

## AUDYT ZGODNOŚCI Z RODO

**W CELU ZMINIMALIZOWANIA RYZYKA UTRATY DANYCH OSOBOWYCH ORAZ  
SPRAWDZENIA CZY WDROŻONE ROZPORZĄDZENIE RODO JEST DOBRZE  
ZAIMPLEMENTOWANE W ŚRODOWISKU URZĘDU - FIRMY  
POLECAMY WYKONANIE AUDYTU ZGODNOŚCI RODO**

25. maja 2018 zaczęło obowiązywać rozporządzenie europejskie RODO. Sądząc po dużej ilości telefonów i pytań kierowanych do naszych specjalistów bezpośrednio od Prezesów i Inspektorów Danych Osobowych odpowiedzialnych za utrzymanie rozporządzenia w zgodności z RODO w organizacjach stwierdzamy, że nadal brakuje dobrych praktyk i podstawowej wiedzy w tym zakresie.

Nasze szkolenia i warsztaty przygotowane specjalnie dla FIRM pozwolą uzupełnić niezbędną wiedzę na ten temat. Dodatkowo podczas **AUDYTU ZGODNOŚCI Z RODO** nasi specjaliści określą stan wdrożenia obowiązującego rozporządzenia unijnego RODO.

Celem audytu zgodności z RODO jest potwierdzenie, czy zgodnie z ustawą RODO zostały zidentyfikowane **wszystkie procesy przetwarzania danych osobowych** oraz ocena tych zgodności z przepisami obowiązującego prawa.

### ZAKRES DZIAŁAŃ AUDYTU ZGODNOŚCI Z RODO

#### 1. Sprawdzenie działań prowadzonych przez dział IT

- Sprawdzenie jak zostały zmodyfikowane zasoby IT oraz funkcjonujące dotychczas zabezpieczenia informatyczne i fizyczne w odniesieniu do wymagań prawnych.
- Sprawdzenie czy wdrożone narzędzia informatyczne wspomagające proces zarządzania bezpieczeństwem danych zostały odpowiednio zmodyfikowane.

#### 2. Analiza ochrony danych osobowych

- Analiza prowadzonych procesów funkcjonujących w banku oraz zakresu i celów przetwarzanych danych osobowych.
- Analiza czy zbiory danych osobowych zostały prawidłowo zdefiniowane oraz sprawdzenie czy podstawy prawne ich przetwarzania zostały prawidłowo określone.
- Sprawdzenie jak zostały określone wymagania i obszary prawne, które miały być dostosowane do wymagań RODO.

- Ocena klasyfikacji procedur funkcjonujących w organizacji z analizą działań mających na celu ochronę danych.

### **3. Ocena analizy ryzyka dla zinwentaryzowanych zbiorów**

- Ocena skutków dla ochrony danych na podstawie analizy ryzyka związanej z przetwarzaniem danych osobowych.
- Sprawdzenie stanu niezbędnych zabezpieczeń fizycznych i systemowych pod kątem zgodności z nowymi przepisami.

### **4. Sprawdzenie opracowanej Polityki Bezpieczeństwa**

Sprawdzenie opracowanej dokumentacji wewnętrznej dotyczącej czynności przetwarzania danych, zawierającej m.in. procedury:

- nadawania uprawnień do przetwarzania danych oraz metod i środków uwierzytelniania w systemach informatycznych,
  - tworzenia i przechowywania kopii zapasowych
  - zabezpieczenia systemu informatycznego przed działaniem szkodliwego oprogramowania
  - współpracy z dostawcami usług, wykonywania przeglądów i konserwacji
  - zarządzania wykorzystywanym oprogramowaniem
- Rozmowa z Inspektorem Danych Osobowych czy obowiązki zostały prawidłowo określone
- Sprawdzenie poprawności prowadzonego REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH
- Analiza opracowanych klauzul informacyjnych, formuł zgód na przetwarzanie danych osobowych. W razie nadmierowej interpretacji uproszczenie niezbędnych zapisów
- Sprawdzenie czy zostały podpisane zweryfikowane umowy z kontrahentami/usługodawcami pod kątem wymaganych prawem klauzul poufności i wymagań w przypadku powierzenia danych osobowych
- Sprawdzenie jak zostały przygotowane uprawnienia dla pracowników
- Sprawdzenie wdrożonych wzorów pozostałych dokumentów określonych w Rozporządzeniu

### **5. Szkolenie dla pracowników**

- Oferujemy szkolenie kierunkowe dla pracowników poszczególnych działów urzędu - firmy w celu określenia i sprawdzenia jak wykonywane są przez nich nowe obowiązki względem rozporządzenia RODO
- W razie konieczności przeprowadzimy szkolenie dla kadry zarządzającej i pracowników dopuszczonych do przetwarzania danych osobowych.

- Szkolenie uzupełniające jak należy na stanowisku bezpośredniej obsługi klienta przestrzegać ZASAD obowiązujących w kontakcie z Klientem:
  - 1) **ZASADA CZYSTEGO BIURKA**

wyraża się tym, że zarówno dokumentów papierowych, jak i jakichkolwiek innych nośników informacji (płyty CD, DVD, pamięci flash, USB itp.) nie pozostawia się bez nadzoru.
  - 2) **ZASADA CZYSTEGO EKRANU**

każdorazowe opuszczenie pomieszczenia w godzinach pracy powinno zostać poprzedzone zablokowaniem komputera, każdorazowe opuszczenie stanowiska pracy w celu załatwienia czynności musi być poprzedzone zablokowaniem ekranu komputera; na wszystkich stacjach aktywny jest wygaszacz ekranu zabezpieczony hasłem, który aktywizuje się automatycznie po przekroczeniu max. 5 – 10 lub 15 minut braku aktywności. Każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony.
  - 3) **ZASADA CZYSTEGO KOSZA**

nieprzydatne dokumenty, brudnopisy, zbędne kopie muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Do kosza na śmieci nie wyrzuca się płyt CD/DVD ani innych nośników; powinny one zostać zniszczone w specjalistycznych niszczarkach. W przypadku, gdy będzie to niemożliwe, nośniki te należy przekazać do Wydziału Informatyki celem ich utylizacji.
  - 4) **ZASADA CZYTEJ DRUKARKI**

wszyscy pracownicy, praktykanci i stażyści zobowiązani są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za dane urządzenie lub zgłosić incydent bezpieczeństwa.
  - 5) **ZASADA WIEDZY KONIECZNEJ**

w myśl której dostęp do informacji ograniczony jest do tych, które są niezbędne do prawidłowego wykonywania obowiązków na danym stanowisku. Za przestrzeganie tej zasady odpowiedzialni są kierownicy.
  - 6) **ZASADA ODPOWIEDZIALNOŚCI ZA ZASOBY**

każdy, kto przetwarza informacje jest odpowiedzialny za zapewnienie ich dostępności, poufności i integralności poprzez przestrzeganie procedur ich bezpiecznego przetwarzania oraz ochronę przyznaných zasobów, w tym za szkody wyrządzone w systemie informatycznym przez nieautoryzowane oprogramowanie lub niewłaściwe korzystanie z urządzeń systemu informatycznego.

7) **ZASADA CHRONIONEGO POMIESZCZENIA**

wyraża się tym, że pod nieobecność osoby uprawnionej w pomieszczeniach (poza ogólnodostępnymi typu korytarze) nie mogą przebywać osoby postronne, po opuszczeniu pomieszczenia osoba odpowiedzialna zamyka je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi ewakuacja).

8) **ZASADA ŚWIADOMOŚCI ZBIOROWEJ**

wszyscy są świadomi konieczności ochrony zasobów, zapewnienia ich dostępności, poufności, integralności i aktywnie w tym procesie uczestniczą.

9) **ZASADA ŚWIADOMEJ KONWERSACJI**

polega na tym, że nie zawsze i wszędzie trzeba mówić co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.

10) **ZASADA NADZOROWANIA KLUCZY I KART MAGNETYCZNYCH**



pobrane klucze i karty magnetyczne do pomieszczeń powinny być zawsze pod kontrolą. Pracownicy odpowiedzialni są za należyte zabezpieczenie kluczy do ich biurek stanowiskowych i szaf biurowych, w których przechowywane są dokumenty; ostatni pracownik opuszczający dane pomieszczenie po zakończeniu pracy zamyka szafy i chowa klucze w bezpieczne, ustalone z pozostałymi współpracownikami miejsce.

Ta sama zasada dotyczy dystrybucji kart magnetycznych, którymi otwierane są dostępy do stref specjalnych np. serwerowni. Po zakończeniu prac w serwerowni przez upoważnionych pracowników karta powinna być zdeponowana w dystrybutorze kart magnetycznych i kluczy. Nadzór nad dystrybutorem powinna sprawować osoba odpowiedzialna za nadzór dostępu do pomieszczeń

11) **ZASADA CZYSTEJ TABLICY**

w przypadku korzystania z tablic w salach ogólnodostępnych osoba organizująca spotkanie musi uprzątnąć wszystkie pozostałe tam materiały i wyczyścić tablice; pracownicy korzystający z tablic w biurach zobowiązani są do nie zamieszczania na tablicach informacji podlegających ochronie.

12) **ZASADA LEGALNOŚCI OPROGRAMOWANIA**

zabrania się samodzielnego instalowania oprogramowania, a także przechowywania na komputerach treści naruszających prawo.

- 13) **ZASADA WERYFIKACJI PRZENOŚNYCH NOŚNIKÓW DANYCH** (np. pendrive, CD, DVD)  
każdy komputer wymusza przeprowadzenie skanowania przez system antywirusowy zewnętrznych nośników danych przed ich uruchomieniem.
- 14) **ZASADA ZGŁASZANIA ZDARZEŃ , INCYDENTÓW, NIEPRAWIDŁOWEJ PRACY SPRZĘTU**  
każdy użytkownik systemu zobowiązany jest do zgłaszania do Działu Informatyki wszelkich zauważonych nietypowych zdarzeń, incydentów oraz nieprawidłowej pracy sprzętu.
- 15) **ZASADA MONITORINGU STANOWISKA KOMPUTEROWEGO**  
każde stanowisko komputerowe jest objęte monitorowaniem działania użytkowników i oprogramowania.
- 16) **ZASADA ASEKURACJI – REDUNDANCJI**  
polega na tym, że każdy mechanizm zabezpieczający system jest ubezpieczony drugim; w szczególnych przypadkach może zostać zastosowana większa liczba mechanizmów zabezpieczających; możliwe jest stosowanie zabezpieczeń technicznych i organizacyjnych.
- 17) **ZASADA KOMPLETNOŚCI**  
skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
- 18) **ZASADA EWOLUCJI**  
każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
- 19) **ZASADA ODPOWIEDZIALNOŚCI**  
używane mechanizmy muszą być adekwatne do sytuacji.
- 20) **ZASADA AKCEPTOWALNEJ RÓWNOWAGI**  
podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.
- 21) **ZASADA INDYWIDUALNEJ ODPOWIEDZIALNOŚCI**  
za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
- 22) **ZASADA OBECNOŚCI KONIECZNEJ**  
prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
- 23) **ZASADA STAŁEJ GOTOWOŚCI**  
system jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
- 24) **ZASADA NAJSŁABSZEGO OGNIWA**  
poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.

25) **ZASADA UPRAWNIONEGO DOSTĘPU DO INFORMACJI**

pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje stosowne oświadczenie o zachowaniu poufności.

26) **ZASADA ŚWIADOMOŚCI ZBIOROWEJ**

wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych banku i aktywnie uczestniczą w tym procesie.

Po przeprowadzeniu inwentaryzacji procesów przetwarzania danych osobowych następuje analiza wraz z Inspektorem Danych Osobowych lub osoba odpowiedzialną jakim obowiązkom podlega organizacja w stosunku do RODO i czy te obowiązki zostały poprawnie wdrożone przez urząd - firmę jako administratora danych osobowych. Po przeprowadzonych analizach zostanie sporządzony protokół, w którym zostaną wskazane rozbieżności w spełnieniu wymagań ustawy RODO.

Na życzenie Klienta dodatkowo możemy wykonać wdrożenie polityki ochrony danych osobowych w całości lub w określonym obszarze, gdyby pojawiły w tym zakresie niejasności.

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

602 220 749                    [andrzej.popiolek@servus-comp.pl](mailto:andrzej.popiolek@servus-comp.pl)

781 555 025                    [anna.strek@servus-comp.pl](mailto:anna.strek@servus-comp.pl)

12 631 91 22                    [biuro@servus-comp.pl](mailto:biuro@servus-comp.pl)

**Servus Comp Sp. z o.o. Sp.k.**

ul. Mazowiecka 25/502, 30-019 Kraków  
Sąd Rejonowy dla Krakowa – Śródmieście,  
XI Wydział Gospodarczy Krajowego Rejestru Sądowego  
NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481

<https://zadbajobezpieczenstwo.pl>

<https://firmapremium.zadbajobezpieczenstwo.pl>

<https://premiumbank.zadbajobezpieczenstwo.pl>

**Nota prawna:**

1. Zaprezentowany materiał jest autorskim opracowaniem i jest objęty prawem autorskim.
2. Niniejszy materiał, ani żaden jego fragment nie może być reprodukowany, przetwarzany i rozpowszechniany w jakikolwiek sposób za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i in. do celów innych niż realizacja przedmiotowej umowy u Klienta.