Gdański Obszar Metropolitalny

Audyt Bezpieczeństwo Informacja
Consulting Jarosław FELIŃSKI
Kontakt 602-105-852; 508-608-136

# „Zakres aktualizacji PBI w świetle nowelizacji przepisów UODO obowiązujących w organizacji”

***-NOWE REGULACJE WYBORCZE 2014 –***

***Ustawa z dnia 5 stycznia 2011r. Kodeks wyborczy [Dz. U. 2011 nr 21 poz. 112]***

## *PRELEGENCI*


*JAROSŁAW J. FELIŃSKI*
*Główny Ekspert*
*TÜV NORD POLSKA Sp. z o.o.*
*ds. Ochrony Danych Osobowych*
*AUDYTOR WIODĄCY 27001*

*BARBARA SZYMAŃSKA*
*Dyrektor IT - UM GDAŃSK*
*Audytor wiodący 27001*

# „CZTERY NOWELE I ODO”

✓ **UODO – 2011/03/07 - art. 29 - 30**

ZMIANA

- ✓ Ustawa z dnia 5 stycznia 2011r. Kodeks wyborczy - [Dz. U. 2011 nr 21 poz. 112]
- ✓ SIO – 2012 – system informacji oświatowej
- ✓ Nowy zbiór do zgłoszenia w GIODO

ZMIANA

- ✓ OD DNIA - 01.07.2013 r.
- ✓ Ustawa z dnia 01.07.2011 r. o zmianie ustawy o utrzymaniu czystości i porządku w gminach oraz niektórych innych ustaw (Dz. U. z 2011 r. Nr 152 poz. 897 ze zm.), która wejdzie w życie z dniem 01.07.2013 r. - tzw. „śmieciówka”
- ✓ Nowy zbiór do zgłoszenia w GIODO

ZMIANA

- ✓ ROZPORZĄDZENIE RADY MINISTRÓW z dnia 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 - PN - ISO 17799 i 27001

ZMIANA

**2014 - ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) - 12 marca 2014 !**

**ZAPOWIADANA ZMIANA**

ISO27001

# „CZTERY NOWELE I ODO"

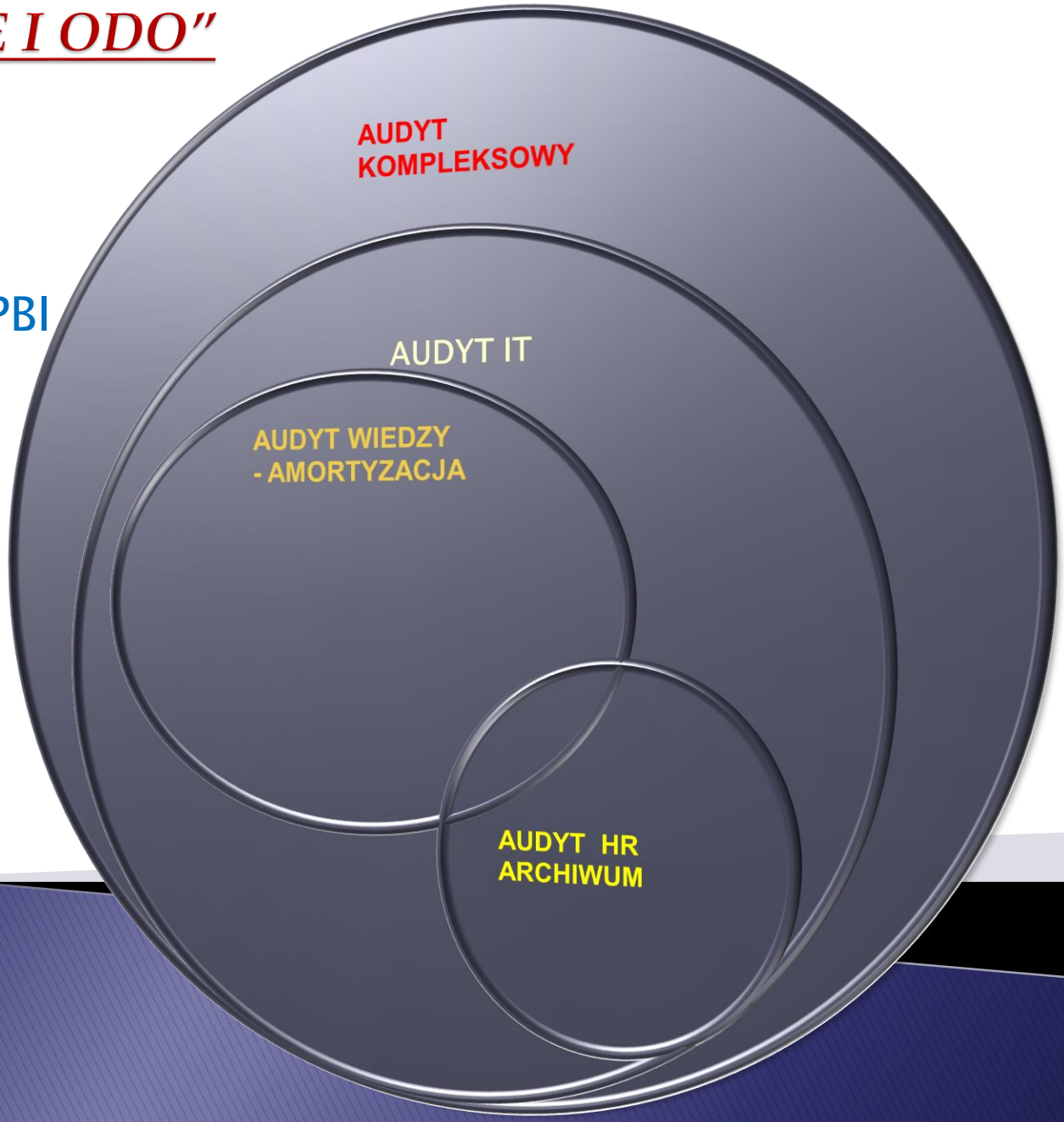
1.Audyt

2.Kontrola Zarządcza PBI

3. INSPEKCJA GIODO

4. INSPEKCJA PIP

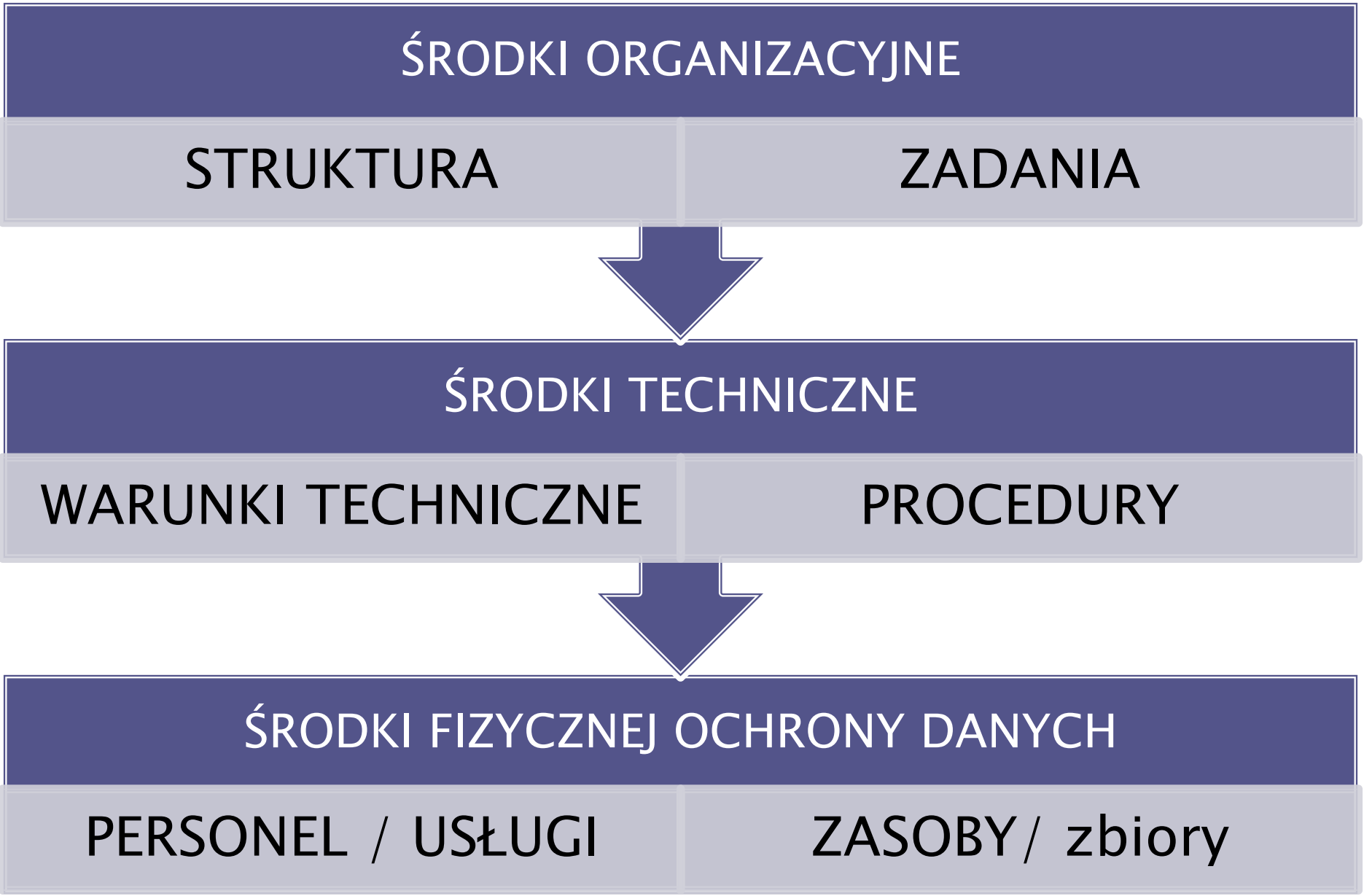
5. INNE KONTROLE



## Przepisy wewnętrzne które należy zweryfikować


- ***INSTRUKCJA KANCELARYJNA;***
- ***JRWA;***
- ***ZAKRESY OBOWIĄZKÓW***

# „Zakres aktualizacji PBI… art.36 UODO



# „Zakres aktualizacji PBI… art.36 UODO

**I. Podstawowe obowiązki ABI:**

ABI w strukturze organizacji;
status i zakres zadań ABI;
dokumentowanie przetwarzania i ochrony danych (polityka i instrukcja): celowość opracowania PBI, analiza ryzyka – co ocenić i jak, ocena zagrożeń
– PN 27001 i 17799.

**II. Obowiązki prawne ABI:**

przesłanki legalności przetwarzania danych osobowych;
zakres i cel przetwarzania danych, poprawność i adekwatność przetwarzanych danych osobowych;
obowiązek informacyjny;
powierzenie przetwarzania danych osobowych – umowa powierzenia

**III. Obowiązki organizacyjne ABI:**

struktura organizacyjna ochrony danych osobowych;
upoważnienia do przetwarzania danych – wariant;
ewidencja osób uprawnionych do przetwarzania danych osobowych;
reagowanie na incydenty;
zasady prowadzenia nadzoru wewnętrznego.

# „Zakres aktualizacji PBI… art.36 UODO

**IV. Obowiązki ABI w zakresie zabezpieczeń fizycznych – zabezpieczenia fizyczne pomieszczeń, nośników, zbiorów papierowych, elektronicznych.**

**V. Obowiązki ABI w zakresie zabezpieczeń informatycznych:**

cloud computing – nowa jakość zarządzania czy nowe zagrożenie?
wymagana dokumentacja;
zadania funkcyjnych (ABI/ ASI):

poziomy bezpieczeństwa**,**

wymagania dla systemów informatycznych,
tryb nadawania uprawnień użytkownikom,

**praca z systemem,**
**kopie bezpieczeństwa,**
**ochrona antywłamaniowa i antywirusowa,**
**przeglądy i konserwacja systemów.**

# „Zakres aktualizacji PBI… art.36 UODO

**VI. Obowiązki ABI w zakresie:**

- analizy i weryfikacji sprawdzonych wzorów organizacyjnych ochrony danych;
- sposobu prowadzenia szkoleń, kontroli, nadzorów;
- nowych kompetencji GIODO po nowelizacji Ustawy;
- „udaremniania” lub „utrudniania” kontroli;
- wykorzystywania i zabezpieczenia danych biometrycznych;

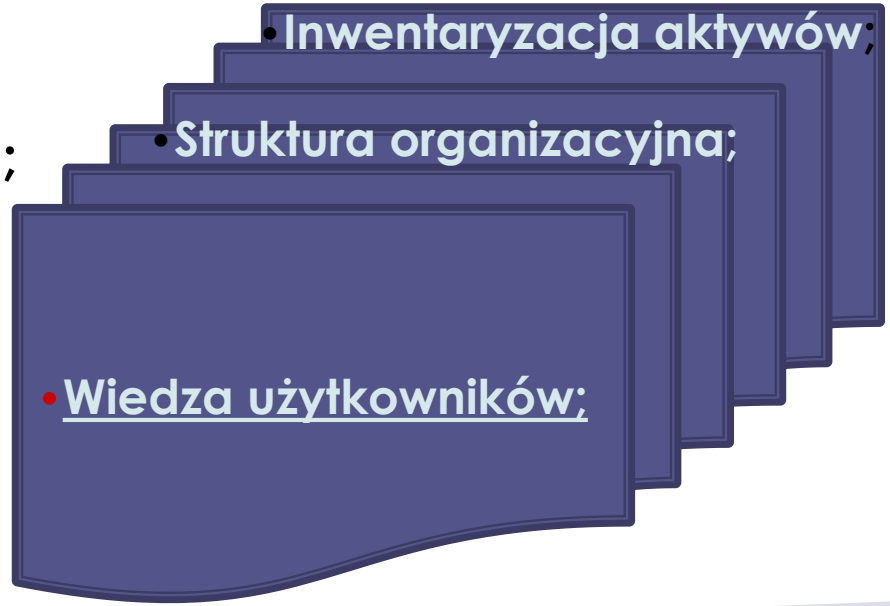
audytowania po wdrożeniu PBI;

# „Zakres aktualizacji PBI… art.36 UODO

**Procesowe zasady tworzenia dokumentacji:**

- **SIWBI –** specyfikacja istotnych warunków bezpieczeństwa informacji;

- Analiza potrzeb;
- Określenie możliwości budżetowych;
- Dywersyfikacja zadań;
- Wdrożenie dokumentacji;
- Szkolenia informacyjne;
- Amortyzacja sprzętu IT;

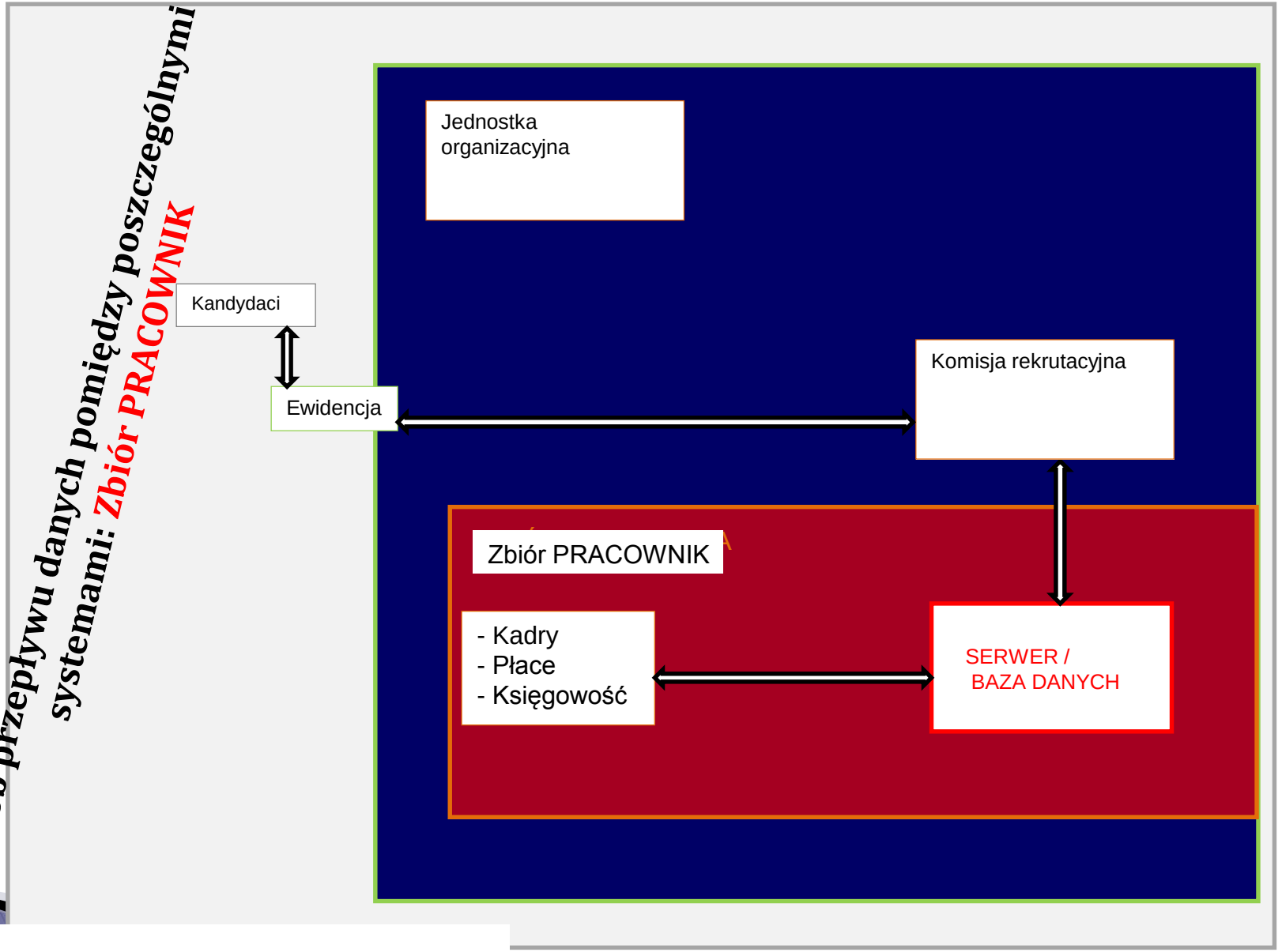



- WSPARCIE? ABI/ AuBI / MBI / IODo

# „Zakres aktualizacji PBI... art.36 UODO

INTERNET

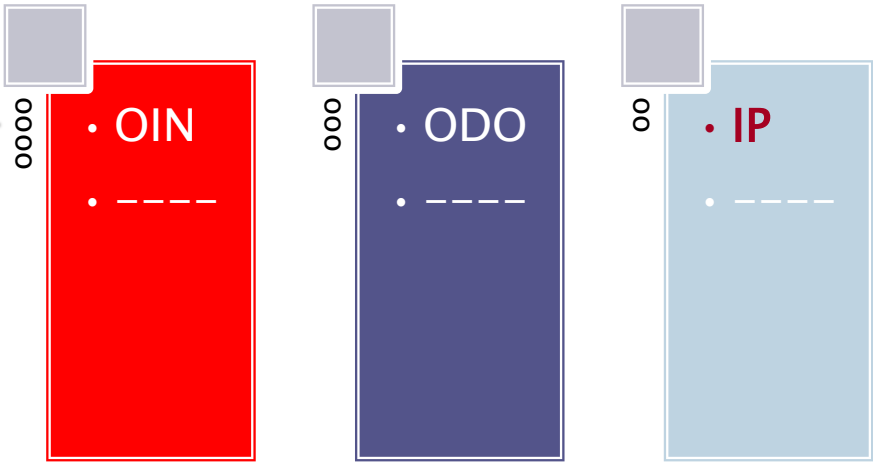
PRZEPŁYW DANYCH WARIANT




Brak dostępu do bazy spoza sieci wewnętrznej

# „Zakres aktualizacji PBI… art.36 UODO

- Klasyfikacja informacji – aktywów informacyjnych
- *„różnorodność”*
- *„różnowartość”* danych – analiza struktury organizacji
- *zagrożenie* – to brak schematu organizacyjnego, oraz właściwie wyznaczonych – *Administratorów*
- *ochrony informacji niejawnych,[ OIN ]*
- ochrony danych osobowych,
- *informacja publiczna*



# „Zakres aktualizacji PBI… art.36 UODO

WNIOSEK KLIENTA

BOK

DZIAŁ

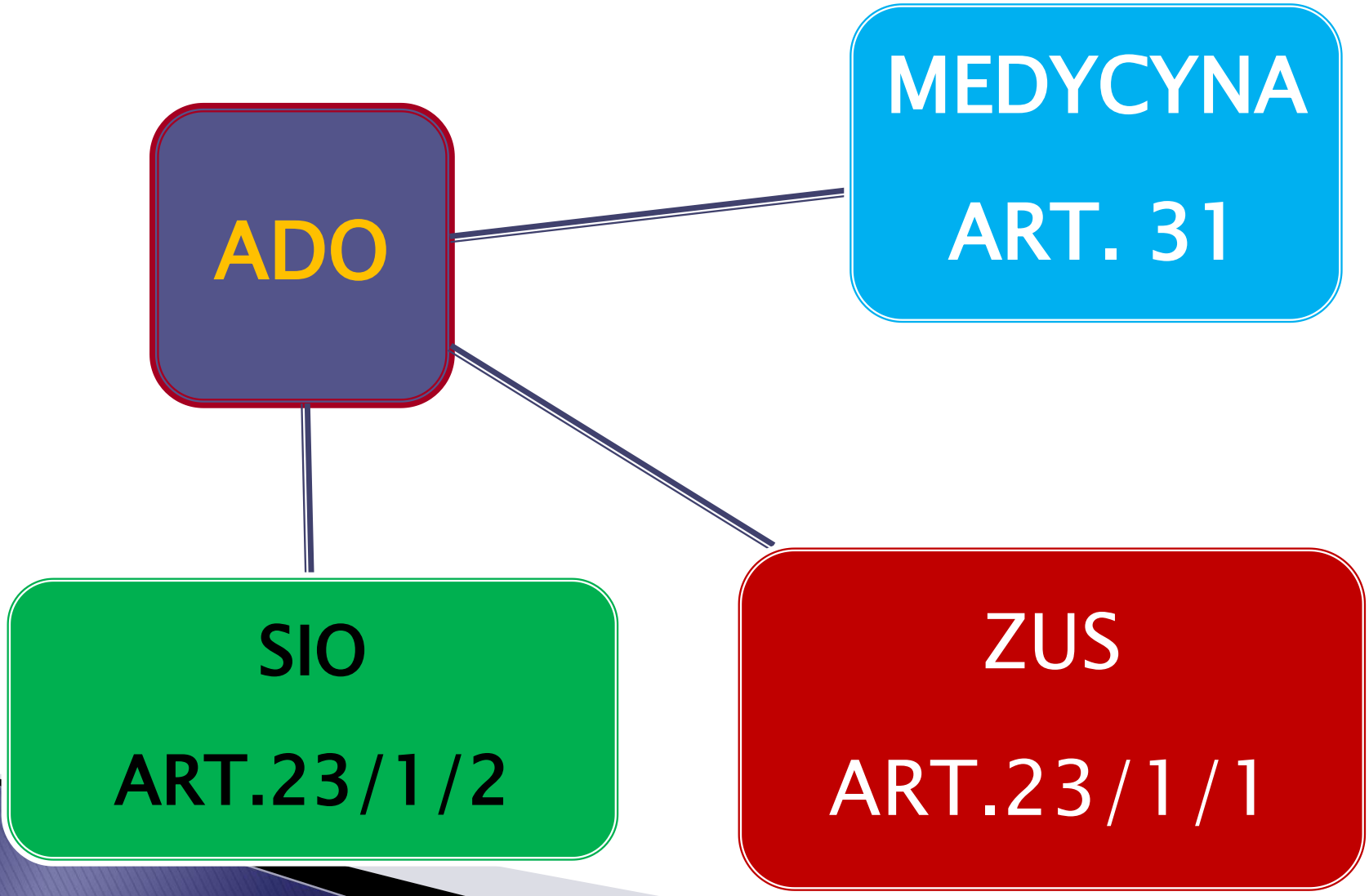
WEWNĘTRZNY CYKL PRZETWARZANIA

OPINIA ABI

DECYZJA ADO

# „Zakres aktualizacji PBI… art.36 UODO

## TRANSFER ZEWNĘTRZNY DANYCH



# „Zakres aktualizacji PBI… art.36 UODO

Kolejność uświadamiania potrzeby ochrony informacji, w aspekcie tworzenia infrastruktury bezpieczeństwa informacji.

**1) Kierownictwo organizacji – konieczne zaangażowanie**

***Forum bezpieczeństwa – KKO PN ISO 27001***

- *zróżnicowanie potrzeb komórek organizacyjnych*
- *Kadry, IT, Marketing, Obsługa Klientów*
- *Doręczenia, Windykacje, Archiwum* ; *Szacowanie ryzyka (27001)*

2) Funkcyjni ABI, ASI

**3) Użytkownicy**

# „Zakres aktualizacji PBI… art.36 UODO

***Teczka PBI***

- *Zarządzenie*
- *Instrukcje [ PBI, IZSI oraz dodatkowe uregulowania ]*
- *==========*

- *Upoważnienia*
- *Oświadczenia*
- *Wykaz/ewidencja*
- *==========*

- *Notatki poaudytowe*
- *Raporty*
- *Analizy i opinie*
- *Plany szkoleń*
- *Sprawdziany/wyniki*
- *Zapotrzebowania na środki finansowe*

# „Zakres aktualizacji PBI… art.36 UODO

**Audyt** – ocena danej osoby, organizacji, systemu, procesu, projektu lub produktu. Audyt jest przeprowadzany w celu upewnienia się co do prawdziwości i rzetelności informacji, a także oceny systemu kontroli wewnętrznej.

Celem audytu może być weryfikacja, czy cel został osiągnięty lub czy jej działania są zgodne z zaakceptowanymi standardami, statusem czy praktykami. Audyt ocenia także procedury kontrolne celem stwierdzenia, czy przedmiot audytu także w przyszłości będzie odpowiadał uzgodnionym do stosowania wymaganiom. Oprócz oceny wskazuje także zalecenia zmian w procedurach, w tym sprawdzających oraz w politykach.[HARMONOGRAM NAPRAWCZY]

KRI –**§ 20.** :

**6) zapewnienia szkolenia osób**

**14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.**

# „Zakres aktualizacji PBI… art.36 UODO

***ALFABET ABI -***
***abecadło Felińskiego***

A – aktywa, **adekwatność**, administrator, audyt (or)
B – bezpieczeństwo, biznes, bezpośredniość
C – **celowość** ochrony informacji
D – deklaracja stosowania, **dostępność**, doskonalenie,
E – efektywność, elastyczność, eksploatacja
F – funkcjonalność, formy ochrony
G – gwarancja ochrony
H – hasła dostępu, homologacje, historie zdarzeń
I – informacja, **integralność**, identyfikacja, incydent
J– jakość, jednolitość informacji
K– kierownictwo, kompletność, kryteria
L– **legalność**, lokalizacja informacji

# „Zakres aktualizacji PBI… art.36 UODO

M– **metodyki**, monitorowanie, mankamenty

N– niezawodność, niezaprzeczalność, naruszenie

O – organizacja, obszary, **odpowiedzialność**

P – poufność, proporcjonalność, procesy, podatność, przeglądy, **przetwarzanie**, powierzanie danych; przepływ

R – ryzyko, rozliczalność, różnorodność

S – system, skuteczność, szacowanie, SZKOLENIE

T – terminy, technika, transakcje, **transfer danych**

U – utrzymanie, ubezpieczenie, usługi, utrata, udostępnianie

W –wdrażanie, wykonalność, własność, wyciek

Z – zarządzanie, zabezpieczenia, zagrożenia

**ROZPORZĄDZENIE RADY MINISTRÓW** z dnia **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 teleinformatycznych1)**

# „Zakres aktualizacji PBI… art.36 UODO

„HISTERYCY DANYCH OSOBOWYCH”

Cytat:

[…] tyle że urzędnicy, jeśli mają podjąć samodzielną decyzję, a nie są pewni, odpowiedzą odmownie […]

[…] Miewają też braki w wiedzy, a co gorsza – nie bardzo mają warunki, żeby tą wiedzę uzyskać i jak zauważa mec. Litwiński, bywa, że pomocy szukają w internecie, zamiast sięgnąć do prawniczej lektury.

>> ZATEM NIE PBI, NIE PROCEDURY

ALE WIEDZA UŻYTKOWNIKÓW ZAPEWNI

SKUTECZNOŚĆ PRZEPŁYWU DANYCH

WEWNĄTRZ I NA ZEWNĄTRZ JEDNOSTKI ORGANIZACYJNEJ <<

Dziennik Gazeta Prawna – 11/13/04/2014r [bieżąca] str. A8 –"Histeria danych osobowych" – autorstwa P. Mira Suchodolska.

# „Zakres aktualizacji PBI… art.36 UODO

- Dziękuję za uwagę.
- jaroslaw.felinski@gazeta.pl
- Proszę o zadawanie pytań