Grant Thornton

An instinct for growth™

Purpurowy Informator

Jak przygotować organizację do kontroli RODO?

Praktyczny poradnik: przebieg kontroli,
plan kontroli na 2019 rok,
pierwsze kary w Polsce i Europie

Czerwiec 2019

Purpurowy Informator – źródło informacji

Z przyjemnością prezentujemy kolejną edycję „Purpurowego Informatora", czyli cyklu analiz, w którym omawiamy ważne dla przedsiębiorców kwestie prawne, księgowe i kadrowe. Tym razem tematem naszego cyklu jest RODO, a konkretnie to, czego można spodziewać się podczas kontroli Urzędu Ochrony Danych Osobowych i jak się do niej przygotować.

Szanowni Państwo,

25 maja 2019 r. minął rok, odkąd weszły w życie nowe, unijne przepisy dotyczące ochrony danych osobowych i przez polską gospodarkę przetoczyła się wielka „operacja RODO", w ramach której wszystkie przedsiębiorstwa w Polsce musiały dostosować się do nowych przepisów. Regulacje te zmuszały firmy do żmudnej pracy nad procesami i bazami danych oraz nakładały wysokie kary za ewentualne uchybienia.

Teraz, gdy prawdopodobnie zdecydowana większość firm w lepszy czy gorszy sposób wdrożyła już procedury RODO, przedsiębiorcy zaczynają zastanawiać się, na ile są bezpieczni, gdy do drzwi zapuka kontrola.

Właśnie dlatego oddajemy w Państwa ręce Purpurowy Informator, który ma zwrócić Państwa uwagę na zagadnienia związane z urzędowymi kontrolami sprawdzającymi poprawność przetwarzania danych osobowych w organizacji. Przybliżamy przebieg kontroli, kryteria ustalania wysokości kar administracyjnych, a także opisujemy część tych, które zostały już nałożone po wejściu w życie RODO.

W opracowaniu ujęte zostały także wskazówki, jak poprawnie przygotować się do kontroli oraz wymienione są sektory, w obrębie których kontrole obecnie się toczą lub będą toczyły się do końca roku 2019.

Zapraszamy do lektury raportu.

Jolanta Jackowiak
Partner
Konsulting, RODO
Departament Doradztwa
Grant Thornton

Pierwsze kary w Polsce i Europie

Polska

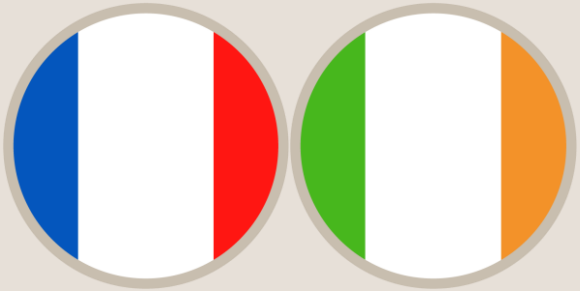
- WYSOKOŚĆ KARY: **ok. 200 tys. EUR**
- Kara dla jednej z największych wywiadowni gospodarczych
- Dane pochodziły z ogólnodostępnych rejestrów, przedsiębiorcy podają je samodzielnie
- Niedopełnienie obowiązku spełnienia prawa do informacji osób, których dane zostały pozyskane z innego źródła

Niemcy

- WYSOKOŚĆ KARY: **20 tys. EUR**
- Kara po ataku hackerskim na sieć społecznościową
- Brak mechanizmów szyfrowania haseł użytkowników
- Wzorcowe działania ze strony administratora: kontakt z organem nadzorczym oraz zwiększenie bezpieczeństwa danych po ataku

Pierwsze kary w Polsce i Europie

Francja/Irlandia



- WYSOKOŚĆ KARY: **50 mln EUR**
- Ukarany: Google
- Najwyższa kara dotycząca RODO
- Postępowanie wszczęto po otrzymaniu skarg
- Informacje o przetwarzaniu danych nie były użytkownikom przedstawione przejrzyście
- Osoby wyrażające zgody nie były wcześniej odpowiednio poinformowane
- Naruszenie nie miało charakteru jednorazowego

Austria

- WYSOKOŚĆ KARY: **Blisko 5 tys. EUR**
- Kara dla podmiotu prywatnego
- Kara nałożona proporcjonalnie do dochodów firmy
- Kara za nieprawidłowy monitoring wizyjny w firmie (obejmował zbyt szeroki zakres chodnika)
- Przechodnie nie byli świadomi przetwarzania w tym miejscu ich wizerunku

Portugalia

- WYSOKOŚĆ KARY: **400 tys. EUR**
- Nieprawidłowości dotyczyły dostępu do systemu zarządzania danymi medycznymi pacjentów
- Nie zapewniono też trwałego usunięcia kont lekarzy, którzy zakończyli pracę
- Błędnie przyznany poziom dostępów – dostęp do danych pacjentów poprzez konta techniczne
- Na wysokość kary wpłynęła niska świadomość administratora danych podczas zarządzania systemami informatycznymi

Przebieg kontroli

Najważniejsze fakty oraz przebieg kontroli krok po kroku

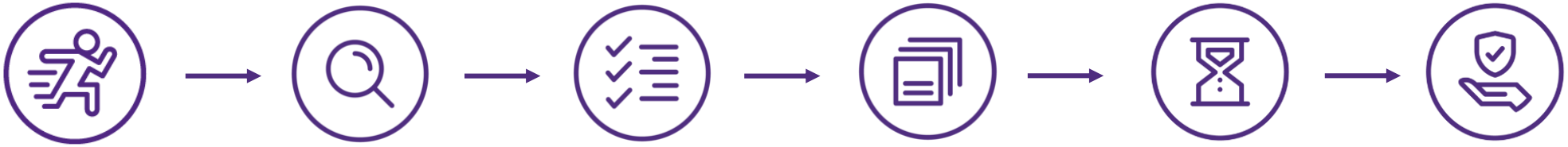
Postepowanie kontrolne trwa nie dłużej niż miesiąc

Kontrolujący ma prawo wstępu na teren i do budynków w godzinach od 6:00 do 22:00

Przed kontrolą kontrolujący okazuje imienne upoważnienie oraz legitymację służbową

Przepisy podlegające kontroli:
- Ustawa o ochronie danych osobowych
- Przepisy sektorowe i wykonawcze
- Przepisy Rozporządzenia – RODO

PRZEBIEG KONTROLI



„Jaka cena tego naruszenia?”

Czyli dążenie państw UE do ujednolicenia skali

Wykroczenia dotyczące przepisów, za które Urząd Ochrony Danych Osobowych ma prawo nałożyć administracyjną karę pieniężną w wysokości do 20 mln EUR, bądź w przypadku przedsiębiorstw – do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, zostały podzielone na 4 kategorie:

KATEGORIA I	Wysokość możliwej grzywny 0 – 200 tys. EUR	Grzywna podstawowa: 100 tys. EUR
KATEGORIA II	Wysokość możliwej grzywny 120 tys. EUR – 500 tys. EUR	Grzywna podstawowa: 310 tys. EUR
KATEGORIA III	Wysokość możliwej grzywny 300 tys. EUR – 750 tys. EUR	Grzywna podstawowa: 525 tys. EUR
KATEGORIA IV	Wysokość możliwej grzywny 450 tys. EUR – 1 mln EUR	Grzywna podstawowa: 725 tys. EUR

Wysokości stawek to **wartości sugerowane**. W uzasadnionych okolicznościach grzywna może przekroczyć wskazane kwoty.

Przytoczony **„taryfikator”** został wydany przez holenderski organ nadzorczy

Przykłady klasyfikacji naruszeń

ARTYKUŁ RODO	OPIS	KATEGORIA
Art. 6	Zgodność z prawem każdego przetwarzania danych	III
Art. 9	Przetwarzanie szczególnych kategorii danych	IV
Art. 13	Informacje podawane w przypadku zbierania danych osobowych od osoby, której dane dotyczą	III
Art. 15	Prawo dostępu przysługujące osobie, której dane dotyczą	III
Art. 22	Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach (w tym profilowanie)	IV
Art. 45	Przekazywanie na podstawie decyzji stwierdzającej odpowiedni poziom ochrony	III

Wysokość kary powinna być proporcjonalna i odstraszająca dla sprawcy i potencjalnych sprawców.

Każdy organ nadzorczy nakładając karę pieniężną winien wziąć pod uwagę m.in.:

- charakter, powagę i czas trwania naruszenia,
- środki podjęte w celu ograniczenia szkód,
- wcześniejsze istotne, popełnione naruszenia,
- stopień współpracy z organem nadzorczym,
- kategorie osób, których dotyczy naruszenie,
- sposób, w jaki organ nadzorczy podjął informację o naruszeniu.

Plan kontroli sektorowych na rok 2019

Kto może spodziewać się kontroli?

Plan kontroli sektorowych zatwierdzany jest przez Prezesa Urzędu Ochrony Danych Osobowych. W roku 2019 pod lupą UODO znajdą się m.in. takie obszary jak telemarketing, monitoring wizyjny czy profilowanie w sektorze bankowym i ubezpieczeniowym.

Kontrole **są wynikiem licznych skarg, pytań oraz zgłoszeń naruszeń ochrony danych osobowych.**

Kontrole są także kontynuacją planu sektorowego z 2018 roku.

1. Monitoring miejski
2. Udostępnianie danych w Biuletynie Informacji Publicznej
3. Sposób prowadzenie rejestru czynności przetwarzania i dokumentowania naruszeń
4. System identyfikacji i monitoringu odpadów
5. Spółdzielnie mieszkaniowe – prowadzenie rejestru członków

1. Telemarketing
2. Brokerzy danych w zakresie zakresie podstaw prawnych przetwarzania danych osobowych
3. Profilowanie w sektorze bankowym i ubezpieczeniowym.

1. Policja
2. Straż Graniczna
3. Areszty śledcze
4. Systemy SIS/VIS – kontrolą objęte będą podmioty uprawnione do dostępu do systemów SIS/VIS

1. Szkoły i placówki oświatowe – monitoring wizyjny
2. Pracodawcy – moniotring wizyjny, rekrutacja
3. Podmioty udzielające świadczeń zdrowotnych – udostępnianie dokumentacji medycznej w ramach realizacji praw pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych.

Jak przygotować organizację do kontroli,
czyli co zrobić aby nie dać się zaskoczyć kontrolerom z Urzędu?

Kontrole z UODO **NIE MUSZĄ** być zapowiedziane.

Często natomiast organizacja jest informowana o planie jej przeprowadzenia na **7 dni wcześniej**.

Jest to **czas wystarczający** aby stworzyć **plan działania** i odpowiednio przygotować się do jej przejścia.

KLUCZOWE DZIAŁANIA, KTÓRE NALEŻY PODJĄĆ:

1. Zapewnienie obecność podczas kontroli Inspektora Ochrony Danych lub osoby odpowiedzialnej za obszar ochrony danych osobowych w organizacji

2. Przygotowanie wszystkich dokumentów mających bezpośredni związek z przedmiotowym zakresem kontroli

3. Dokonanie wewnętrznego audytu miejsc przetwarzania danych osobowych oraz nośników i systemów teleinformatycznych

4. Zapewnienie podczas kontroli obecności osób posiadających najpełniejszą wiedzę z zakresu procesów przetwarzania

5. Poinformować o kontroli pracowników i w razie konieczności ponownie przeszkolić ich z zakresu ochrony danych osobowych w organizacji

Zapraszamy do kontaktu

Potrzebujesz wsparcia?
Jesteśmy do dyspozycji

Jolanta Jackowiak
Partner
Konsulting, RODO
Departament Doradztwa
T+48 601 934 173
E Jolanta.Jackowiak@pl.gt.com

Grant Thornton to jedna z wiodących organizacji audytorsko-doradczych na świecie. Wiedza, doświadczenie i zaangażowanie ponad 3000 partnerów oraz 50 000 pracowników Grant Thornton dostępne są dla klientów w 136 krajach. W Polsce działamy od 26 lat, a ponad 550-osobowy zespół oraz obecność w kluczowych aglomeracjach (Warszawa, Poznań, Katowice, Wrocław, Kraków i Toruń) pozwala nam wspierać w rozwoju ponad 1600 firm i organizacji rocznie.