

XXIII MIĘDZYNARODOWY KONGRES OTWARTEGO SYSTEMU OCHRONY ZDROWIA OSOZ

REFERAT:

Wdrożenie RODO w praktyce z wykorzystaniem KS-BDO@2018



Wczesne ostrzeganie
Kompensacja zakłóceń
Promocja zdrowia
Relacje w rodzinie
Samoleczenie zapobiegawcze
Leczenie zapobiegawcze
Odporność naturalna
Samoleczenie naprawcze
Leczenie naprawcze



PL

Prelegent : Krzysztof Struk (BDO@KAMSOFT.PL)

Stanowisko: Analityk

OSOZ - OTWARTY SYSTEM OCHRONY ZDROWIA

Nowe wyzwania

Największa zmiana prawna (w historii) w obszarze ochrony i przetwarzania danych osobowych, wrażliwych

Przeniesienie odpowiedzialności na Organizację („podmiot przetwarzający”) -
wysokie kary finansowe (nawet do 4% rocznego obrotu)

Wymóg właściwego przygotowania i ciągłej pracy Organizacji
nad doborem środków i narzędzi do zabezpieczenia danych oraz
monitoringu ich przetwarzania

Szacowanie ryzyk, prowadzenie rejestru Czynności Przetwarzania

Obowiązki informacyjne i respektowanie prawa wolności osób

Zgody elektroniczne

Rosnąca skala cyberataków i szybka reakcja



Jak nad tym zapanować praktycznie ?

Otoczenie prawne – najistotniejsze zmiany

Brak zgłaszania zbioru do UODO (stara nazwa GIODO)

Prowadzenie szacowania ryzyk i oceny skutków

Umożliwienie egzekwowanie praw przez Osobę jak:
poprawa danych, pobranie elektronicznej kopii danych,
zgłoszenie wniosku o bycie zapomnianym

Przetwarzanie danych wyłącznie w minimalnym zakresie i okresie
oraz zgodnie z celem przetwarzania

Niezwłoczne informowanie stron (Organy, Osoby) o naruszeniu
integralności ochrony danych

Nie tylko kary nakładane przez Organ ale też odszkodowania dla Osób

Ograniczenie (a w zasadzie wyłączenie) przekazywania danych
do państw trzecich (z poza UE)

RODO jako obowiązek codzienny a nie okazjonalny



Czy wiem wszystko ?

Pierwsze kroki

1. Wybór osoby w Organizacji i właściwego Partnera
2. Kontakt z Producentem mojej Aplikacji
3. Inwentaryzacja stanu bieżącego (stan prawny, fizyczny)
4. Sprawdzenie aktualnego zawartości Polityki Bezpieczeństwa (oraz procedur)
5. Weryfikacja zgodności z prawem
6. Weryfikacja stosowanych zabezpieczeń
7. **Dokumentowanie wykonanych kroków**



Od czego zacząć ?

Cykliczne zadania związane z zarządzaniem ochroną danych

- Wykonywanie analizy kontekstu działania Organizacji
- Zbieranie zasad i celów przetwarzania danych (także planowanych)
- Przeprowadzanie analizy ryzyka
- Ocena skutków
- Aktualizacja Polityki Bezpieczeństwa oraz procedur
- Wdrażanie w Organizacji
- Edukacja Personelu
- Efektywny monitoring działania Organizacji i Produktów**



Czy podołam ?

KS-BDO a RODO

KS-BDO dedykowany dla obszaru wsparcia zarządzania ochroną danych osobowych

Zmiana dostępności KS-BDO

Pełne dostosowanie do nowych zadań wynikających z RODO

Szeroki wsad prawno-biznesowy a wynikający z możliwości wykorzystywania Produktów KAMSOF

Ocena działania procesowa (zgodnie z obowiązującymi wytycznymi)

Rozwój KS-BDO w trybie bieżącym (wraz z zmianą świata zewnętrznego)

Wsparcie Organizacji i Administratora w realizacji czynności

Zintegrowany z Produktami KAMSOF

Dowolne uzupełnienia o własną specyfikę działania



Jak nad tym zapanować praktycznie ?

Zebranie stanu bieżącego – kontekst Organizacji

Zestaw ukierunkowanych pytań ankietowych w celu systematycznego zbudowania wiedzy o aktualnej rzeczywistości w Organizacji (AsIs) oraz planach (ToBe)

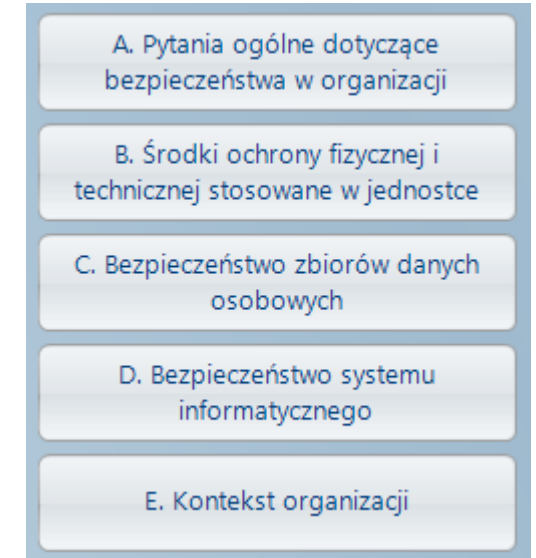
Kategoria A – pytania ogólne (informacyjne, prawne, ogólne)

Kategoria B – ochrona fizyczna danych (lokalizacje, zabezpieczenia)

Kategoria C – zabezpieczenia zbiorów danych osobowych

Kategoria D – zabezpieczenia systemów informatycznych (sprzęt, kopie zapasowe)

Kategoria E – weryfikacja ogólna organizacji



*Czy mam wiedzę o wszystkim
co muszę zrobić ?*

Wyodrębnienie zasady i cele przetwarzania danych

KS

Bezpieczeństw... Ankieta

Dokumentacja Zasady przetwarzania danych Współpraca z KS-AOV

Zamknij Zapisanie odpowiedzi Przenieś odpowiedzi Wczytaj plik przeniesienia Wyświetlaj podpowiedzi

Wybór procesu przetwarzania
Realizacja recepty papierowej i innych

Sekcja A Sekcja B

Postęp wypełniania ankiety

A. Podstawy przetwarzania danych

B. Obowiązki Administratora Danych Osobowych

i Należy wskazać podstawy prawne przetwarzania danych osobowych np. zgoda, umowa, obowiązek prawny. Jeśli to możliwe można wskazać dokładną przesłankę prawną uzasadniającą przetwarzanie danych. RODO Art.9, Art. 6

A1 Jakie podstawy prawne przetwarzania danych w tym procesie?

- ☐ Art.9 ust.1 lit. D (Fundacja, Stowarzyszenie);
- ☐ Art.9 ust.1 lit. E (Dane upublicznione).
- ☐ Art.9 ust.1 lit. F (Sądy, Dochodzenie lub obrona roszczeń).
- ☐ Art.9 ust.1 lit. G (Zadanie realizowane w interesie publicznym).
- ☐ Art.9 ust.1 lit. H (Profilaktyka zdrowotna, medycyna).
- ☐ Art.9 ust.1 lit. I (Zadanie realizowane w interesie publicznym w dziedzinie zdrowia publicznego).
- ☐ Art.9 ust.1 lit. J (Archiwum, Badania naukowe, Statystyki).

Dane osobowe

- ☒ Art.6 ust.1 lit. A (Zgoda);

Podstawy prawne, Administrator i miejsce przetwarzania danych, cele, odbiorcy, kategorie danych, okres przechowywania danych, stosowane zabezpieczenia, zgody, stosowanie prawa co do wolności osób, ...

Analiza ryzyka

A. Nieuprawniony dostęp do danych

B. Nieuprawnione ujawnienie

C. Zniszczenie/Utrata

D. Nieuprawniona modyfikacja

E. Inne zagrożenia



Należy wskazać zagrożone aktywa w ramach analizowanego procesu i zagrożenia nieuprawnionym dostępem, z uwzględnieniem aktyw wspomagających związanych z przetwarzaniem danych takich jak sprzęt, oprogramowanie, lokalizacja.

A2 Jakie aktywa mogą być zagrożone nieuprawnionym dostępem do danych w ramach tego procesu?

Lp.	Nazwa	Wybór
1	Dokument papierowy będący podstawą wydania leków (dane wrażliwe)	☐
2	Dokumenty papierowe kadrowe - księgowe zawierające dane osobowe dotyczące pracowników	☒
3	Dokumenty papierowe księgowe zawierające d.o. dotyczące kontrahentów/pacjentów (faktury wystawiane przez aptekę)	☒
4	Dokument elektroniczny będący podstawą wydania leków (dane wrażliwe)	☐
5	Dokumenty elektroniczne kadrowe - księgowe zawierające dane osobowe dotyczące pracowników	☐
6	Dokumenty elektroniczne księgowe zawierające d.o. dotyczące kontrahentów/pacjentów (faktury wystawiane przez aptekę)	☒
7	Kopia zapasowa	☒
8	Podstawowy system obsługi apteki	☐
9	Systemy kadrowo-płacowe	☐
10	System księgowy	☐
11	Inne systemy przetwarzające dane osobowe	☐
12	Apteka internetowa	☐



Zaznacz wszystko

Szukaj wg

Wartość

Szukaj

(wybierz)



+

Inwentaryzacja stanu oraz ocena ryzyka dla każdego procesu, w którym następuje przetwarzanie danych, w podziale na istotne kategorie określone w RODO

Poziom istotności zagrożenia, prawdopodobieństwa wystąpienia, decyzja

ISTOTNOŚĆ

D				
C				
B				
A				

1

2

3

4

PRAWDOPODOBIENSTWO

ISTOTNOŚĆ ZAGROŻENIA

Istotność	W skrócie	Poufność	Klasyfikacja danych	Dostępność
A	Mało istotne	Ujawnienie danych nie powoduje żadnych negatywnych konsekwencji.	Zwykłe	Mało ważne. Utrata danych nie spowoduje utrudnień w pracy placówki, można bez problemu odtworzyć dane lub uzyskać dostęp do danych w innym miejscu.
B	Ograniczone	Ujawnienie danych powoduje drobne szkody i może narazić podmiot na kłopoty np. możliwość odpowiedzialności z ustawy (ochrona danych osobowych).	Wrażliwe	Średnio ważne. Utrata danych spowoduje zakłócenia w pracy i konieczność odtwarzania danych, ale są one odtwarzalne. Zakłócenia potrwać najwyżej 1 dzień roboczy.
C	Poważne	Ujawnienie danych powoduje znaczne szkody, odpowiedzialność z ustawy (ochrona danych osobowych) i kary finansowe.	Wrażliwe	Ważne. Utrata zasobu spowoduje zakłócenia w pracy i konieczność odtwarzania danych, z trudem będą odtwarzalne, zakłócenia potrwać co najmniej kilka dni roboczych.
D	Krytyczne	Ujawnienie danych powoduje znaczne szkody, utratę przychodów, cofnięcie zezwolenia na działanie placówki, odpowiedzialność z ustawy (ochrona danych osobowych).	Wrażliwe/Ścisłe poufne/Zastrzeżone	Bardzo ważne. Utrata zasobu spowoduje zakłócenia w pracy i konieczność odtwarzania danych, z trudem będą odtwarzalne lub nie będzie możliwość odzyskania danych.

PRAWDOPODOBIENSTWO

Ocena	W skrócie	Częstotliwość
1	Znikome	Wątpliwe żeby zagrożenie wystąpiło, wydaje się to niemożliwe np. nieuprawniony dostęp do dokumentów przechowywanych w strzeżonym sejfie, w pokoju z dostępem na kod.
2	Małe	Może się zdarzyć (raz na kilka lat), ale wystąpienie jest raczej mało realne.
3	Średnie	Może się zdarzyć (raz na rok)
4	Duże	Zagrożenie jest bardzo realne, prędzej czy później się zdarzy (raz na kwartał)

A8 Jaka została podjęta decyzja w kontekście wskazanego poziomu ryzyka dla analizowanego procesu i zagrożenia?

Decyzja

☐ Akceptacja

☐ Redukcja

☐ Unikanie

☐ Przeniesienie

Inne Produkty

Weryfikacja dostosowania do RODO

Audyt bezpieczeństwa

Ograniczenie dostępu

Uzupełnienie Polityki Bezpieczeństwa/procedur o inne obszary

Wykonanie szacowania ryzyk i ich wdrożenie

Możliwe zastosowania KS-BDO do dokumentowania innych rozwiązań



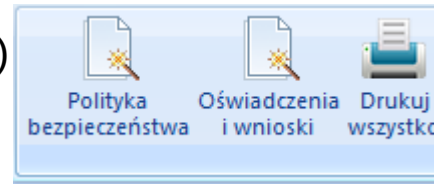
Pomocy

Co dalej

Generacja Polityki Bezpieczeństwa i procedur z nią związanych

Uporządkowanie dostępów do danych (prawne, fizyczne)

Wdrożenie zabezpieczeń wynikających z analizy ryzyk



Ciągła weryfikacja/monitoring bezpieczeństwa (poziom bezpieczeństwa w aplikacjach), obsługa incydentów, testy bezpieczeństwa własnej infrastruktury

Aktualizacja Produktów i warstwy techniczno-systemowej a w szczególności w wyniku publikacji poprawek krytycznych

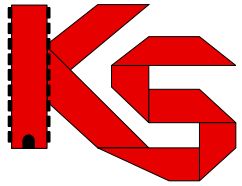
Przestrzeganie praw wolności osób (poprawa danych, wgląd, pobranie kopii danych, prawo do bycia zapomnianym)

Współpraca z moim Partnerem/Dostawcą rozwiązań w celu doskonalenia Produktów

Rozwiązania chmurowe KAMSOFIT



*Każda droga prowadzi do Rzymu
ale czasami jest za długa*



DZIĘKUJĘ ZA UWAGĘ
THANK YOU FOR YOUR ATTENTION

