



**Jesteśmy gotowi – oferta firm szkoleniowo-doradczych z zakresu RODO**

**Konferencja**

**RODO PIĘĆ PO 12-TEJ**

czyli Rozporządzenie o Ochronie Danych Osobowych nowe fakty, interpretacje

---

15 czerwca 2018 r., Muzeum Lotnictwa, al. Jana Pawła II 39, Kraków

# Dzień dobry



Marcin Rek,  
Dyrektor ds. Rozwoju Biznesu  
nFlo Sp. z o.o.

[Marcin.Rek@nFlo.pl](mailto:Marcin.Rek@nFlo.pl)

+48 501 175 514

# Pion Bezpieczeństwa Biznesowego - Usługi

- ∞ Ochrona bezpieczeństwa osobowego i obiektowego.
- ∞ Doradztwo i wsparcie w zakresie zarządzania Organizacją.
- ∞ Zapobieganie ryzykom nadużyć, korupcji, prania pieniędzy (AML).
- ∞ Systemy i środki antykorupcyjne
- ∞ Whistleblowing IT System
- ∞ Audyty bezpieczeństwa ochrony informacji w systemach IT.
- ∞ Przygotowanie do audytów zgodności z Normami ISO.

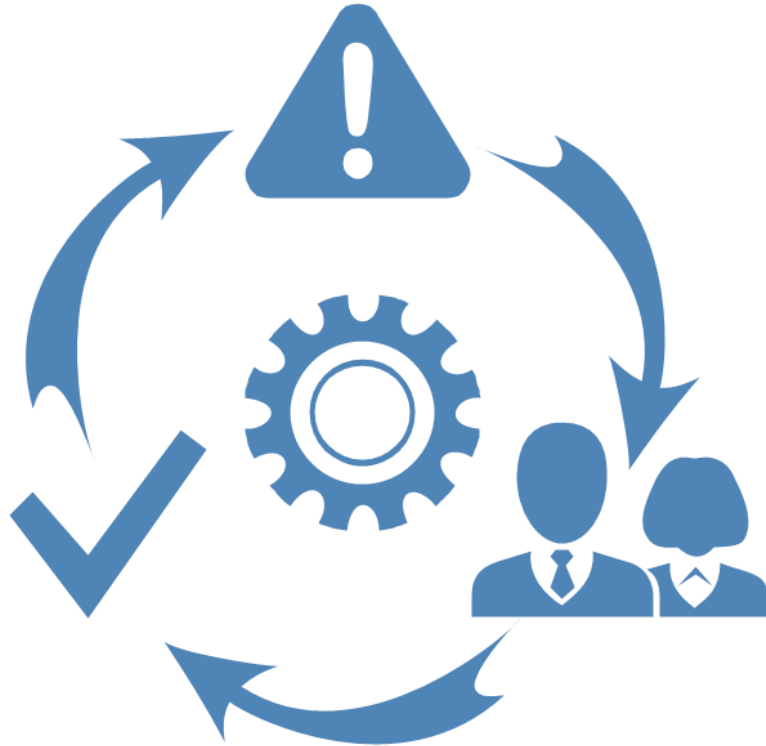
# Ochrona Bezpieczeństwa Osobowego i Obiektowego

- ∞ Ochrona Informacji,
- ∞ Ochrona danych osobowych/RODO: Analiza luk, Przeglądy, Doradztwo, Przygotowanie dokumentacji, Analiza Ryzyka Informacyjnego,
- ∞ Ochrona informacji niejawnych,
- ∞ Ochrona Infrastruktury Krytycznej – monitorowanie działalności podmiotu w zakresie ochrony infrastruktury krytycznej,
- ∞ Ocena i/lub opracowanie Planów Ciągłości Działania,
- ∞ Planowanie ochrony obiektowej, fizycznej, osobowej,
- ∞ Doradztwo/szkolenia z zakresu technik walki, interwencji, strzelania bojowego i policyjnego,
- ∞ Profilaktyka antyterrorystyczna.

# Jak szybko można wdrożyć RODO ???



Stosowanie RODO to proces ↗ ...



... ↗ którego cechą powinna być ciągłość działania

# 10 kroków do RODO

1. Przeprowadzenie wewnętrznego audytu **celem dokonania weryfikacji stanu prawnego i organizacyjnego** firmy w zakresie przygotowania do nowych regulacji.
2. Uświadomienie osobom kluczowym w organizacji, jakie mogą być konsekwencje niedostosowania organizacji do przepisów nowego rozporządzenia.
3. Dokonanie weryfikacji czy, z uwagi na skalę przetwarzania danych osobowych w organizacji, konieczne jest **prowadzenie rejestru czynności przetwarzania i powołanie Inspektora Ochrony Danych** (nawet jeżeli w organizacji nie będzie konieczności powołania Inspektora Ochrony Danych, dobrze jest powołać osobę odpowiedzialną za nadzór nad przetwarzaniem danych).
4. Ustalenie **zakresu i harmonogramu prac**, których wykonanie jest niezbędne do tego, żeby przetwarzać dane osobowe zgodnie z RODO.
5. **Analiza ryzyka** i dokonanie zmian w obowiązujących w firmie regulacjach wewnętrznych, takich jak polityka bezpieczeństwa, polityka prywatności, systemy IT etc.

# 10 kroków do RODO

6. Dostosowanie zgód, które dzisiaj zbieramy, które umożliwiają nam przetwarzanie danych osobowych, do nowych wymagań prawnych.
7. Weryfikacja procedur pod względem obejmowania wszystkich praw, jakie mają osoby fizyczne, w tym sposobów usuwania danych osobowych, przekazywania danych drogą elektroniczną etc.
8. Zastanowienie się nad wdrożeniem systemów dla weryfikacji wieku osób (chodzi głównie o dane osób małoletnich) i pozyskiwania zgody na czynności związane z przetwarzaniem danych od rodzica lub opiekuna prawnego.
9. Weryfikacja, działania odpowiednich procedur do wykrywania, raportowania i badania naruszeń ochrony danych osobowych, w tym bezpieczeństwa IT .
10. Zapoznanie się z wytycznymi dotyczącymi oceny skutków w zakresie ochrony danych DPIA Data Protection Impact Assessments i wypracowanie sposobu ich wdrożenia w organizacji.



# Przykładowy harmonogram usługi doradczej nFlo, przygotowania Firmy do procesu stosowania RODO

# Etap I

- I. Czas trwania: dzień pierwszy i drugi projektu.
  
- II. Zakres:
  1. Spotkanie organizacyjne.
  2. Szkolenie wstępne.
  
- III. Rezultat:
  1. Organizacja Zespołów Klienta i Doradcy.
    - a) utworzenie PMO Klienta;
    - b) nadzór nad Projektem, zarządzanie przepływem dokumentów i informacji;
    - c) uzgodnienie kanałów i częstotliwości komunikacji;
    - d) przeprowadzenie szkolenia wstępnego.
  2. Uzgodnienie słownika pojęć.
  3. Przedstawienie metodyki prac analitycznych.
  4. Wstępne zidentyfikowanie podstawowych procesów biznesowych, w których są przetwarzane dane osobowe i ich właścicieli.
  5. Uzgodnienie zakresu wyboru procesów Klienta przeznaczonych do analizy.
  6. Uzgodnienie harmonogramu Projektu.

# Etap II

- I. Czas trwania: do 3 tygodni
  
- II. Zakres:
  1. Wstępne rozpoznanie istniejącego SZBI, jego struktury, obszaru, zastosowania, podstawowych elementów, procedur i osób zaangażowanych.
  
  2. Wstępna analiza luk SZBI.
  
- III. Rezultat:
  1. Zidentyfikowanie gotowości Systemu Zarządzania Bezpieczeństwem Informacyjnym organizacji oraz posiadanej infrastruktury IT, do wymagań RODO.
  
  2. Zidentyfikowanie luk SZBI organizacji wraz z rekomendacjami.
  
  3. Raport Statusowy

# Etap III

- I. Czas trwania: do 3-4 tygodni
- II. Zakres:
  1. Identyfikacja oraz wycena zasobów informacyjnych.
- III. Rezultat:
  1. Zidentyfikowanie wszystkich obszarów przetwarzania danych osobowych, zakresów tych danych oraz ich wycena zgodnie z trzema wymaganiami:
    - a) P – poufność;
    - b) I – integralność;
    - c) D – dostępność.
  2. Zidentyfikowanie:
    - a) podstawy prawnej przetwarzania danych szczególnej kategorii;
    - b) dokonywania profilowania oraz podstawy prawnej profilowania: zgoda, usprawiedliwiony cel, przepis prawa
    - c) procesów, w których dochodzi do zautomatyzowanego podejmowania decyzji wobec osób, których dane dotyczą
  3. Raport Statusowy

# Etap IV

- I. Czas trwania: do 2 tygodni
- II. Zakres:
  1. Analiza zidentyfikowanych procesów przetwarzania danych osobowych.
- III. Rezultat:
  1. Poprzez rozpoznanie procesów biznesowych realizowanych w organizacji, wyspecyfikowanie tych, które wiążą się z przetwarzaniem danych osobowych i nadanie im określonego waloru istotności, z punktu widzenia konieczności wprowadzenia wymaganych zabezpieczeń.
  2. Raport Statusowy.

# Etap V

- I. Czas trwania: do 3-4 tygodni
  
- II. Zakres:
  1. Audyt Informatyczny.
  2. Audyt SZBI.
  
- III. Rezultat:
  1. Zidentyfikowanie zgodności posiadanych aplikacji informatycznych z RODO.
  2. Analiza sposobu zarządzania dostępem (kontami) do SI dla użytkowników tych systemów
  3. Raport Statusowy.

W związku z badaniem, które z procesów (szczególnie: HR, księgowość, usługi IT i prawne, bezpieczeństwo obiektywne i osobowe, marketing (w tym dane dostawców i klientów)), są bezpośrednio związane z przetwarzaniem danych osobowych, przeprowadzenie oceny zgodności z przepisami ciążącymi na administratorze danych, m. in. obowiązek informacyjny, prawo dostępu do danych, poprawność w zakresie określenia obszaru przetwarzania danych, prawo do usuwania danych, ich sprostowania, etc.

# Etap VI

I. Czas trwania: do 3 tygodni.

II. Zakres:

1. Audyt prawny.
2. Umowy.
3. Powierzenie danych.
4. Ewidencja upoważnień ADO.

III. Rezultat:

1. Analiza podstawowej dokumentacji przetwarzania danych osobowych organizacji.
2. Analiza poprawności procesu nadawania, odbierania i ewidencjonowania upoważnień do przetwarzania danych osobowych.
3. Analiza poprawności procesu nadawania, odbierania i ewidencjonowania uprawnień dostępowych do systemów informatycznych, służących do przetwarzania danych osobowych.
4. Analiza procesu zgłaszania incydentów i zagrożeń związanych z bezpieczeństwem informacji.
5. Analiza innych wewnętrznych procedur pod kątem zgodności z RODO – wykaz rekomendacji i sposobów ich realizacji.
6. Listy pytań kontrolnych i formularze dot. RODO.
7. Analiza zgodności umów powierzenia danych osobowych z przepisami ustawy o ochronie danych osobowych i RODO.
8. Ocena systemu GRC (Governance-Risk-Compliance) i jego gotowości do RODO.
9. Raport statusowy.

# Etap VII

- I. Czas trwania: 2-3 tygodni
- II. Zakres:
  1. System zarządzania ryzykiem dla RODO.
- III. Rezultat: „Polityka zarządzania ryzykiem informacyjnym”, w skład której wejdą:
  1. Metodyka zarządzania ryzykiem
    - a) Identyfikacja ryzyka,
    - b) Szacowanie ryzyka,
    - c) Pomiar ryzyka,
    - d) Ranking ryzyka,
    - e) Macierz ryzyka,
    - f) Mapa ryzyka,
    - g) Lista mechanizmów kontrolnych,
    - h) Rejestr ryzyka.
  2. Analiza ryzyka dla spełnienia wymagań RODO.
  3. Raport statusowy.



# Etap VIII

I. Czas trwania: do 3 tygodni.

II. Zakres:

1. Wypracowanie propozycji w zakresie usunięcia zidentyfikowanych luk.
2. Opracowanie projektów niezbędnych procedur, w związku z obowiązywaniem RODO.

III. Rezultat:

1. Opracowanie szczegółowych rekomendacji zmian w procesach biznesowych w celu zapewnienia zgodności z RODO.
2. Opracowanie projektów niezbędnych procedur, w kontekście i w związku z obowiązywaniem RODO.
3. Zaprojektowanie formularzy zgód.
4. Zaprojektowanie procedur dot. wypełniania obowiązków informacyjnych.
5. Zaprojektowanie szablonów zapisów do umów powierzenia danych osobowych.
6. Wsparcie w przygotowaniu rejestru wszystkich czynności przetwarzania danych osobowych (wzór rejestru, wytyczne dla systemów informatycznych w celu dostosowania do prowadzenia rejestru itp).
7. Wsparcie w ustaleniu okresów retencji poszczególnych kategorii danych osobowych.

**8. RAPORT KOŃCOWY** – o gotowości Systemu do spełniania wymagań RODO.

# Etap IX - szkolenia

- I. Czas trwania: 2 dni + e-learning
  
- II. Zakres:
  1. Poziom zarządczy.
  2. Poziom kierowniczy.
  3. Poziom pracowniczy (e-learning).
  
- III. Rezultat – nabyta i potwierdzona wiedza o stosowaniu RODO na każdym z poziomów, materiały szkoleniowe.

**Czas trwania oznacza zasób na przeprowadzenie badania; wartości te nie sumują się; harmonogram przeprowadzenia Projektu jest ostatecznie ustalany z FIRMA, a skumulowany czas realizacji to maksymalnie: 3,5-4 miesiące.**

# Usługi dodatkowe:

1. W przypadku takiej konieczności – możliwe jest zaprojektowanie umów do przekazywania danych poza EOG (do państw trzecich) oraz wsparcie w przygotowaniu wiążących reguł korporacyjnych, dla przedłożenia UODO do zatwierdzenia w trybie decyzji administracyjnej.
2. Rekomendujemy wykonanie audytu post implementacyjnego, realizowanego poprzez dokonanie punktowego sprawdzenia po upływie 3 miesięcy od zakończenia usługi. Czas trwania takiego audytu to ok. 2 tygodnie.

# Korzyści

- ∞ Zapewnienie profesjonalnego, stabilnego, ostrożnego i wiarygodnego zarządzania obszarem ochrony danych osobowych, zgodnego z wymaganiami RODO,
- ∞ Powiązanie bezpieczeństwa podstawowych procesów produkcyjnych z bezpieczeństwem teleinformatycznym i ochroną danych osobowych,
- ∞ Uniknięcie odpowiedzialności prawnej i reputacyjnej,
- ∞ Wzrost świadomości pracowników,

# Korzyści

- ∞ Lepsza ochrona danych osobowych,
- ∞ Ocena rozwiązań w zakresie Governance-Risk-Compliance,
- ∞ Przegląd systemów IT i wydanie rekomendacji w zakresie dostosowania ich działania wg wymagań RODO przez niezależnego i profesjonalnego Doradcę,
- ∞ **Rozsądne zapewnienie**, że Kierownictwo uniknie wysokich kar administracyjnych, z tytułu nawet nieświadomego zaniechania obowiązków.

# Szkolenia - Centrum Edukacyjne Effective IT Trainings

- ∞ Ochrona danych osobowych - przygotowanie do wprowadzenia RODO.
- ∞ Inspektor Ochrony Danych - dwudniowy certyfikowany kurs z egzaminem.
- ∞ Audytor Systemu Zarządzania Bezpieczeństwem Informacji.
- ∞ Audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji.
- ∞ Jak wdrożyć System Zarządzania Bezpieczeństwem Informacji.
- ∞ Systemy zarządzania bezpieczeństwem informacji praktyczne warsztaty z normy 27001.
- ∞ Elementy RODO i bezpieczeństwa informacji w zarządzaniu zasobami ludzkimi.
- ∞ GDPR - Certified Information Privacy Manager.
- ∞ GDPR - Certified Information Privacy Professional/Europe (CIPP/EU).
- ∞ Polityka Bezpieczeństwa Informacji.
- ∞ Praktycznie o RODO - reforma ochrony danych osobowych w służbie zdrowia.
- ∞ Praktycznie o RODO/GDPR – unijna reforma ochrony danych osobowych.
- ∞ Wpływ RODO na działalność jednostki samorządu terytorialnego.

# Bezpieczeństwo

Szkolenia z zakresu bezpieczeństwa IT

Filtrowanie

Resetuj

SZUKAJ OFERTY

rodo

Odśwież

Nazwa ▾	Kod ↕	Cena od ↕
Analiza informacji	SECAI	1700 PLN
Elementy RODO i bezpieczeństwa informacji w zarządzaniu zasobami ludzkimi	SC-RD-01	1700 PLN
Identyfikacja i eskalacji incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego	SC-RD-06	3900 PLN
Inspektor Ochrony Danych - dwudniowy certyfikowany kurs z egzaminem	SC-RD-03	1500 PLN
Jak wdrożyć System Zarządzania Bezpieczeństwem Informacji?	SEC9	3100 PLN
Najnowsze rozwiązania antykorupcyjne - norma ISO 37001	SC-KO-02	1900 PLN
Ochrona danych osobowych - przygotowanie do wprowadzenia RODO	SC-RD-02	800 PLN
Optymalizacja kosztów firmy poprzez redukcję ryzyk osobowych, w tym ujawnianie oszustw kompetencyjnych	SC-KO-08	1900 PLN
Polityka Bezpieczeństwa Informacji	SEC8	1700 PLN
Praktycznie o RODO - reforma ochrony danych osobowych w służbie zdrowia	SC-RD-04	800 PLN
Praktycznie o RODO/GDPR - unijna reforma ochrony danych osobowych	SC-RD-05	800 PLN
Wpływ RODO na działalność jednostki samorządu terytorialnego	SC-RD-07	550 PLN
Zarządzanie ryzykiem w bezpieczeństwie informacji	SC-ZA-02	2700 PLN

# Szkolenia – Konkurs



**in** : Obserwuj nFlo

**@** : Marcin.Rek@nFlo.pl

**🔓** : „RODO pięć po 12-tej”



# Szkolenia – Konkurs

## **Ochrona danych osobowych po zmianie ustawy (1 dzień)**

<http://www.eitt.pl/oferta/ochrona-danych-osobowych-po-zmianie-ustawy-1048>

- Cena szkolenia: 900 zł netto
- Cena konkurs: 600 zł netto

## **Inspektor Ochrony Danych - kurs z egzaminem (2 dni)**

<http://www.eitt.pl/oferta/inspektor-ochrony-danych-dwudniowy-certyfikowany-kurs-z-egzaminem-19>

- Cena szkolenia: 1500 zł netto
- Cena konkurs: 995 zł netto

# Pion IT – Usługi wdrożeniowe i doradcze

- ∞ Wirtualizacji serwerów, pamięci masowych, sieci, desktopów
- ∞ Bezpieczeństwa infrastruktury sieciowej i aplikacyjnej
- ∞ Migracji baz danych, zmiany platform, optymalizacji konfiguracji
- ∞ Zarządzania rolami, uprawnieniami
- ∞ Monitoringu systemów, sieci oraz aplikacji
- ∞ Testowania nowych wersji aplikacji
- ∞ Automatyzacji procesów zarządzania infrastrukturą
- ∞ Zarządzania konfiguracją platform i aplikacji (MDM)
- ∞ Monitorowania, diagnostyki i wsparcia użytkowników
- ∞ Backupu danych z platform mobilnych
- ∞ Relokacji infrastruktury pomiędzy centrami danych

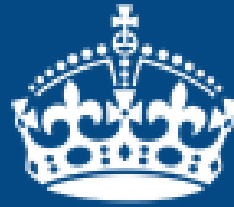
# Pion IT – obszary, produkty

- ∞ Zarządzanie Bezpieczeństwem IT
  - ∞ IT GRC – eSecure SecureVisio
  - ∞ NGFW, NGIPS, WAF, NAC, DLP, PAM, Antymalware, Sandbox, SIEM – Fortinet, IBM, Wheel Systems, Extreme Networks, eSecure
  - ∞ Database Access Monitor, Database Firewall – IBM Guardium
  - ∞ Kryptografia – UseCrypt, Billon
- ∞ Zabezpieczenie i zarządzanie danymi
  - ∞ Backup – IBM Spectrum Protect, Storware: KODO, FlyCoat, VProtect

# System klasy IT GRC

Automatyzacja zarządzania bezpieczeństwem organizacji w świetle RODO

SECURE  VISIO



**KEEP  
CALM  
AND  
COMPLY WITH  
GDPR**

Dziękuję za uwagę i zapraszam do współpracy.



Marcin Rek,  
Dyrektor ds. Rozwoju Biznesu  
nFlo Sp. z o.o.  
[Marcin.Rek@nFlo.pl](mailto:Marcin.Rek@nFlo.pl)  
+48 501 175 514