyzuje czym są dane o stanie zdrowia

Zgodnie z art. 4 pkt 15 RODO „*dane dotyczące zdrowia*” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.



Możliwość przetwarzania danych wrażliwych w tym danych o stanie zdrowia dopuszczona jest, gdy spełniono co najmniej jeden wymienionych w Rozporządzeniu wyjątków.

W przypadku usługodawców w zakresie opieki zdrowia jest to przesłanka :
niezbędność przetwarzania do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub społecznej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub społecznej na podstawie prawa Unii lub prawa krajowego lub zgodnie z umową z pracownikiem służby zdrowia.



Dodatkowe obowiązki dla podmiotów przetwarzających dane osobowe.

Obowiązki informacyjne.

Privacy impact assesment - ocena skutków przetwarzania danych dla prywatności.

Wdrożenie programu zgodności przetwarzania danych.

Ochrona prywatności by design i by default.



Uprawnienia osób fizycznych.

Rozporządzenie reguluje też kwestię uprawnień osób fizycznych do ochrony ich danych, w szczególności w następujących obszarach:

- a. Prawo do przeniesienia danych.
- b. Prawo sprzeciwu.
- c. Prawo do bycia zapomnianym.
- d. Wnoszenie skarg.
- e. Prawo do odszkodowania.



Zwiększone uprawnienia organów i kary.



Obowiązki związane z zabezpieczeniem danych osobowych?



Wiele obowiązków, przewidzianych dla administratorów na gruncie ustawy o ochronie danych osobowych, pozostanie w swej istocie niezmiennymi również po 25 maja 2018 r. (np. obowiązek informacyjny wobec podmiotów danych).

Co istotne, przepisy RODO przewidują dla administratorów danych również nowe zadania, zaś kilka obowiązków (w tym te szczególnie uciążliwe dla administratorów) przejdzie do historii.



Stosownie do przepisów RODO, administrator zobowiązany jest do zapewnienia odpowiedniego stopnia bezpieczeństwa przetwarzanych danych osobowych. Przepisy RODO nie zawierają przy tym precyzyjnych wskazówek, jakie to konkretnie środki mając być w tym celu stosowane.

Ich wybór w całości pozostawiony został administratorowi.

Dokonując wyboru środków technicznych i organizacyjnych administrator powinien wcześniej ocenić czy gwarantowany przez te środki stopień bezpieczeństwa będzie adekwatny do ryzyka wiążącego się z przetwarzaniem danych osobowych. Dla zabezpieczenia danych w sposób zgodny z przepisami RODO, kluczowe znaczenie będzie miało rzetelne ocenienie ryzyka związanego z przetwarzaniem danych. Ocena ta, a w konsekwencji również dobranie adekwatnych środków bezpieczeństwa powinny być dokonywane przy uwzględnieniu wymienionych w RODO czynników.



Co należy uwzględnić wdrażając środki zabezpieczające dane osobowe:

- aktualny stan wiedzy technicznej
- koszt wdrażania środka
- charakter, zakres, kontekst i cele przetwarzania danych osobowych
- ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia
- ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych



PRZYKŁADOWE ŚRODKI BEZPIECZEŃSTWA WEDŁUG RODO:

pseudonimizacja i szyfrowanie danych osobowych

środki zdolne do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania

środki zdolne do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania



Istotną nowością jest również rezygnacja z wymogu prowadzenia wykazu zbiorów danych jako elementu polityki bezpieczeństwa oraz obowiązku zgłaszania zbiorów danych do rejestracji GIODO.

Na gruncie RODO zostały one zastąpione obowiązkiem rejestrowania czynności przetwarzania danych.



W rejestrze czynności przetwarzania muszą znaleźć się m.in. następujące informacje:

INFORMACJE ZAMIESZCZANE W REJESTRZE CZYNNOSCI PRZETWARZANIA:

- Imię i nazwisko lub nazwę oraz dane kontaktowe administratora (oraz współadministratorów, przedstawiciela administratora oraz inspektora ochrony danych).
- Cele przetwarzania danych.
- Opis kategorii osób, których dane dotyczą, oraz kategorii danych ich dotyczących.
- Kategorie odbiorców, którym dane zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych.



INFORMACJE ZAMIESZCZANE W REJESTRZE CZYNNOSCI PRZETWARZANIA:

- Gdy ma to zastosowanie, informacje o transferach danych osobowych do państw trzecich lub organizacji międzynarodowej, ze wskazaniem tych państw lub organizacji (wraz z udokumentowaniem odpowiednich środków bezpieczeństwa).
- Planowane terminy usunięcia poszczególnych kategorii danych – jeżeli jest to możliwe.
- Ogólny opis stosowanych technicznych i organizacyjnych środków bezpieczeństwa zapewniających bezpieczeństwo danych osobowych – jeżeli jest to możliwe.
- Forma prowadzenia rejestru czynności przetwarzania:
Pisemna, w tym elektroniczna.



INFORMACJE ZAMIESZCZANE W REJESTRZE CZYNNOSCI PRZETWARZANIA:

- Kto jeszcze jest zobowiązanych do prowadzenia rejestru:
Przedstawiciel administratora Podmiot przetwarzający (procesor)
- Podmioty wyłączone z obowiązku: Przedsiębiorca lub podmiot zatrudniający mniej niż 250 osób.
- Wyłączenie to nie dotyczy jednak trzech przypadków:
 - ☐ gdy dokonywane przez te podmioty przetwarzanie danych może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą;
 - ☐ przetwarzanie danych nie ma charakteru sporadycznego;
 - ☐ przetwarzanie dotyczy szczególnych kategorii danych (danych wrażliwych) lub danych dotyczących wyroków skazujących za przestępstwa i naruszeń prawa.



Kto będzie mógł pełnić funkcję inspektora ochrony danych i jakie będzie miał zadania?



Od 25 maja 2018 roku trzy kategorie administratorów oraz podmiotów przetwarzających w imieniu administratora będą musiały powoływać inspektorów ochrony danych. Powołanie inspektora będzie obligatoryjne dla:

1. Organów i podmiotów publicznych z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2. Podmiotów, których główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę;
3. Administratorzy, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych dotyczących wyroków skazujących i naruszeń prawa.



Inspektor ochronnych danych osobowych wyznaczany jest zgodnie z RODO na podstawie kwalifikacji zawodowych i wiedzy, nie tylko na temat prawa, ale i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania powierzonych mu zadań. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego, ale może też wykonywać swoje zadania na podstawie umowy o świadczenie usług.



Artykuł 38 rozporządzenia ogólnego wskazuje, jaki jest status inspektora ochrony danych.

Inspektor nie może otrzymywać instrukcji dotyczących wykonywanych przez niego zadań.

Nie może być też odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor musi też podlegać bezpośrednio najwyższemu kierownictwu.

Warto zwrócić uwagę na fakt, że przepisy rozporządzenia wymagają też tego, by administrator oraz podmiot przetwarzający wspierali inspektora ochrony danych w wypełnianiu przez niego zadań.

To wsparcie oznaczać ma zapewnienie zasobów niezbędnych do wykonania zadań inspektora, dostęp do danych i operacji przetwarzania oraz, co bardzo ważne, zasoby niezbędne do utrzymania wiedzy fachowej inspektora.



Zgodnie z RODO, zadania inspektora ochrony danych obejmują:

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia ogólnego oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie
2. Monitorowanie przestrzegania RODO oraz innych przepisów 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
3. Udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania tej oceny
4. Współpraca z organem nadzorczym
5. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami.



Jak krajowe prawo postrzega nowych Inspektorów a starych ABI?

W ocenie projektodawcy najwłaściwszym rozwiązaniem, jest przesądzenie wprost, że osoby wykonujące w dniu 24 maja 2018 r. funkcję administratora bezpieczeństwa informacji, pełnią funkcję inspektora ochrony danych do dnia 1 września 2018 r.

Do tego czasu, każdy z inspektorów ochrony danych ma czas na podjęcie decyzji o dalszym pełnieniu takiej funkcji (i dokonaniu stosowanego zawiadomienia do Prezesa Urzędu).

W razie braku do tego czasu jakiegokolwiek aktywności z ich strony, w dniu 1 września 2018 r. z mocy prawa przestaną pełnić funkcję inspektorów ochrony danych.



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 1. Rozpoznaj obecną sytuację

Zanim skupisz się na konkretnych wymogach Rozporządzenia, dobrze będzie rzucić okiem na obecnie funkcjonujące w Twojej firmie zasady ochrony prywatności i [danych osobowych](#).

Przeprowadź analizę dokonanych sprawdzeń, posiadanej dokumentacji.

Zdobywaj wiedzę w zakresie nowych regulacji, interpretacji przepisów. Śledź pojawiające się poradniki w zakresie realizacji RODO.



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 2. Przyjrzyj się również samym danym, które twoja jednostka przetwarza

Zadaj sobie cztery proste pytania:

- 1.Czy dane, które przetwarzam są nadal potrzebne?
- 2.Czy nie archiwizujecie danych dłużej niż jest to wymagane?
- 3.Czy dysponujecie zgodami udzielonymi przez Klientów?
- 4.Czy przechowujecie dane w sposób bezpieczny?

Jeśli nie potrzebujesz już jakichś danych – nie zatrzymuj ich! Tutaj mniej oznacza więcej. Warto też zidentyfikować osobę lub osoby w Twojej organizacji, które będą odpowiadać za zgodność w zakresie ochrony danych.



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 3. Uzupełnij lub przygotuj dokumentację/procedury

Na obecnym etapie warto skupić się na uzupełnieniu i przygotowanie dokumentacji.

Wdrożenie ISO 27001 zapewnia 70% zgodności z RODO



Zadania dla Administratorów danych / Inspektorów Ochrony Danych w zakresie wdrożenia RODO

Krok 4. Privacy by Design, czyli bezpieczeństwo uwzględnione w fazie projektowania

Jeśli już teraz uwzględniysz kwestie prywatności w planowanych działaniach i projektach, to w 2018 roku będziesz w stanie zapewnić, że są one zgodne z europejskimi standardami RODO.

Planując działania weź pod uwagę:
konieczność przechowywania danych, środki zabezpieczające [dane osobowe](#),
anonimizacje danych, itp.



PODEJŚCIE OPARTE NA RYZYKU

Etapy procesu doboru zabezpieczeń :

1. Określenie i opisanie procesów przetwarzania danych w tym charakter, zakres, cel i kontekst przetwarzania.
W tym miejscu dokonujemy oceny, czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla danych osobowych a także czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
2. Określenie praw i wolności jakie zostały przyznane osobom, których dane dotyczą;
3. Zidentyfikowanie zagrożeń naruszenia praw i wolności tych osób związanych z planowanym lub już realizowanym przetwarzaniem danych osobowych;



PODEJŚCIE OPARTE NA RYZYKU

Etapy procesu doboru zabezpieczeń :

4. Dokonanie oceny ryzyka naruszenia praw i wolności (czyli określenie prawdopodobieństwa i skutków wystąpienia zidentyfikowanych zagrożeń);
5. Dobór środków technicznych i organizacyjnych do zidentyfikowanych zagrożeń w zależności od poziomu ryzyka, a także w zależności od stanu wiedzy technicznej i kosztów wdrożenia tych środków;
6. Dokonanie oceny, czy ryzyko jest akceptowalne.
Biorąc pod uwagę zagrożenia stopień ryzyka oraz dobrane środki zabezpieczające oceniamy czy ryzyko naruszenia praw i wolności osób fizycznych jest akceptowalne, tzn. czy operacje przetwarzania danych są zgodne z wymaganiami RODO oraz czy identyfikuje się wysokie ryzyko naruszenia praw i wolności osób fizycznych



PODEJŚCIE OPARTE NA RYZYKU

7. Dokonanie oceny skutków dla ochrony danych w przypadku stwierdzenia zaistnienia ryzyka naruszenia praw i wolności oraz w innych przypadkach np. kiedy organ wskaże taką konieczność;
8. Przeprowadzenie uprzedniej konsultacji z organem nadzorczym (art. 36 RODO) – przedstawienie dokumentacji oceny skutków dla ochrony danych osobowych.

WAŻNE

Ostatnie dwa etapy będą występowały tylko wówczas, gdy przetwarzanie danych osobowych wiązałoby się z wysokim ryzykiem naruszenia praw i wolności podmiotu danych albo gdy organ krajowy ustanowił by taką konieczność.





Analiza ryzyka

Analiza ryzyka jest jednym z elementów procesu zarządzania ryzykiem. Wykonuje się ją podczas projektowania systemu/sieci TI, cyklicznie w trakcie eksploatacji oraz w przypadku zaistnienia incydentu naruszenia bezpieczeństwa TI. W oparciu o wyniki analizy ryzyka dobiera się zabezpieczenia. Zastosowane zabezpieczenia powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, wymagania biznesowe i wymagania z analizy ryzyka zasobów posiadających wartość dla działania instytucji. Ryzyko jakie powstaje po wprowadzeniu zabezpieczeń nazywamy ryzykiem szczątkowym.

Aby poprawnie przeprowadzić analizę ryzyka potrzebujemy określonej wiedzy. Musi być nam znana polityka bezpieczeństwa wdrożona w danej jednostce organizacyjnej (np. kontrola dostępu do pomieszczeń lub monitoring), musimy wiedzieć co chronimy i przed kim/czym, a także konieczna jest wiedza na temat środków jakimi dysponujemy (ludzie, pieniądze, czas).

Analiza ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak aby to ryzyko zminimalizować lub całkowicie go zlikwidować.



Analiza ryzyka

Aby przeprowadzić poprawnie analizę ryzyka na początku należy określić:

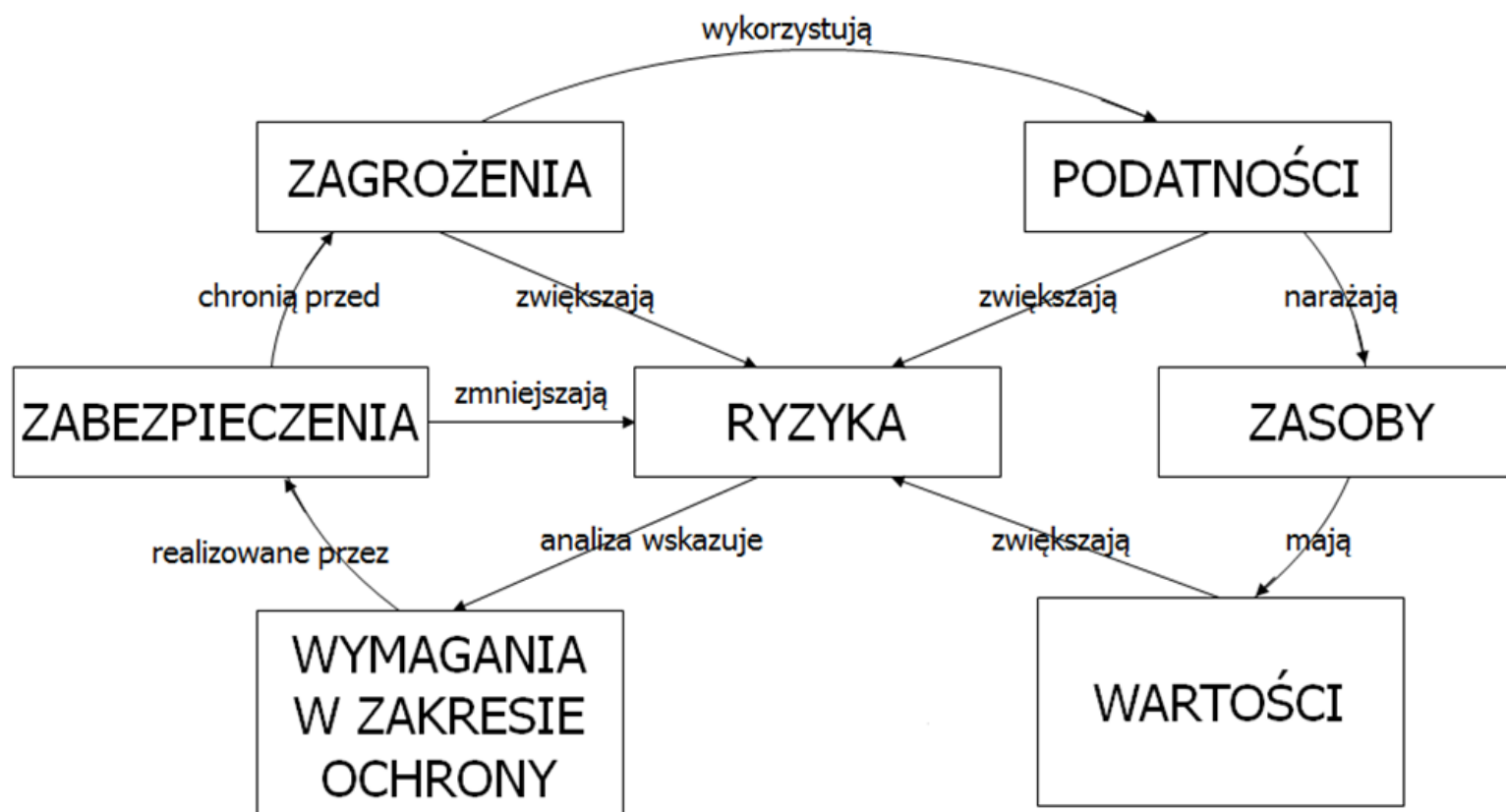
- zasoby, które będziemy chronić;
- zagrożenia – czynnik, który może powodować wystąpienie incydentu;
- podatność – słabość zasobów, która może być wykorzystana przez zagrożenie;
- skutki – jaki wpływ będzie miał zaistniały incydent na system/sieci TI.

Uzbrojeni w taką wiedzę możemy zacząć szacować ryzyko, które w dalszej fazie pozwoli wysunąć nam wnioski do dokumentacji bezpieczeństwa systemu.

Zasobami systemu są wszystkie elementy służące do przetwarzania, przechowywania, lub przekazywania informacji oraz do zapewnienia im właściwego poziomu bezpieczeństwa.

Analiza ryzyka

Postępowanie z ryzykiem



Materiały z którymi warto się zapoznać:

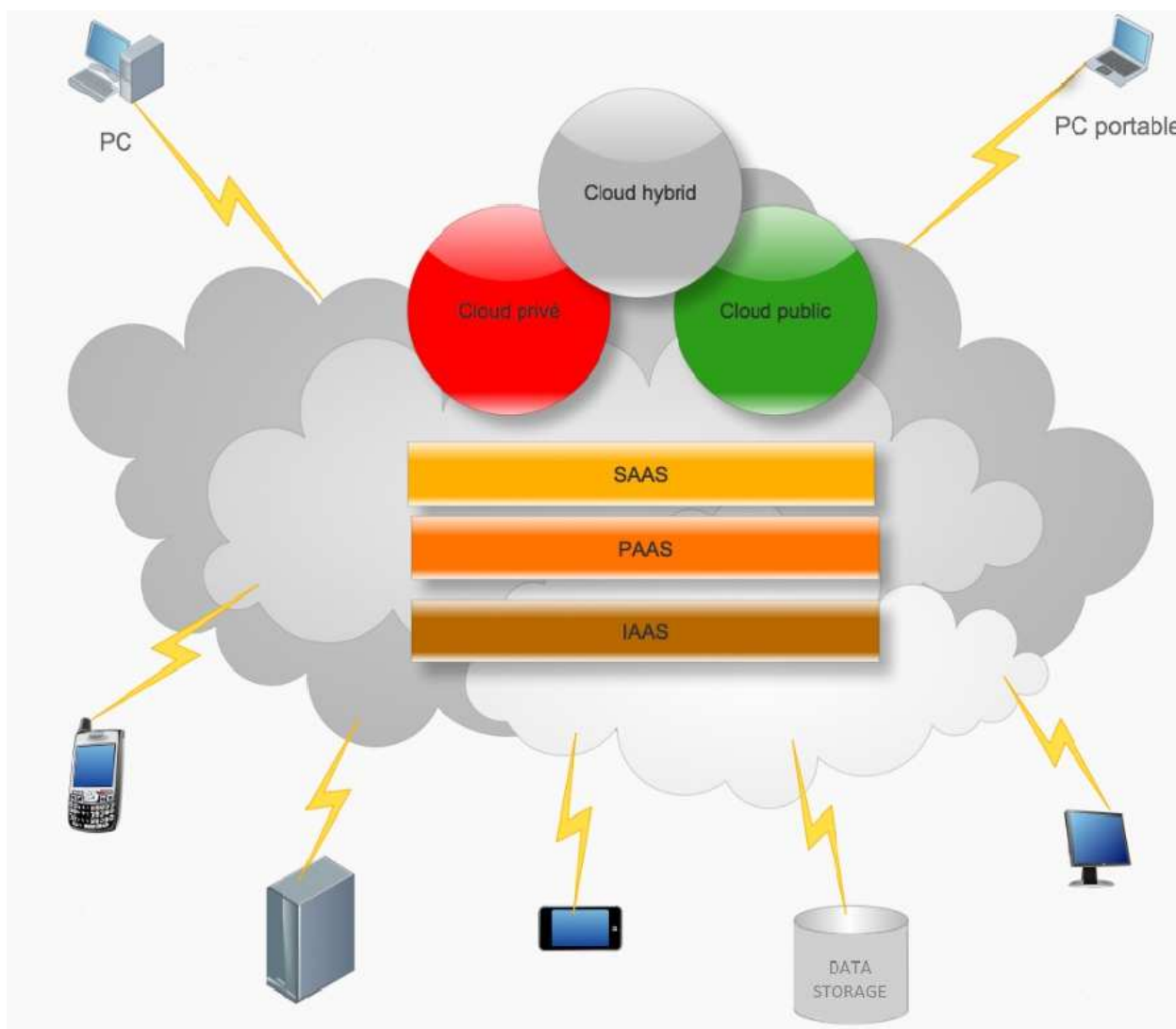
[Wytyczne GIODO Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych](#)

[Wytyczne Grupy Roboczej art. 29 dotyczące inspektorów ochrony danych \(WP 243\)](#)

Baza wiedzy portalu GDPR.pl



Przetwarzanie informacji w chmurze





Przetwarzanie informacji w chmurze

Rozróżniamy trzy podstawowe rodzaje chmur:

- prywatne (ang. private cloud) – rodzaj chmur stanowiących część organizacji, uruchamiane i zarządzane w środowisku organizacji,
- publiczne (ang. public cloud) – rodzaj chmur, które są dostarczane przez zewnętrznego dostawcę,
- hybrydowe (ang. hybrid) – połączenie chmury prywatnej i publicznej, gdzie część pracuje w środowisku organizacji a część w środowisku publicznym.



Przetwarzanie informacji w chmurze

Modele chmury obliczeniowej

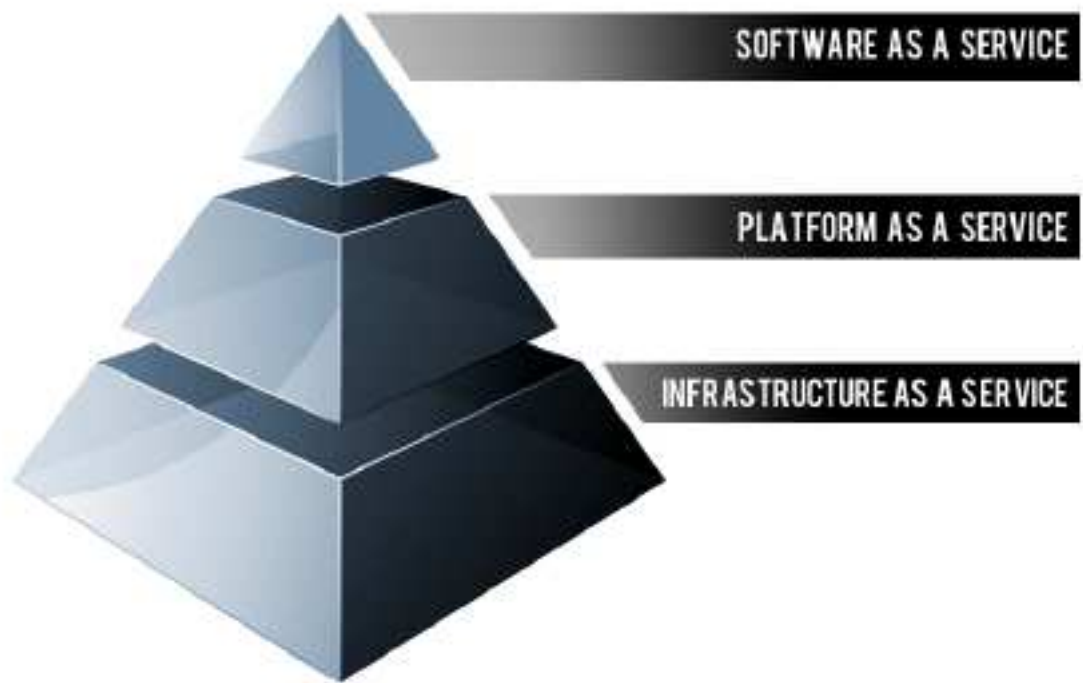
Najczęściej spotykanymi modeli chmury obliczeniowej są:

- Software as a Service (SaaS) – organizacja korzysta z aplikacji umieszczonych w chmurze. Kontrola podstawowej infrastruktury, w tym również zasobów sieciowych, serwerów, systemów i składowania danych znajduje się w kompetencjach i odpowiedzialności dostawcy.
- Platform as a Service (PaaS) – cechą charakterystyczną jest umożliwienie instalacji własnych aplikacji i systemów w infrastrukturze dostawcy.
- Infrastructure as a Service (IaaS) – cechą charakterystyczną jest dostarczanie podstawowych zasobów obliczeniowych, sieciowych, przechowywania danych i innych. W tym modelu istnieje możliwość instalowania i uruchamiania dowolnego oprogramowania.



Przetwarzanie informacji w chmurze

Odpowiedzialność





Przetwarzanie informacji w chmurze

Odpowiedzialność

Tak ułożone modele tworzą stos nazywany w skrócie SPI (S>P>I), w którym im niżej stosu dostawca dostarcza usługę tym organizacja jest w większym stopniu odpowiedzialna za zarządzanie ryzykiem i zabezpieczeniem środowiska.

Można również umownie przyjąć, że odpowiedzialność dostawcy i organizacji w modelu IaaS kształtuje się w stosunku 50/50, w modelu PaaS odpowiedzialność dostawcy wzrasta aby w modelu SaaS osiągnąć najwyższy poziom, pozostawiając po stronie organizacji odpowiedzialność tylko za interfejs użytkownika.

Przetwarzanie Informacji Bezpieczeństwo



Poufność odnosi się do stosowania rozwiązań kryptograficznych.

Warto pamiętać że w modelu IaaS, klient usługi w chmurze nie może polegać na rozwiązaniu szyfrowania oferowanym przez dostawcę usługi w chmurze, ale może zdecydować się na szyfrowanie danych osobowych przed wysłaniem ich do chmury.

Również w zakresie komunikacji pomiędzy dostawcą usługi a klientem wymagane jest stosowanie autoryzacji i uwierzytelniania, natomiast pomiędzy ośrodkami wymiany danych komunikacja powinna być zaszyfrowana.

Przetwarzanie informacji

Bezpieczeństwo



Integralność jest właściwością polegającą na zapewnieniu dokładności i kompletności aktywów co odnosząc wprost do danych oznacza, że są one prawdziwe i nie zostały złośliwie lub przypadkowo zmienione podczas przetwarzania, przechowywania lub przekazywania.

Naruszenia integralności danych przetwarzanych w chmurze można wykryć lub im zapobiec przy pomocy systemów służących wykrywaniu/zapobieganiu włamaniom (IPS/IDS) jako funkcji często występujących w urządzeniach klasy UTM.

Przetwarzanie informacji

Bezpieczeństwo



Dostępność tzn. właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

Zagrożeniem dla dostępności usług uruchomionych w środowisku chmurowym jest chociażby atak z wykorzystaniem DoS (odmowa usługi), dlatego administratorzy danych w celu zapewnienia ciągłości działania powinni zapewnić sobie prawo do kontroli w zakresie zastosowanych środków bezpieczeństwa w tym m.in.: łączy zapasowych, nadmiarowych zasobów oraz skutecznych mechanizmów wykonywania kopii zapasowych.

Przetwarzanie informacji

Bezpieczeństwo



Najważniejszym w kontekście zapewnienia bezpieczeństwa przetwarzanym informacjom jest wskazanie procesów, w których dane są przetwarzane, funkcje jakie pełnią w organizacji, danych oraz aplikacji służących do ich przetwarzania.

Przetwarzanie informacji

Model bezpieczeństwa



- Identyfikacja wymagań zewnętrznych i wewnętrznych,
- Określenie zakresu funkcjonowania,
- Opracowanie strategii,
- Wdrożenie Polityki Bezpieczeństwa,
- Monitorowanie i doskonalenie.

Przetwarzanie informacji

Etapy budowania bezpieczeństwa



- Wskazanie ról i odpowiedzialności za zarządzanie bezpieczeństwem,
- Określenie wymagań i kompetencji,
- Identyfikacja aktywów,
- Ustanowienie procesu oceny pod kątem integralności, dostępności i integralności przetwarzanych danych – analiza ryzyka,
- Analiza i ocena ryzyka,
- Postępowanie z ryzykiem

Przetwarzanie informacji

Etapy budowania bezpieczeństwa



- Ustanowienie Polityki Bezpieczeństwa Informacji
- Zapewnienie ochrony przetwarzanej informacji
- Monitorowanie i doskonalenie
- Podejmowanie działań korygujących.

Przetwarzanie informacji

Wytyczne, zasady i rekomendacje budowania bezpieczeństwa



☐ **Bezpieczeństwo fizyczne i środowiskowe**

- Obszary bezpieczne
- Bezpieczeństwo sprzętu
- Lokalizacja sprzętu
- Systemy wspomagające
- Bezpieczeństwo okablowania
- Konserwacja sprzętu
- Obsługa nośników
- Bezpieczeństwo sprzętu poza siedzibą
- Bezpieczna likwidacja sprzętu
- Wynoszenie sprzętu poza siedzibę organizacji

☐ **Bezpieczeństwo sieciowe**

Przetwarzanie informacji

Wytyczne, zasady i rekomendacje budowania bezpieczeństwa



☐ **Bezpieczeństwo systemów**

- Ochrona antywirusowa
- Usługi dostarczane przez strony trzecie
- Planowanie i odbiór systemów
- Zarządzanie zmianą
- Szyfrowanie danych medycznych

☐ **Kontrola dostępu**

- Zarządzanie tożsamością (uwierzytelnianie)
- Zarządzanie dostępem użytkowników
- Odpowiedzialność użytkowników
- Kontrola dostępu do aplikacji
- Kontrola dostępu do sieci
- Praca na odległość, wykorzystywanie urządzeń przenośnych

Przetwarzanie informacji

Wytyczne, zasady i rekomendacje budowania bezpieczeństwa



- ☐ Stosowanie metod kryptograficznych
- ☐ Audytowalność i niezaprzeczalność danych i zdarzeń w systemie
- ☐ Archiwizacja danych medycznych
- ☐ Zarządzanie incydentami związanymi z bezpieczeństwem informacji
- ☐ Zarządzanie ciągłością działania
 - Tworzenie i odtwarzanie kopii zapasowych
 - Dostępność i niezawodność (SLA)
 - Postępowanie na wypadek awarii/katastrofy i utraty danych
 - Plany BCP i DRP



INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

Postępowanie z incydentami bezpieczeństwa informacji stanowi bardzo ważny element programu zarządzania bezpieczeństwem informacji.

Wraz z procesami zarządzania ryzykiem (ang. *risk management*), zarządzania zdarzeniami bezpieczeństwa (ang. *security event management*), zarządzania podatnościami (ang. *vulnerability management*) i testami bezpieczeństwa, ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa aktywów informacyjnych na działalność przedsiębiorstwa, w tym na ciągłość operacyjną jego procesów biznesowych, systemów i infrastruktury teleinformatycznej.



INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

Incydentem bezpieczeństwa informacji jest zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych.

W szczególności incydentami bezpieczeństwa informacji są:

- przypadki naruszenia poufności (ujawnienie niepowołanym osobom), integralności (uszkodzenie, przekłamanie, zniszczenie) i dostępności (dane nie są dostępne w użytecznej postaci na żądanie uprawnionych użytkowników) danych, niezależnie od ich nośnika, w tym także przechowywanych i przetwarzanych w systemach informatycznych oraz transmitowanych przez łącza sieci;

INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

- niedostępność oraz działania niezgodne ze specyfikacją (błędne) systemów informatycznych, zwłaszcza systemów i aplikacji krytycznych (z wyłączeniem kontrolowanych i zaplanowanych prac oraz dysfunkcji niemających wpływu na bezpieczeństwo informacji;
- infekcje, propagacja i działanie szkodliwego oprogramowania (malware – kody i skrypty mające szkodliwe, przestępcze lub złośliwe działanie, do których zaliczają się między innymi wirus, robak internetowy, koń trojański, spyware, keylogger, rootkit, dialer, exploit etc.);
- rozpoznanie, penetracja i próby omijania systemów zabezpieczeń;
- niewłaściwe wykorzystywanie lub nadużywanie zasobów informacyjnych;



INCYDENTY W BEZPIECZEŃSTWIE INFORMACJI

- ataki nieautoryzowanego dostępu do aplikacji, systemów oraz ataki eskalacji poziomu uprawnień w systemach;
- kradzież lub zniszczenie urządzeń przetwarzających lub/i przechowujących informacje oraz nośników danych;
- wyłudzenia (lub próby wyłudzeń) informacji wrażliwych, takich jak np. hasła dostępowe czy tajemnice przedsiębiorstwa;
- ataki socjotechniczne, ataki z wykorzystaniem phishing'u, skimming'u oraz innych technik zagrażających naruszeniu poufności, dostępności i integralności informacji;
- incydenty wielokomponentowe (złożone incydenty dotyczące wielu systemów, wykorzystujące wiele wektorów ataków itp.);

Przetwarzanie informacji

Cyberbezpieczeństwo, Infrastruktura krytyczna i ciągłość działania



Dyrektywa NIS (Dyrektywa Parlamentu i Rady UE 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii przyjęta została 6 lipca 2016 roku.) zakłada poszerzenie współpracy państw członkowskich w kwestii cyberbezpieczeństwa.

Jednym z sektorów objętych dyrektywą jest sektor e-zdrowia zawierający zagadnienia dotyczące przetwarzania dokumentacji medycznej w postaci elektronicznej. Dyrektywy PE i Rady (UE) 2016 /1148 z dn. 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów teleinformatycznych

Przetwarzanie informacji

Cyberbezpieczeństwo, Infrastruktura krytyczna i ciągłość działania

Zgodnie z Dyrektywą NIS konieczne jest zapewnienie przez poszczególne podmioty mające udział w przetwarzaniu informacji minimalnego poziomu ochrony dla infrastruktury w tym sieci i systemów przetwarzających dokumentację medyczną. Poprzez realizację tego wymogu rozumieć należy wdrożenie odpowiednich środków bezpieczeństwa w warstwie organizacyjnej, technicznej i systemowej oraz w przypadku wystąpienia poważnych incydentów bezpieczeństwa informacji podjęcie odpowiednich działań ograniczających ich skutki, a co najważniejsze powiadomienie krajowego organu cyberbezpieczeństwa jakim jest CERT Polska. Krajowy organ będzie mógł nakładać sankcje na podmioty, które nie dostosują się do Dyrektywy NIS i nie wdrożą zabezpieczeń zapewniających spełnienie minimalnego poziomu bezpieczeństwa sieci i systemów.



Przetwarzanie informacji

Cyberbezpieczeństwo, Infrastruktura krytyczna i ciągłość działania

Dyrektywa NIS nakłada na kraje członkowskie obowiązek zachowania ciągłości funkcjonowania infrastruktury krytycznej, a co za tym idzie nakłada na podmioty odpowiedzialność za ciągłość działania i świadczenie tzw. usług krytycznych.

W sektorze e-zdrowia są to usługi związane z zapewnieniem:

- ciągłości działania systemów informacji zdrowotnej przetwarzającej elektroniczną dokumentację medyczną,
- dostępnością repozytoria danych czyli bazy danych w jednostkach, w którym informacja jest przechowywana lokalnie,
- dostępnością dla użytkowników systemów informatycznych realizowaną między innymi poprzez ciągłość pracy serwerów odpowiedzialnych uwierzytelnianie tj. przeprowadzenie kontroli dostępu i uwierzytelniania użytkowników,
- ciągłości działania informatycznych systemów laboratoryjnych - Laboratory Information System (LIS)
- ciągłości działania informatycznych systemów radiologicznych - Radiology Information Systems (RIS)
- dostępności elektronicznej dokumentacji medycznej zawartych w elektronicznych kartach zdrowia,
- kluczowych usług niezbędnych do świadczenia opieki zdrowotnej.



Dziękuję za uwagę.

e-mail: wspolpraca-regiony@csioz.gov.pl



Centrum Systemów Informacyjnych
Ochrony Zdrowia