



Security Point

RODO

**Nie należy się go bać.
Należy stosować!**

Prelegent

Sławomir Grabik

Ekspert Bezpieczeństwa Informacji

Plan spotkania

- Dane osobowe – jak rozumieć ten termin?
- RODO i GIODO – co właściwie się zmienia?
- RODO – najważniejsze terminy i regulacje
- RODO? Czy to w ogóle dotyczy mojej firmy?
- 25 maja 2018 – i co dalej?
- Podsumowanie
- Czas na pytania

Plan spotkania

- **Dane osobowe – jak rozumieć ten termin?**
- RODO i GIODO – co właściwie się zmienia?
- RODO – najważniejsze terminy i regulacje
- RODO? Czy to w ogóle dotyczy mojej firmy?
- 25 maja 2018 – i co dalej?
- Podsumowanie
- Czas na pytania



Dane osobowe

oznaczają informacje o zidentyfikowanej
lub możliwej do zidentyfikowania
osobie fizycznej



Możliwa do zidentyfikowania osoba fizyczna

to osoba, którą można bezpośrednio
lub pośrednio zidentyfikować,
w szczególności na podstawie
identyfikatora



Dane osobowe – jak rozumieć ten termin?

Co może być identyfikatorem

Imię i nazwisko, numer identyfikacyjny
(PESEL, NIP), dane o lokalizacji,
identyfikator internetowy (login), itp..



Co może być identyfikatorem

Należy pamiętać, że identyfikatorem będzie także jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej



Plan spotkania

- Dane osobowe – jak rozumieć ten termin?
- **RODO i GIODO – co właściwie się zmienia?**
- RODO – najważniejsze terminy i regulacje
- RODO? Czy to w ogóle dotyczy mojej firmy?
- 25 maja 2018 – i co dalej?
- Podsumowanie
- Czas na pytania



25 maja 2018

- Konieczność prowadzenia dokumentacji przetwarzania danych osobowych
- Rozliczalność przetwarzania
- Prawo do przenoszenia danych osobowych
- Prawo do dostępu do danych osobowych
- Prawo do poprawiania / usunięcia danych osobowych
- „Privacy by design”





25 maja 2018

Art.

58

- Ostrzeżenie dla administratora

Art.

58

- Ograniczenie przetwarzania (czasowe / całkowite)

Art.

58

- Nakaz zawiadomienia osoby, której dane dotyczą

Art.

58

- Kara pieniężna do 10 mln EUR lub 2% rocznego obrotu

Art.

83

- Kara pieniężna do 20 mln EUR lub 4% rocznego obrotu

Art.

107

- Kara grzywny, kara ograniczenia lub pozbawienia wolności do lat 3

Art.

108

- Kara grzywny, kara ograniczenia lub pozbawienia wolności do lat 2



Plan spotkania

- Dane osobowe – jak rozumieć ten termin?
- RODO i GIODO – co właściwie się zmienia?
- **RODO – najważniejsze terminy i regulacje**
- RODO? Czy to w ogóle dotyczy mojej firmy?
- 25 maja 2018 – i co dalej?
- Podsumowanie
- Czas na pytania

25 maja 2018

Wejście w życie

04 maja 2016

Publikacja w
Dz. U. UE

27 kwietnia 2016

Przyjęcie
rozporządzenia

Czas na wdrożenie i stosowanie. Nie będzie ŻADNYCH dodatkowych terminów.



RODO – definicja

- **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/WE (ogólne rozporządzenie o ochronie danych)**





IODO - definicja

- **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/WE (ogólne rozporządzenie o ochronie danych)**



Plan spotkania

- Dane osobowe – jak rozumieć ten termin?
- RODO i GIODO – co właściwie się zmienia?
- RODO – najważniejsze terminy i regulacje
- **RODO? Czy to w ogóle dotyczy mojej firmy?**
- 25 maja 2018 – i co dalej?
- Podsumowanie
- Czas na pytania



RODO? Czy to w ogóle dotyczy mojej firmy?

- ✓ **Masz pacjentów – przetwarzasz i magazynujesz dane. Do tego są to dane drażliwe**
- ✓ **Zatrudniasz pracowników – przetwarzasz i magazynujesz dane osobowe**
- ✓ **Sprzedajesz przez internet – przetwarzasz i magazynujesz dane osobowe**
- ✓ **Masz klientów – przetwarzasz i magazynujesz dane osobowe**
- ✓ **Wielkość zbioru (ilości danych) nie ma tu znaczenia.**



RODO? Czy to w ogóle dotyczy mojej firmy?

**RODO muszą, co do zasady,
wprowadzić wszystkie
podmioty gromadzące
dane osobowe
z wyłączeniem osób fizycznych**



Security Point

Plan spotkania

- Dane osobowe – jak rozumieć ten termin?
- RODO i GIODO – co właściwie się zmienia?
- RODO – najważniejsze terminy i regulacje
- RODO? Czy to w ogóle dotyczy mojej firmy?
- **25 maja 2018 – i co dalej?**
- Podsumowanie
- Czas na pytania



25 maja 2018 – i co dalej?

Każda firma jest ZOBOWIĄZANA:

- Przeprowadzić wieloapsektową analizę obecnej sytuacji
- Wykonać ocenę ryzyk związanych z przetwarzaniem i magazynowaniem danych osobowych
- Wdrożyć adekwatne do potrzeb rozwiązania



Plan spotkania

- Dane osobowe – jak rozumieć ten termin?
- RODO i GIODO – co właściwie się zmienia?
- RODO – najważniejsze terminy i regulacje
- RODO? Czy to w ogóle dotyczy mojej firmy?
- 25 maja 2018 – i co dalej?
- **Podsumowanie**
- Czas na pytania

Pierwsze czynności jakie powinny zostać podjęte przez administratorów danych osobowych:

- ✓ rzetelna analiza aktualnego stanu ochrony danych osobowych w Spółce
- ✓ identyfikacja zakresów danych osobowych przetwarzanych przez Spółkę
- ✓ określenie sposobów pozyskiwania tych danych oraz ich rodzaje, ze szczególnym uwzględnieniem tego czy Spółka nie przetwarza danych szczególnych, dotychczas nazywanych danymi wrażliwymi.
- ✓ przegląd zawartych umów w szczególności tych których wykonanie wiąże się z przekazywaniem danych osobowych i weryfikacja podstaw prawnych dalszego ich przetwarzania
- ✓ aktualizacja umów powierzenia danych osobowych. Chodzi tutaj głównie o umowy outsourcingowe ale nie tylko. W praktyce ważnym problemem jest przekazywanie danych osobowych w ramach spółek danej grupy kapitałowej.
- ✓ przegląd posiadanych zgód na przetwarzanie danych jak i tego czy informacje, które zostały przekazane „podmiotom danych”, a więc mówiąc wprost „Kowalskim”, odpowiadają wymogom RODO

Podsumowanie

- ✓ skrupulatna ocena potencjalnych zagrożeń dla danych osobowych mogących wystąpić w działalności spółki jak również istniejących zabezpieczeń
- ✓ podjęcie decyzji co do rodzaju działań jakie należy wdrożyć, aby dochować wymogów należytej ochrony danych osobowych.

To, co zmienia się w podejściu do ochrony danych osobowych to najogólniej mówiąc- podejście do ochrony danych osobowych. Ochrona danych osobowych ma być trwałym procesem, weryfikowanym i aktualizowanym a nie wdrożeniem konkretnych dokumentów formalnych.

RODO nie określa zatem jakie konkretne dokumenty należy wdrożyć. Ciężar wyboru tego jakie działania będą adekwatne do możliwych zagrożeń dla ochrony danych osobowych RODO przenosi na administratorów danych Osobowych, a więc w przypadku Spółek na Zarząd.

A co w przypadku kontroli RODO?

Trzeba pamiętać, że w razie ewentualnej kontroli organu nadzorczego Spółka **będzie musiała** wykazać w jaki sposób chroni dane osobowe, ale również to, że podjęła niezbędne kroki celem „zdiagnozowania” potencjalnych zagrożeń oraz ich wyeliminowania.

25 maja już niebawem, co z tymi którzy dziś nie mają nic?

Wiele ze Spółek decyduje się obecnie na przeprowadzenie **audytów** zakończonych **pisemnym raportem** i dopiero w oparciu o taki raport podejmuje działania techniczne czy organizacyjne zmierzające do zwiększenia ochrony danych osobowych.

Plan spotkania

- Dane osobowe – jak rozumieć ten termin?
- RODO i GIODO – co właściwie się zmienia?
- RODO – najważniejsze terminy i regulacje
- RODO? Czy to w ogóle dotyczy mojej firmy?
- 25 maja 2018 – i co dalej?
- Podsumowanie
- **Czas na pytania**

Czas na pytania





Security Point

Security Point

ul. Królewska 67

05-827 Grodzisk Mazowiecki

Tel. +48 22 350 73 32

Mail: rodo@security-point.pl

www.security-point.pl