KOMPAS FORSAFE 2020

Kary organów nadzorczych w Unii Europejskiej

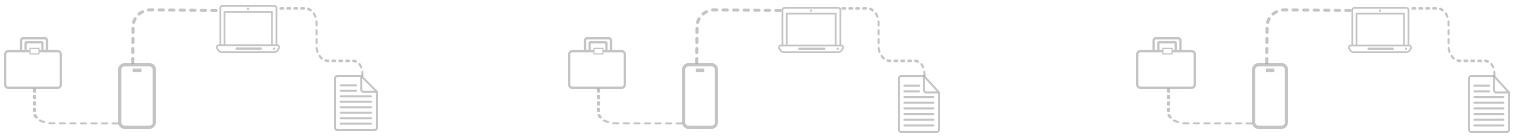
Kary i decyzje Urzędu Ochrony Danych Osobowych

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

KOMPAS FORSAFE to specjalnie stworzony dla Was cykl informacyjny, którego celem jest przybliżenie wydawanych decyzji i nakładanych kar przez organy nadzorcze w krajach Unii Europejskiej oraz w Polsce – przez Prezesa Urzędu Ochrony Danych Osobowych, w przypadku naruszeń prawa o ochronie danych osobowych.

Co znajdziecie w naszym cyklu?

- Przegląd najważniejszych kar i decyzji wydanych przez organy nadzorcze w Polsce oraz w krajach Unii Europejskiej
- Opis incydentów bezpieczeństwa, na skutek których doszło do naruszenia przepisów o ochronie danych osobowych
- Uzasadnienie decyzji organów nadzorczych
- Rekomendacje ekspertów FORSAFE, dzięki którym na pewno unikniecie naruszeń oraz potencjalnych kar



PRZYPOMINAMY!

Administrator danych, który naruszył RODO, podlega odpowiedzialności prawnoadministracyjnej:

- Decyzje Prezesa UODO mogą obejmować kary pieniężne:
  do **20 mln euro** lub **4% rocznego obrotu za najpoważniejsze naruszenia**, m.in. zasad przetwarzania danych, praw osób, których dane dotyczą, lub niestosowanie się do nakazów organu nadzorczego, a **za pozostałe naruszenia – do 10 mln euro lub 2% rocznego obrotu,** w zależności od tego, która kwota jest wyższa.
- a także różnego rodzaju nakazy mające na celu zapewnienie zgodności z RODO,

oraz cywilnej :

- osoba, której dane dotyczą, ma prawo do odszkodowania za szkodę majątkową lub niemajątkową wynikającą z naruszenia RODO.

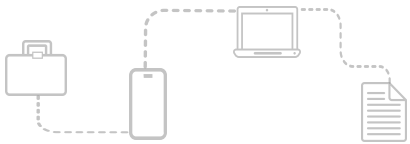
Ponadto każda osoba, która nielegalnie przetwarza dane osobowe lub udaremnia przeprowadzenie kontroli przestrzegania przepisów o ochronie danych, podlega odpowiedzialności karnej, przewidzianej ustawą o ochronie danych osobowych.

Czy wiecie, że?

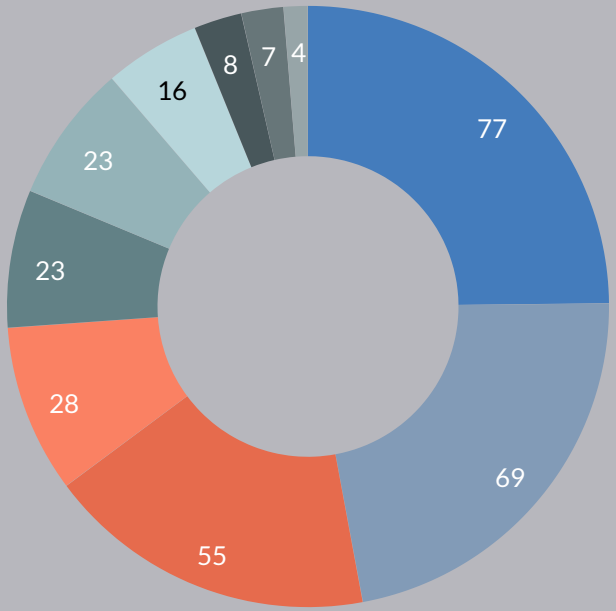
310 To łączna ilość kar nałożonych w Unii Europejskiej w 2020 roku - z tego najwięcej w HISZPANII (132 kar)

35 258 708€ to najwyższa nałożona kara w 2020 roku na H&M w Niemczech

28€ to najniższa kara w UE nałożona przez węgierski organ nadzorczy na Google



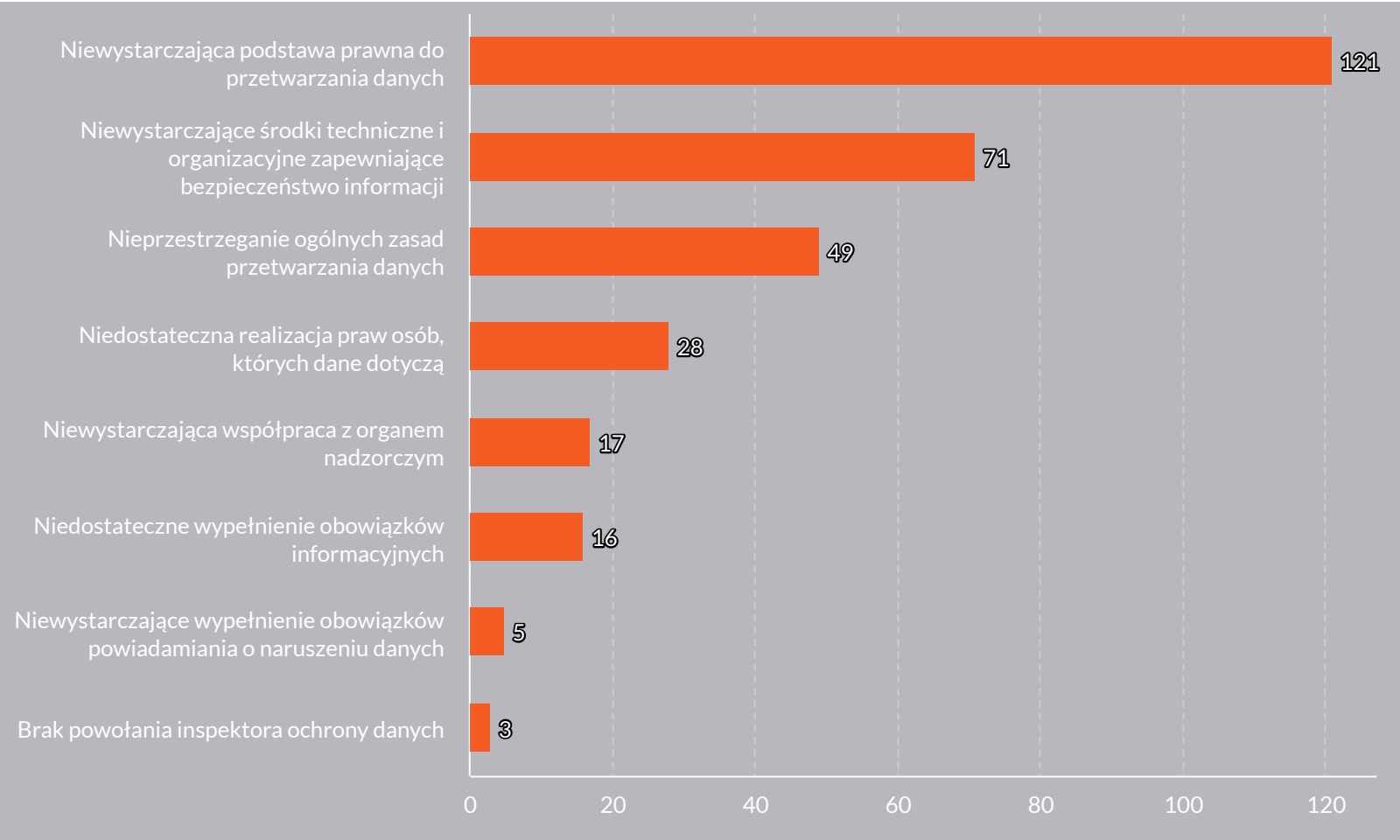
Kary w Unii Europejskiej według branż w 2020 roku



- Przemysł i handel (24.84%)
- Media, telekomunikacja, radiofonia i telewizja (22.26%)
- Sektor publiczny i edukacja (17.74%)
- Finanse, ubezpieczenia i doradztwo (9.03%)
- Osoby prywatne i stowarzyszenia prywatne (7.42%)
- Służba zdrowia (7.42%)
- Transport i energia (5.16%)
- Hotelarstwo (2.58%)
- Inne (2.26%)
- Pracodawcy (1.29%)

W krajach Unii Europejskiej branża przemysłowo-handlowa oraz branże telekomunikacyjne i marketingowe w największym stopniu są narażone na naruszenia, a co za tym idzie - na kary ze strony organów nadzorczych.

Kary w Unii Europejskiej według rodzaju naruszenia



Kary w poszczególnych krajach Unii Europejskiej

	Najwyższa kara	Najniższa kara
NIEMCY	35 258 708 €	900 000 €
WŁOCHY	27 800 000 €	1 000 €
UK	22 046 000 €	1 405 000 €
SZWECJA	5 000 000 €	11 200 €
FRANCJA	2 250 000 €	3 000 €
HOLANDIA	830 000 €	525 000 €
BELGIA	600 000 €	1 000 €
IRLANDIA	450 000 €	40 000 €
POLSKA	443 000 €	1 168 €
WĘGRY	288 000 €	28 €
NORWEGIA	276 000 €	13 900 €
DANIA	147 800 €	6 700 €
FINLANDIA	100 000 €	7 000 €

Kary w poszczególnych krajach Unii Europejskiej

	Najwyższa kara	Najniższa kara
HISZPANIA	80 000 €	540 €
ISLANDIA	20 600 €	9 000 €
RUMUNIA	15 000 €	500 €
LITWA	15 000 €	15 000 €
ŁOTWA	15 000 €	6 250 €
GRECJA	15 000 €	1 000 €
CYPR	15 000 €	1 000 €
WYSPA MAN	13 500 €	13 500 €
BUŁGARIA	5 110 €	2 000 €
AUSTRIA	600 €	100 €
ESTONIA	500 €	48 €
PORTUGALIA, MALTA, CZECHY	0 €	0 €

W naszym cyklu Kompas FORSAFE zawarliśmy w tym roku przegląd najciekawszych przypadków kar nakładanych przez organy nadzorcze w krajach Unii Europejskiej na przestrzeni ostatnich lat.

W drugiej części tego opracowania znajdziecie omówione przez nas dotychczas kary i decyzje organów nadzorczych Unii Europejskiej oraz Prezesa Urzędu Ochrony Danych Osobowych.

Na kogo i dlaczego zostały nałożone kary?

Jakie było uzasadnienie decyzji?

Co rekomendujemy?

Kary organów nadzorczych w Unii Europejskiej

1. Kara dla Google Inc. (21.01.2019)
2. Kara dla Österreichische Post (23.10.2019)
3. Kara dla Deutsche Wohnen SE (30.10.2019)
4. Kara dla Eni Gas e Luce (11.12.2019)
5. Kara dla Telecom Italia Mobile (15.01.2020)
6. Kara dla Wind Tre S.p.A (09.07.2020)
7. Kara dla Hennes & Mauritz Online Shop A.B. & Co. KG (01.10.2020)
8. Kara dla British Airways (16.10.2020)
9. Kara dla Marriott International Inc. (30.10.2020)
10. Kara dla Vodafone Italia S.p.A. (12.11.2020)

11 KARA DLA GOOGLE INC.

KOMPAS FORSAFE

Kraj oraz organ nadzorczy **Francja**
French Data Protection Authority (CNIL)

Data wydania decyzji **21.01.2019 r.**

Podmiot kontrolowany **Google Inc.**

Wysokość kary **50 000 000 EUR**

Rodzaj naruszenia

Naruszenie Art. 5, Art. 6, Art. 13, Art. 14 RODO.
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

W maju 2018 r. do CNIL wpłynęły skargi od austriackiej organizacji „None Of Your Business" oraz francuskiej organizacji pozarządowej „La Quadrature du Net". 10 000 osób upoważniło powyższe organizacje do skierowania sprawy do CNIL, której przedmiotem były zarzuty wobec firmy GOOGLE w zakresie braku ważnej podstawy prawnej do przetwarzania danych osobowych użytkowników tej Spółki a w szczególności w celu personalizowania reklam. We wrześniu 2018 r. dokonano kontroli dokumentów, do których użytkownik może mieć dostęp podczas tworzenia konta GOOGLE w trakcie konfiguracji urządzenia mobilnego z systemem Android. W rezultacie CNIL uznał, iż GOOGLE LLC dopuściło się naruszenia polegającego na braku przejrzystości, nieadekwatnych informacjach i braku ważnej zgody na spersonalizowane reklamy.

Kompas FORSAFE

BY UNIKNĄĆ TAKIEGO NARUSZENIA ZALECAMY:

1) Pozyskiwanie zgody użytkownika na przetwarzanie danych wcelu personalizacji reklam.

2) Sformułowanie zgody na przetwarzanie danych w celupersonalizacji reklam w sposób jednoznaczny, tzn. użytkownik musi być świadomy na co i w jakim zakresie wyraża zgodę.

3) Sformułowanie zgody na przetwarzanie danych w sposób konkretny, tzn. użytkownik musi być świadomy w jakim celu wyraża zgodę.

Kraj oraz organ nadzorczy

Austria

Austrian Data Protection Authority (dsb)

Data wydania decyzji

23.10.2019 r.

Podmiot kontrolowany

Österreichische Post

Wysokość kary

18 000 000 EUR

Rodzaj naruszenia

Art. 5 (1) a), Art. 6 RODO
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

Austriacka poczta dopuściła się bezprawnego przetwarzania danych osobowych ok. 3 milionów swoich klientów, zbierając m.in. następujące informacje: imię i nazwisko, adres zamieszkania, wiek, płeć, preferencje polityczne, częstotliwość otrzymywania paczek, częstotliwość relokacji.
Na podstawie posiadanych informacji austriacka poczta dokonywała profilowania klientów oraz sprzedawała ich dane partiom politycznym oraz firmom, by te mogły wysyłać ukierunkowane reklamy wyborcze. Klienci austriackiej poczty nie byli świadomi tego procederu.

Kompas FORSAFE

WYSTRZEGAJ SIĘ TAKICH NARUSZEŃ!

1) Monitoruj, weryfikuj i kontroluj zakres przetwarzania danych osobowych w aspekcie jego legalności.

2) Weryfikuj bazy marketingowe w zakresie posiadania zgody na działania marketingowe oraz realizuj je wyłącznie wobec osób, które wyraziły na to zgodę.

3) Sprzedawaj bazy marketingowe jedynie w przypadku, w którym została odnotowana zgoda na realizowanie działań marketingowych przez podmioty zewnętrzne nabywające bazę.

Kraj oraz organ nadzorczy

Niemcy

Data Protection Authority of Berlin

Data wydania decyzji

30.10.2019 r.

Podmiot kontrolowany

Deutsche Wohnen SE

Wysokość kary

14 500 000 EUR

Rodzaj naruszenia

Naruszenie Art. 5 i Art. 25 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

W czerwcu 2017 r. pracownicy niemieckiego organu nadzorczego przeprowadzili czynności kontrolne w Deutsche Wohnen SE. W wyniku kontroli odnotowano, iż Spółka wykorzystuje system do archiwizacji danych osobowych najemców, nieprzewidujący możliwości usunięcia danych, które nie są już potrzebne. Spółka przechowywała dane osobowe najemców pomimo ustania pierwotnego celu ich przetwarzania, takie jak: zestawienia wynagrodzeń, formularze do ujawnienia informacji, wyciągi z umów o pracę szkolenia, dane podatkowe, dane dotyczące ubezpieczenia społecznego i zdrowotnego oraz wyciągi bankowe. Kolejna kontrola przeprowadzona w marcu 2019 r. potwierdziła stan zastany w czerwcu 2017 r. Stwierdzono, że Spółka nie wykonała zaleceń pokontrolnych i nie usunęła nieprawidłowości z systemu archiwizacyjnego. Poza nałożeniem sankcji za to strukturalne naruszenie, Berliński Rzecznik ds. Ochrony Danych nałożył jeszcze na przedsiębiorstwo dalsze kary pieniężne w wysokości pomiędzy 6 000, a 17 000 Euro za niezgodne z prawem przechowywanie danych osobowych najemców w 15 konkretnych przypadkach.

Kompas FORSAFE

JAK ZAPOBIEGAĆ TAKIM NARUSZENIOM?

1) Wprowadź procedurę retencji danych oraz regularnie weryfikuj czas przetwarzania danych osobowych.

2) Sprawdzaj dane zawarte w systemie archiwizacyjnym oraz archiwum papierowym w celu nadzoru nad terminem usunięcia danych osobowych ze względu na ustanie celu przetwarzania danych osobowych.

Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)

Data wydania decyzji

11.12.2019 r.

Podmiot kontrolowany

Eni Gas e Luce

Wysokość kary

8 500 000 EUR

Rodzaj naruszenia

Naruszenie Art. 5, Art. 6, Art. 17 i Art. 21 RODO.
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

Włoski Urząd Ochrony Danych otrzymał liczne skargi i zgłoszenia na Eni Gas e Luce S.p.A., które odnosiły się do niezgodnego z prawem przetwarzania danych osobowych w celach telemarketingowych, polegających m.in. na realizacji rozmów promocyjnych bez zgody osoby, z którą się kontaktowano, lub pomimo jej odmowy odbierania rozmów promocyjnych oraz na prowadzeniu rozmów promocyjnych z osobami zarejestrowanymi w publicznym rejestrze sprzeciwów. W toku czynności kontrolnych ujawniono dodatkowo kilka naruszeń prawa o ochronie danych, w tym:
a) brak wdrożenia środków technicznych i organizacyjnych w celu uwzględnienia dostarczonych przez użytkowników informacji dotyczących zgody lub jej braku na wykorzystanie danych osobowych tych osób;
b) przechowywanie danych osobowych zawartych w umowach przez okres dłuższy, niż jest to związane z realizacją celów, w których były przetwarzane;
c) przetwarzanie danych o potencjalnych klientach, które zostały zebrane od podmiotów, nieposiadających zgody na udostępnienie takich danych do podmiotów trzecich.

Kompas FORSAFE

JAK ZAPOBIEGAĆ TAKIM NARUSZENIOM?

1) Weryfikuj bazy marketingowe w zakresie posiadania udokumentowanej zgody na działania marketingowe oraz realizuj działania marketingowe wyłącznie wobec osób, które wyraziły na to zgodę.

2) Wprowadź procedury określające zasady pracy na danych osobowych przez podmioty zewnętrzne działające w imieniu Spółki.

3) Zapewnij kontrolę nad działaniami marketingowymi realizowanymi przez podmioty zewnętrzne w imieniu Spółki.

4) Wdróż procedury zarządzania listami rezygnacji z otrzymywania kampanii marketingowych (tzw. „czarna lista") oraz weryfikuj je cyklicznie.

5) Wymieniaj informacje z podmiotami realizującymi działania marketingowe w zakresie list rezygnacji z otrzymywania kampanii marketingowych (tzw. „czarna lista").

6) Wprowadź procedury retencji danych oraz regularnie weryfikuj czas przetwarzania danych osobowych.

7) Kupuj bazy danych osobowych jedynie od rzetelnego dostawcy, który zagwarantuje legalność pozyskania zgód na działania marketingowe, a także możliwość dalszej ich sprzedaży podmiotom trzecim.

Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)

Data wydania decyzji

15.01.2020 r.

Podmiot kontrolowany

Telecom Italia Mobile

Wysokość kary

27 800 000 EUR

Rodzaj naruszenia

Art. 5, Art. 6, Art. 17, Art. 21, Art. 32 RODO
Niewystarczająca podstawa prawna do przetwarzania danych

Przedmiot decyzji

Od stycznia 2017 r. do początku 2019 r. włoski Urząd Ochrony Danych otrzymał setki zgłoszeń i skarg na TIM, które odnosiły się do otrzymywania niezamówionej informacji handlowej bez zgody osób, których dane dotyczą oraz pomimo rejestracji ich numerów telefonów w publicznym rejestrze sprzeciwów i pomimo skorzystania przez nich, z prawa do bycia zapomnianym. Inne zastrzeżenia to: brak odpowiedzi na żądania zgłaszane przez osoby, których dane dotyczą w zakresie praw wynikających z przepisów o ochronie danych osobowych, w szczególności prawa dostępu do ich danych oraz sprzeciwu wobec przetwarzania w celach promocyjnych; nieprawidłowe przetwarzanie danych w związku z realizacją konkursów; błędnie sformułowany obowiązek informacyjny oraz błędnie skonstruowana zgoda przy dostarczonych przez Spółkę aplikacjach; pobieranie na formularzach papierowych jednej zgody, która była wykorzystywana w różnych celach w tym marketingowych; przechowywanie danych dłużej, niż było to konieczne.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Weryfikuj bazy marketingowe w zakresie posiadania zgody na działania marketingowe oraz realizuj działania marketingowych jedynie wobec osób, które wyraziły na to zgodę.

2) Zapewnij kontrolę nad działaniami marketingowymi realizowanymi przez podmioty zewnętrzne w imieniu Spółki.

3) Wprowadź procedury zarządzania listami rezygnacji z kampanii marketingowych (tzw. „czarna lista") oraz ich cykliczną weryfikację.

4) Wdróż środki techniczne i organizacyjne dotyczące obsługi wniosków o skorzystanie z praw podmiotów danych.

5) Zapewnij wymianę informacji z podmiotami realizującymi działania marketingowe w zakresie list rezygnacji z kampanii marketingowych (tzw. „czarna lista") oraz obsługi wniosków o skorzystanie z praw podmiotów danych.

6) Wprowadź procedury retencji danych oraz regularnie weryfikuj czas przetwarzania danych osobowych.

7) Weryfikuj zgody na przetwarzanie danych osobowych pod kątem celu przetwarzania (jeden cel przetwarzania = jedna zgoda) oraz dobrowolności wyrażenia zgody.

8) Realizuj obowiązek informacyjny w sposób przejrzysty.

21 KARA DLA HENNES & MAURITZ

KOMPAS FORSAFE

Kraj oraz organ nadzorczy

Niemcy

Data Protection Authority of Hamburg

Data wydania decyzji

01.10.2020 r.

Podmiot kontrolowany

H&M Hennes & Mauritz Online Shop A.B. & Co. KG

Wysokość kary

35 258 708 EUR

Rodzaj naruszenia

Naruszenie Art. 5, 6, RODO.
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

Firma H&M prowadząca centrum usługowe w Norymberdze od 2014 r. monitorowała kilkuset swoich pracowników. Kierownicy podczas rozmów zbierali informacje o wakacjach, nieobecnościach chorobowych, objawach chorobowych, diagnozach, życiu prywatnym, problemach rodzinnych, czy przekonaniach religijnych. Na podstawie rozmów tworzone były notatki, które były przechowywane na dysku sieciowym. Do zapisanych informacji miało dostęp ok. 50 innych menadżerów w całej firmie. Pozyskane dane były wykorzystywane między innymi do oceny wydajności pracy pracowników oraz podejmowania decyzji o zatrudnieniu. W październiku 2019 r. doszło do błędu w konfiguracji dysku sieciowego a zgromadzone na nim dane przez kilka godzin stały się dostępne dla wszystkich pracowników. Urząd Ochrony Danych w Hamburgu dowiedział się o tym fakcie z doniesień prasowych i wszczął w firmie kontrolę, która potwierdziła stosowane praktyki.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Nie naruszaj prawa do prywatności pracowników.

2) Pozyskuj o pracownikach jedynie takie informacje, jakie są wymagane przez przepisy prawa.

3) Zanim zaczniesz zbierać o pracownikach dane wykraczające poza zakres wskazany w przepisach danych – skonsultuj się z Inspektorem Ochrony Danych lub osobą odpowiedzialną za ochronę danych osobowych w firmie.

23 KARA DLA BRITISH AIRWAYS

KOMPAS FORSAFE

Kraj oraz organ nadzorczy — **Wielka Brytania**
Information Commissioner (ICO)

Data wydania decyzji — **16.10.2020 r.**

Podmiot kontrolowany — **British Airways**

Wysokość kary — **22 046 000 GBP***

*16.10.2020 r. ICO zmniejszyło pierwotny wymiar kary ze 183 390 000 GBP m.in. ze względu na wpływ pandemii COVID-19 („koronawirusa") na branżę lotniczą.

Rodzaj naruszenia

Naruszenie Art. 32 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

We wrześniu 2018 roku British Airways zgłosiło do Information Commissioner (ICO) naruszenie dotyczące częściowego przekierowania ruchu użytkowników na fałszywą stronę internetową British Airways. Za pośrednictwem fałszywej witryny pozyskiwane były dane klientów. Naruszenie dotyczyło łącznie około 500 000 osób.

Kompas FORSAFE

Klienci British Airways padli ofiarą metody wyłudzania danych określonej jako pharming. Jest to rodzaj oszustwa przypominający phishing, ale w tym przypadku odwiedzający prawdziwą stronę linii lotniczych byli przekierowani na podszywające się pod nią strony, które instalowały na ich urządzeniach złośliwe oprogramowanie lub zbierały dane osobowe.

BY UNIKNĄĆ TAKIEGO NARUSZENIA ZALECAMY:

1) Sprawdzanie adresów URL stron www. Upewnijcie się, że przed adresem strony jest skrót **„https”**. Litera „s” oznacza, że jest to połączenie zabezpieczone, oraz że strona jest bezpieczna.

2) Korzystanie z usług wiarygodnego dostawcy Internetu i zachowanie ostrożności wobec odwiedzanych stron.

3) Korzystanie z programu antywirusowego, który będzie monitorował, czy strony są godne zaufania.

DODATKOWE REKOMENDACJE ICO:

1) Ograniczenie dostępu do aplikacji, danych i narzędzi tylko do tych, które są wymagane do pełnienia roli użytkownika.

2) Przeprowadzenie rygorystycznych testów w formie symulacjicyberataku na systemy przedsiębiorstwa.

3) Ochrona kont pracowników i osób trzecich za pomocą uwierzytelniania wieloskładnikowego.

25 KARA DLA WIND TRE

KOMPAS FORSAFE

Kraj oraz organ nadzorczy **Włochy**
Italian Data Protection Authority (Garante)

Data wydania decyzji **13.07.2020 r.**

Podmiot kontrolowany **Wind Tre S.p.A**

Wysokość kary **16 700 000 EUR**

Rodzaj naruszenia

Art. 5, Art. 6, Art. 12, Art. 24, Art. 25 RODO.
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

Włoski Urząd Ochrony Danych otrzymał liczne skargi na firmę Wind Tre S.p.A., które odnosiły się do m.in.: do otrzymywania niezamówionych wiadomości wysłanych bez uprzedniej zgody podmiotu danych za pośrednictwem wiadomości SMS, e-mail, rozmów telefonicznych i połączeń automatycznych. Klienci skarżyli się na brak możliwości skorzystania z prawa do cofnięcia zgody oraz sprzeciwienia się wobec przetwarzania danych w celach marketingu bezpośredniego, ponieważ informacje odnoszące się do danych kontaktowych zawartych w Polityce ochrony danych na stronie internetowej były niekompletne. Skargi dotyczyły również publikowania danych osobowych na publicznych listach telefonicznych pomimo sprzeciwu podmiotów danych, oraz wyrażania zgód na różne czynności przetwarzania podczas instalowania i konfigurowania aplikacji.

Kompas FORSAFE

JAK ZAPOBIEGAĆ TAKIM NARUSZENIOM?

1) Weryfikuj bazy marketingowe w zakresie posiadania udokumentowanej zgody na działania marketingowe oraz realizuj działania marketingowe jedynie wobec osób, które wyraziły na to zgodę.

2) Weryfikuj zgody na przetwarzanie danych osobowych pod kątem dobrowolności ich wyrażenia.

3) Zapewnij kontrolę nad działaniami marketingowymi realizowanymi przez podmioty zewnętrzne w imieniu Spółki.

4) Wprowadź procedury realizacji praw podmiotów danych.

5) Wdróż środki techniczne i organizacyjne dotyczące obsługi wniosków o skorzystanie z praw podmiotów danych.

6) Sprawdź politykę ochrony danych osobowych zamieszczoną na stronie internetowej pod kątem aktualności danych kontaktowych.

7) Zapewnij kontrolę łańcucha dostawców usług w zakresie ochrony danych osobowych.

27 KARA DLA MARRIOTT INTERNATIONAL INC.

KOMPAS FORSAFE

Kraj oraz organ nadzorczy

Wielka Brytania

Information Commissioner (ICO)

Data wydania decyzji

30.10.2020 r.

Podmiot kontrolowany

Marriott International Inc.

Wysokość kary

18 400 000 GBP*

*ICO podkreśliło, że ustalając wysokość grzywny wzięło również pod uwagę gospodarczy wpływ pandemii.

Rodzaj naruszenia

Naruszenie Art. 32 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

W listopadzie 2018 roku Marriott zgłosiło do Information Commissioner (ICO) naruszenie dotyczące incydentu cybernetycznego polegającego na ujawnieniu danych osobowych zawartych w około 339 milionach rekordów gości na całym świecie, z czego około 30 milionów dotyczyło mieszkańców 31 krajów Europejskiego Obszaru Gospodarczego (EOG) a 7 milionów związanych było z mieszkańcami Wielkiej Brytanii. Podatność danych rozpoczęła się najprawdopodobniej w 2014 r., kiedy to doszło do naruszenia systemu informatycznego grupy hoteli Starwood. W 2016 r. Marriott nabył Starwood, ale ujawnienie danych o klientach zostało odkryte dopiero w 2018 r.

Kompas FORSAFE

ZALECAMY ZWRÓCENIE UWAGI NA:

1. Stosowanie wieloskładnikowego uwierzytelniania dla kont w systemach, programach, aplikacjach uprawniających do dostępu do danych osobowych.

2. Wdrożenie odpowiedniego bieżącego monitorowania ruchu sieciowego i aktywności użytkowników, w szczególności aktywności na kontach uprzywilejowanych.

3. Weryfikację jakie systemy, usługi i informacje są wykorzystywane przez użytkowników.

4. Monitorowanie baz danych.

5. Kontrolę systemów krytycznych.

6. Wdrożenie systemu zarządzania zdarzeniami i incydentami bezpieczeństwa.

7. Przeanalizowanie systemu zarządzania zdarzeniami i incydentami bezpieczeństwa w aspekcie generowanych alertów.

8. Wdrożenie „białej listy", tj. oprogramowania, które pozwala tylko niektórym użytkownikom lub adresom IP na dostęp do określonych systemów lub oprogramowania, w zależności od ich określonej roli. Zaleca się wykorzystywanie „białej listy" na:
a) urządzeniach, do których można uzyskać zdalny dostęp;
b) urządzeniach, które przechowują duże ilości lub wrażliwe kategorie danych osobowych;
c) wszelkich innych systemach, które uważane są za „krytyczne" dla operacji sieciowych;
d) terminalach POS oraz wszelkich innych urządzeniach, które przetwarzają transakcje kartami płatniczymi.

9. Regularne testowanie i ocenianie skuteczności zastosowanych środków bezpieczeństwa.

Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)

Data wydania decyzji

12.11.2020 r.

Podmiot kontrolowany

Vodafone Italia S.p.A.

Wysokość kary

12 251 601 EUR

Rodzaj naruszenia

Naruszenie Art. 5 (1), (2), Art. 6 (1), Art. 7, Art. 15 (1), Art. 16, Art. 21, Art. 24, Art. 25 (1), Art. 32, Art. 33 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Urząd Ochrony Danych we Włoszech otrzymał liczne skargi i zgłoszenia na operatora telekomunikacyjnego Vodafone Italia S.p.A., które odnosiły się do niezgodnego z prawem przetwarzania danych osobowych w celach telemarketingowych. Dochodzenie w tej sprawie ujawniło dodatkowo kilka naruszeń prawa o ochronie danych, w tym:

a) brak wdrożenia systemów kontroli „łańcucha" zbierania danych osobowych od momentu pierwszego kontaktu z potencjalnym klientem,
b) przekazywanie przez podmioty zewnętrzne danych do Vodafone bez zgody na przekazywanie danych osobowych pomiędzy niezależnymi administratorami danych,
c) dostęp personelu podmiotów zewnętrznych do korporacyjnych baz danych Vodafone,
d) brak zgłoszenia zawiadomienia o naruszeniu danych osobowych do organu nadzorczego,
e) brak realizacji praw podmiotów danych w sposób prawidłowy.

Kompas FORSAFE

JAK ZAPOBIEGAĆ TAKIM NARUSZENIOM?

1) Weryfikuj bazy marketingowe w zakresie posiadania udokumentowanej zgody na działania marketingowe oraz realizuj działania marketingowe jedynie wobec osób, które wyraziły na to zgodę.

2) Wdrażaj systemy kontroli „łańcucha" zbierania danych osobowych już od momentu pierwszego kontaktu potencjalnego klienta.

3) Wprowadzaj procedury określające zasady pracy na danych osobowych przez podmioty zewnętrzne działające w imieniu Spółki.

4) Kontroluj działania marketingowe realizowane przez podmioty zewnętrzne w imieniu Spółki.

5) Ureguluj dostępy personelu podmiotów zewnętrznych do korporacyjnych baz danych Spółki.

6) Kontroluj łańcuch dostawców usług w zakresie ochrony danych osobowych.

7) Wprowadź procedury realizacji praw podmiotów danych.

8) Stosuj środki techniczne i organizacyjne dotyczące obsługi wniosków o skorzystanie z praw podmiotów danych.

9) Kupuj bazy danych osobowych jedynie od rzetelnego dostawcy, gwarantującego legalność pozyskania zgód na działania marketingowe oraz na sprzedaż baz danych podmiotom trzecim.

Kary i decyzje Urzędu Ochrony Danych Osobowych

1. Kara dla Spółki prywatnej zajmującej się analizą danych (15.03.2019)
2. Kara dla Dolnośląskiego Związku Piłki Nożnej (25.04.2019)
3. Kara dla Morele.net (10.09.2019)
4. Kara dla QuickClickNow (16.10.2019)
5. Kara dla Burmistrza Aleksandrowa Kujawskiego (18.10.2019)
6. Kara dla Szkoły Podstawowej nr 2 w Gdańsku (18.02.2020)
7. Kara dla Vis Consulting (9.03.2020)
8. Kara dla East Power (29.05.2020)
9. Kara dla Przedsiębiorcy prowadzącego przedszkole i żłobek (03.06.2020)
10. Kara dla Głównego Geodety Kraju (02.07.2020 i 24.08.2020)
11. Kara dla Szkoły Głównej Gospodarstwa Wiejskiego (21.08.2020)
12. Kara dla Virgin Mobile Polska (03.12.2020)
13. Kara dla TUiR WARTA S.A. (09.12.2020)
14. Kara dla ID Finance Poland (17.12.2020)

32 KARA DLA PRYWATNEJ SPÓŁKI ZAJMUJĄCEJ SIĘ ANALIZĄ DANYCH

KOMPAS FORSAFE

Data wydania decyzji

15.03.2019 r.

Podmiot kontrolowany

Spółka prywatna zajmująca się dostarczaniem i analizą danych

Wysokość kary

943 470 PLN*

*Sąd anulował karę z powodu błędów proceduralnych

Rodzaj naruszenia

Naruszenie Art. 14 RODO.
Niedostateczne wypełnienie obowiązków informacyjnych.

Przedmiot decyzji

We wrześniu 2018 roku pracownicy Urzędu Ochrony Danych Osobowych (UODO) przeprowadzili kontrolę w prywatnej spółce zajmującej się dostarczaniem i analizą danych. Przedmiotem kontroli było przetwarzanie przez Spółkę danych osobowych pozyskiwanych ze źródeł publicznie dostępnych, w tym z rejestrów publicznych. Pracownicy UODO zweryfikowali dopełnienie obowiązku informacyjnego w stosunku do osób fizycznych prowadzących działalność gospodarczą - przedsiębiorców, którzy ją obecnie prowadzą lub zawiesili, a także przedsiębiorców, którzy prowadzili taką działalność w przeszłości. W ocenie UODO Spółka nie spełniła obowiązku informacyjnego wobec 6 671 368 osób, których dane osobowe są przetwarzane przez administratora danych.

Kompas FORSAFE

BY UNIKNĄĆ TAKIEGO NARUSZENIA ZALECAMY:

1) Bezwzględne spełnianie obowiązku informacyjnego wobec wszystkich osób, których dane osobowe podlegają przetwarzaniu przez administratora danych.

Administrator pozyskując dane osobowe ze źródeł publicznie dostępnych, w tym z rejestrów publicznych (m.in. Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej, Bazy REGON Głównego Urzędu Statystycznego) zobowiązany jest do spełnienia obowiązku informacyjnego wobec:

a) osób fizycznych prowadzących działalność gospodarczą,

b) osób będących wspólnikami lub członkami organów spółek,

c) osób będących wspólnikami lub członkami organów fundacji,

d) osób będących wspólnikami lub członkami organów stowarzyszeń.

Data wydania decyzji

25.04.2019 r.

Podmiot kontrolowany

Dolnośląski Związek Piłki Nożnej

Wysokość kary

55 750,50 PLN

Rodzaj naruszenia

Naruszenie Art. 6 RODO.
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

W lipcu 2018 roku Dolnośląski Związek Piłki Nożnej (DZPN) z siedzibą we Wrocławiu zgłosił do Prezesa Urzędu Ochrony Danych Osobowych naruszenie dotyczące niezamierzonej publikacji danych osobowych osób, którym przyznano licencje sędziowskie w roku 2015, w zakresie imienia, nazwiska, numeru PESEL oraz adresu zamieszkania na stronie internetowej DZPN.
Naruszenie dotyczyło 585 osób. DZPN poinformował organ nadzorczy o usunięciu tego naruszenia natomiast Urząd Ochrony Danych Osobowych (UODO) otrzymał skargę od jednej z osób, której dane osobowe zostały udostępnione na stronie internetowej DZPN. UODO dokonało sprawdzenia, w wyniku którego ustalono, iż opublikowane dane osobowe sędziów nadal widnieją na stronie internetowej DZPN.

Kompas FORSAFE

BY UNIKNĄĆ TAKIEGO NARUSZENIA ZALECAMY:

1) Podczas publikacji danych osobowych na stronie internetowej kierowanie się zasadą minimalizacji.

2) Opracowanie procedury zarządzania stroną www zawierającej schemat działania w sytuacji wprowadzania danych osobowych na stronę internetową.

3) Weryfikowanie czy dane podlegające usunięciu ze strony internetowej faktycznie zostały usunięte.

4) Weryfikowanie czy podmiot przetwarzający wywiązał się ze zlecenia usunięcia danych ze strony internetowej.

Data wydania decyzji

10.09.2019 r.

Podmiot kontrolowany

Morele.net

Wysokość kary

2 830 410 PLN

Rodzaj naruszenia

Naruszenie Art. 32 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

W listopadzie i grudniu 2018 roku Morele.net trzykrotnie zgłosiła do Prezesa Urzędu Ochrony Danych Osobowych naruszenie dotyczące uzyskania nieuprawnionego dostępu do bazy danych klientów Spółki. Naruszenie dotyczyło łącznie około 2 200 000 użytkowników. Wobec niektórych użytkowników zastosowano metodę zwaną phishingiem mającą na celu wyłudzenie danych, m.in. uwierzytelniających do rachunku bankowego.

Kompas FORSAFE

JAK UNIKNĄĆ TAKIEGO NARUSZENIA?

1) Wdróż mechanizm dwuetapowego uwierzytelniania do aplikacji i programów dostępnych z poziomu Internetu, w których przetwarzane są dane osobowe.

2) Wprowadź procedury i system powiadamiania o zdarzeniach niepożądanych, monitoruj ruch sieciowy.

3) Regularnie testuj, mierz i oceniaj skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

4) Wprowadź środki organizacyjne i techniczne umożliwiające udowodnienie otrzymania zgody podmiotu danych, w szczególności w sposób pozwalający na utrwalenie faktu otrzymania zgody.

5) Poprzedź usunięcie danych analizą zasadności ich usunięcia.

6) Udokumentuj usunięcie danych.

Data wydania decyzji

16.10.2019 r.

Podmiot kontrolowany

ClickQuickNow Sp. z o.o.

Wysokość kary

201 559,50 PLN

Rodzaj naruszenia

Naruszenie Art. 5 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

W lutym 2019 roku pracownicy Urzędu Ochrony Danych Osobowych (UODO) przeprowadzili kontrolę w ClickQuickNow Sp. z o.o., której przedmiotem było przetwarzanie przez Spółkę danych osobowych, z wyłączeniem danych dotyczących osób zatrudnionych. W ocenie UODO Spółka nie zapewniła osobom, których dane dotyczą łatwego skorzystania z ich uprawnienia w zakresie wycofania zgody na przetwarzanie ich danych osobowych oraz realizacji prawa do bycia zapomnianym.

Kompas FORSAFE

BY UNIKNĄĆ TAKIEGO NARUSZENIA ZALECAMY:

1) Zaprojektowanie procesu obsługi wniosków o odwołanie zgody na przetwarzanie danych, w taki sposób, by osoby, których dane dotyczą mogły skutecznie skorzystać ze swojego prawa do wycofania zgody oraz prawa do bycia zapomnianym.

2) Zaprojektowanie procesu odwołania zgody w taki sposób, aby spełnione było kryterium prostego i szybkiego odwołania zgody.

40 KARA DLA BURMISTRZA ALEKSANDROWA KUJAWSKIEGO

KOMPAS FORSAFE

Data wydania decyzji

18.10.2019 r.

Podmiot kontrolowany

Burmistrz Aleksandrowa Kujawskiego

Wysokość kary

40 000 PLN

Rodzaj naruszenia

Naruszenie Art. 28 RODO.
Niewłaściwa umowa powierzenia przetwarzania danych.

Przedmiot decyzji

Na przełomie stycznia i lutego 2019 roku pracownicy Urzędu Ochrony Danych Osobowych (UODO) przeprowadzili planowaną kontrolę w Urzędzie Miejskim w Aleksandrowie Kujawskim, której przedmiotem było przetwarzanie danych osobowych przez Burmistrza Aleksandrowa Kujawskiego w ramach procesu wysyłki korespondencji i prowadzenia Biuletynu Informacji Publicznej (BIP), a także sposób prowadzenia rejestru czynności przetwarzania oraz dokumentowania naruszeń ochrony danych osobowych. Ustalono, że Administrator nie zawarł umów powierzenia przetwarzania danych z podmiotami, którym przekazywał dane osobowe, a co za tym idzie, udostępniał je bez podstawy prawnej (chodziło o firmy dzierżawiące serwery oraz dostarczające oprogramowanie do stworzenia BIP i udzielające wsparcia serwisowego w tej sferze). Kolejne uchybienie dotyczyło braku dokumentacji wewnętrznej umożliwiającej kontrolę okresu retencji dla danych znajdujących się w BIP (dostępne były oświadczenia majątkowe, których okres przechowywania minął). Dodatkowo, w rejestrze czynności przetwarzania, nie zostali wskazani wszyscy odbiorcy danych oraz planowane terminy usunięcia danych. Administrator nie sporządził kopii zapasowych nagrań z posiedzeń rady miejskiej. Ich dostępność w BIP ograniczała się jedynie do serwisu YouTube, na którym zostały umieszczone w ramach dedykowanego kanału. Działanie to nie zostało również uwzględnione w analizie ryzyka.

Kompas FORSAFE

JAKIE DZIAŁANIA POWINNY ZOSTAĆ PODJĘTE?

1) Zawarcie umowy powierzenia z podmiotem, który jest odpowiedzialny za prowadzenie strony internetowej Biuletynu Informacji Publicznej.

2) Opracowanie polityki dotyczącej przetwarzania danych osobowych w Biuletynie Informacji Publicznej.

3) Analiza danych opublikowanych w Biuletynie Informacji Publicznej pod kątem ich aktualności i celowości publikacji oraz terminu usunięcia danych osobowych.

4) Przeprowadzenie przez organ publiczny analizy ryzyka związanego z korzystaniem z narzędzia służącego do transmisji nagrań z obrad Rady Gminy/Miasta/Powiatu.

5) Wdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Gminy/Miasta/Powiatu, w tym wykonywanie kopii zapasowych.

6) Prowadzenie rejestru czynności przetwarzania danych osobowych zgodnie z wytycznymi art. 30 ust. 1 Rozporządzenia.

7) Uwzględnienie informacji o odbiorcy danych w rejestrze czynności przetwarzania danych osobowych.

8) Uwzględnienie w rejestrze czynności przetwarzania danych osobowych dla każdego procesu przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych zgodnie z zasadą ograniczonego przechowywania.

Data wydania decyzji

18.02.2020 r.

Podmiot kontrolowany

Szkoła Podstawowa nr 2 w Gdańsku

Wysokość kary

20 000 PLN

Rodzaj naruszenia

Naruszenie Art. 5, Art. 9 RODO.
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

Urząd Ochrony Danych Osobowych (UODO) otrzymał informację o nieprawidłowościach w procesie przetwarzania danych osobowych uczniów Szkoły Podstawowej nr 2 w Gdańsku, polegających na gromadzeniu odcisków palców dzieci korzystających ze stołówki szkolnej. W konsekwencji zgłoszenia wszczęto postępowanie z urzędu w sprawie zaistniałych nieprawidłowości. W wyniku kontroli stwierdzono, że szkoła od 2015 r. korzysta z czytnika biometrycznego umieszczonego przy wejściu do stołówki szkolnej, który identyfikuje dzieci pobierające posiłki w stołówce szkolnej w celu weryfikacji uiszczenia opłaty za posiłek w danym dniu. Aby opisana sytuacja była „legalna", Szkoła pobierała od rodziców zgody na korzystanie z czytnika na odcisk palca, która była umieszczona w umowie o korzystanie z posiłków w stołówce szkolnej.
Zdaniem Prezesa UODO tego typu zasady wprowadzają nierówne traktowanie uczniów i ich bezpodstawne zróżnicowanie, gdyż wyraźnie promują uczniów posiadających identyfikację biometryczną. Wykorzystywanie danych biometrycznych w zestawieniu z celem, w jakim są one przetwarzane, jest nieproporcjonalne. Prezes UODO uważa również, że dane osobowe dzieci wymagają szczególnej ochrony.

Kompas FORSAFE

W JAKICH SYTUACJACH MOŻNA KORZYSTAĆ Z DANYCH BIOMETRYCZNYCH?

Dane biometryczne mogą być wykorzystywane m.in. w celach:

1) zapewnienia bezpieczeństwa osobowego,

2) zapewnienia bezpieczeństwa przemysłowego,

3) ochrony informacji,

4) weryfikacji osób podejrzanych i ocenie ich udziału w przestępstwach,

5) wydawania dokumentów identyfikacyjnych (paszportów),

6) kontroli dostępu do określonych sfer bezpieczeństwa.

Wykorzystując dane biometryczne zawsze należy rozważyć czy jest to adekwatne w stosunku do celu, jaki będzie realizowany.

Data wydania decyzji

9.03.2020 r.

Podmiot kontrolowany

Vis Consulting Sp. z o.o.

Wysokość kary

20 000 PLN

Rodzaj naruszenia

Naruszenie Art. 31, Art. 58 RODO.
Niewystarczająca współpraca z organem nadzorczym.

Przedmiot decyzji

Firma Vis Consulting Sp. z o.o. została poddana przez Prezesa UODO kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, w nawiązaniu do ustaleń dokonanych w toku innej kontroli przeprowadzonej u jednego z kontrahentów Spółki. W wyniku tej kontroli wyszło na jaw, że ma ona podpisaną umowę o współpracy w zakresie outsorcingu usług telemarketingowych. Urząd chciał więc przeprowadzić czynności kontrolne w firmie, która faktycznie wykonywała połączenia telefoniczne i przetwarzała dane. Celem kontroli miało być zbadanie legalności przetwarzania danych osobowych przy użyciu przedmiotowego systemu. Pomimo dwóch prób przeprowadzenia kontroli, Spółka nie zapewniła dostępu do danych osobowych i innych informacji oraz pomieszczeń, a tym samym uniemożliwiła Prezesowi UODO przeprowadzenia czynności kontrolnych. W efekcie spółka została ukarana za brak współpracy.

Kompas FORSAFE

Współpracuj w trakcie kontroli z pracownikami Urzędu Ochrony Danych Osobowych!

Pamiętaj! Na potrzeby kontroli kontrolujący ma prawo:

1) do wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń administratora;

2) do wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;

3) do przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

5) zlecać sporządzanie ekspertyz i opinii.

Data wydania decyzji

29.05.2020 r.

Podmiot kontrolowany

East Power Sp. z o.o.

Wysokość kary

15 000 PLN

Rodzaj naruszenia

Naruszenie Art. 31 RODO, Art. 58 RODO
Niewystarczająca współpraca z organem nadzorczym.

Przedmiot decyzji

Sprawa zaczęła się od skargi obywatela Niemiec, który otrzymywał komunikację marketingową pomimo złożonego sprzeciwu. Nadawcą niechcianej korespondencji była firma East Power sp. z o.o. – działająca m.in. na terenie Niemiec agencja pracy. Skarga została pierwotnie zgłoszona do niemieckiego organu nadzorczego. Ponieważ jednak spółka ma siedzibę w Polsce, sprawę przejął Prezes UODO. Polski organ nadzorczy zwrócił się do East Power o złożenie wyjaśnień – w szczególności wskazanie podstawy prawnej dla przetwarzania danych osobowych osoby skarżącej. Na przestrzeni kilkunastu miesięcy PUODO starał się ustalić stan faktyczny sprawy, jednak bez skutku. Wnioski o udostępnienie dokumentów, przekazanie informacji lub złożenie wyjaśnień pozostawały bez odpowiedzi, były realizowane z opóźnieniem bądź wykonywane przez udzielanie wymijających odpowiedzi. W związku z utrudnianiem rozwiązania sprawy przez firmę PUODO podjął decyzję o nałożeniu administracyjnej kary pieniężnej w wysokości 15 000 zł za brak odpowiedniej współpracy z organem nadzorczym.

Kompas FORSAFE

Współpracuj w trakcie kontroli z pracownikami Urzędu Ochrony Danych Osobowych!

Pamiętaj! Na potrzeby kontroli kontrolujący ma prawo:

1) do wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń administratora;

2) do wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;

3) do przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

4) żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

5) zlecać sporządzanie ekspertyz i opinii.

48 KARA DLA PRZEDSIĘBIORCY PROWADZĄCEGO PRZEDSZKOLE

KOMPAS FORSAFE

Data wydania decyzji

03.06.2020 r.

Podmiot kontrolowany

Przedsiębiorca prowadzący niepubliczny żłobeki przedszkole

Wysokość kary

5 000 PLN

Rodzaj naruszenia

Naruszenie Art. 31 i Art. 58 RODO.
Niewystarczająca współpraca z organem nadzorczym.

Przedmiot decyzji

Prezes UODO nałożył 5 tys. zł kary na indywidualnego przedsiębiorcę prowadzącego niepubliczny żłobek i przedszkole. Powodem nałożenia kary było niezapewnienie Prezesowi UODO dostępu do danych osobowych i innych informacji niezbędnych do realizacji jego zadań – czyli do oceny, czy administrator w sposób zgodny z przepisami RODO zawiadomił po naruszeniu osoby, których dane dotyczyły. Przedsiębiorca zgłosił do Prezesa UODO naruszenie ochrony danych osobowych, polegające na utracie dostępu do danych osobowych przechowywanych w prowadzonym niepublicznym żłobku i przedszkolu. Naruszenie nastąpiło na skutek działania innego podmiotu, który wymienił w lokalu wszystkie zamki, zamykając wewnątrz wyposażenie przedszkola, w tym komputery i dokumentację zawierającą dane osobowe pracowników, dzieci uczęszczających do przedszkola i żłobka oraz ich opiekunów prawnych. W związku z dokonanym zgłoszeniem Prezes UODO kilkukrotnie zwrócił się do Przedsiębiorcy z prośbą o uzupełnienie informacji, ale nie uzyskał stosownej odpowiedzi. Była to główna przyczyna nałożenia kary.

Kompas FORSAFE

Zapamiętaj!

Dokonując zgłoszenia naruszenia danych osobowych, współpracuj z Prezesem Urzędu Ochrony Danych Osobowych w ustaleniu stanu faktycznego sprawy oraz prawidłowego jej rozstrzygnięcia.

50 KARA DLA GŁÓWNEGO GEODETY KRAJU

KOMPAS FORSAFE

Data wydania decyzji

02.07 i 24.08.2020r.

Podmiot kontrolowany

Główny Geodeta Kraju

Wysokość kary

100 000 PLN*

*24.08.2020 r. PUODO nałożył maksymalny wymiar kary tytułem niewystarczającej podstawy prawnej do przetwarzania danych. Wpływ na nią miało również zachowanie GGK w trakcie kontroli.

Rodzaj naruszenia

Naruszenie Art. 31, Art. 58 RODO
Niewystarczająca współpraca z organem nadzorczym.

Przedmiot decyzji

W marcu 2020 roku pracownicy Urzędu Ochrony Danych Osobowych (UODO) przeprowadzili kontrolę w Głównym Urzędzie Geodezji i Kartografii. Przedmiotem kontroli było zbadanie procesu udostępniania przez Głównego Geodetę Kraju za pośrednictwem portalu internetowego GEOPORTAL2 (geoportal.gov.pl) danych osobowych z ewidencji gruntów i budynków.
Główny Geodeta Kraju udaremnił jednak przeprowadzenie czynności kontrolnych w zaplanowanym zakresie. Odmówił składania jakichkolwiek zeznań w zakresie legalności publikowania na GEOPORTAL2 (geoportal.gov.pl) informacji o numerach ksiąg wieczystych, jak również nie pozwolił kontrolującym na zbadanie systemów informatycznych wykorzystywanych w procesie publikowania danych na GEOPORTAL2. Ostatecznie w toku kontroli pozyskana została jedynie dokumentacja określająca środki organizacyjne zastosowane przez Głównego Geodetę Kraju w celu zapewnienia bezpieczeństwa danych oraz dowody potwierdzające wyznaczenie inspektora ochrony danych.

Kompas FORSAFE

ZAPAMIĘTAJ!
Współpracuj w trakcie kontroli z pracownikami UrzęduOchrony Danych Osobowych.

Na potrzeby kontroli kontrolujący ma prawo do:

1) wstępu w godzinach od 6.00 do 22.00 na gruntoraz do budynków, lokali lub innych pomieszczeń;

2) wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;

3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;

4) żądania złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwania w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

5) zlecania sporządzania ekspertyz i opinii.

Data wydania decyzji

21.08.2020 r.

Podmiot kontrolowany

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie

Wysokość kary

50 000 PLN*

Rodzaj naruszenia

Naruszenie Art. 32 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie (SGGW) zgłosiła do Prezesa Urzędu Ochrony Danych Osobowych naruszenie ochrony danych osobowych kandydatów na studia w SGGW, które miało miejsce w listopadzie 2019 r. i związane było z kradzieżą przenośnego prywatnego komputera pracownika SGGW. Przedmiotowe naruszenie dotyczyło około 81 624 kandydatów na studia wpisanych do Systemu Obsługi Kandydatów (SOK) z okresu ostatnich 5 lat.
W listopadzie 2019 roku pracownicy Urzędu Ochrony Danych Osobowych (UODO) dokonali czynności kontrolnych i ustalili, iż naruszenie związane było z kradzieżą przenośnego prywatnego komputera pracownika SGGW, pełniącego również funkcję sekretarza Uczelnianej Komisji Rekrutacyjnej SGGW. Skradziony laptop był używany przez ww. pracownika do celów prywatnych i służbowych, w tym również do przetwarzania danych osobowych kandydatów na studia w SGGW na potrzeby czynności rekrutacyjnych w ramach pełnionej przez tą osobę funkcji. Pracownik importował na swój prywatny komputer z SOK pełny zestawy danych osobowych kandydatów na studia. SGGW nie posiadała informacji o tym fakcie, a operacja eksportu danych nie była rejestrowana w SOK.

Kompas FORSAFE

PUODO w raporcie końcowym zwrócił uwagę na następujące zagadnienia:

DOKUMENTACJA

- ☑ Opracowanie polityki ochrony danych rozumianej jako strategia ochrony danych, plan działań mający umożliwić osiągnięcie celu, jakim jest skuteczna ochrona danych.
- ☑ Wdrożenie procedury wykorzystywania sprzętu prywatnego do celów służbowych.
- ☑ Wdrożenie procedury retencji danych.
- ☑ Wdrożenie procedury zgłaszania naruszeń bezpieczeństwa danych osobowych.
- ☑ Uwzględnienie w polityce ochrony danych planu utrzymania zgodności oraz prowadzenia audytów wewnętrznych, w tym m.in. zasad monitorowania i audytu procedur wewnętrznych.
- ☑ Opracowanie metodyki analizy ryzyka.

CZYNNOŚCI

- ☑ Opracowanie polityki ochrony danych rozumianej jako strategia ochrony. Zapewnienie ochrony danych osobowych na płaszczyźnie nie tylko formalnej (dokumentacja), ale i praktycznej.
- ☑ Wykonywanie przeglądów i aktualizacji dokumentacji opisującej system ochrony danych osobowych w szczególności w sytuacji zmian w przepisach o ochronie danych osobowych.
- ☑ Monitorowanie procedur związanych z ochroną danych osobowych oraz dostosowywanie ich do procesów przetwarzania danych.
- ☑ Monitorowanie, weryfikacja i kontrola nad sposobem i zakresem przetwarzania danych osobowych.
- ☑ Weryfikacja procesów przetwarzania danych osobowych w aspekcie retencji danych.
- ☑ Usunięcie danych lub ich anonimizacja po osiągnięciu celów przetwarzania.
- ☑ Prowadzenie rejestru czynności przetwarzania danych osobowych zgodnie z wytycznymi art. 30 ust. 1 Rozporządzenia.
- ☑ Uwzględnienie informacji o odbiorcy danych w rejestrze czynności przetwarzania danych osobowych.
- ☑ Cykliczne monitorowanie zawartości rejestru czynności przetwarzania danych osobowych.
- ☑ Wykonywanie analizy ryzyka dla procesów przetwarzania danych osobowych z uwzględnieniem: terminu jej wykonania, informacji o osobie wykonującej analizę ryzyka, informacji o terminie zatwierdzenia oraz osobie zatwierdzającej analizę ryzyka.

ŚRODKI TECHNICZNE I ORGANIZACYJNE

- ☑ Wdrożenie środków technicznych zabezpieczających komputery przenośne przed nieuprawnionym dostępem.
- ☑ Wdrożenie środków technicznych zabezpieczających pliki z danymi osobowymi przed nieuprawnionym dostępem.
- ☑ Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
- ☑ Wdrożenie środków takich jak zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
- ☑ Przeanalizowanie systemów informatycznych i aplikacji pod kątem rozliczalności.
- ☑ Zastosowanie zasady rozliczalności w systemach informatycznych realizowanej w formie automatycznie generowanych zapisów (tzw. logów) zawierających określony zestaw informacji umożliwiający stwierdzenie kto, kiedy, jakie operacje oraz w odniesieniu do jakich danych wykonał w systemie.
- ☑ Weryfikacja programów i aplikacji w zakresie rejestrowania eksportu danych oraz zakresu eksportowanych danych.

ROLA INSPEKTORA OCHRONY DANYCH

- ☑ Ustalenie przez Inspektora Ochrony Danych priorytetów w swojej pracy, które powinny polegać na indywidualnym i samodzielnym określaniu środków oraz metod działania i dostosowywania ich do specyfiki konkretnego administratora.

- ☑ Wykonywanie zadań przez Inspektora Ochrony Danych z uwzględnieniem należytego ryzyka związanego z operacjami przetwarzania danych osobowych.

- ☑ Przeprowadzanie audytów przez Inspektora Ochrony Danych, obejmujących następujące etapy: zbieranie informacji, analizowanie i sprawdzanie zgodności przetwarzania, informowanie, doradzanie i rekomendowanie określonych rozwiązań.

  Etap zbierania informacji powinien uwzględniać zbieranie informacji o podmiocie i stosowanych w nim procesach przetwarzania danych, w tym identyfikacja czynności przetwarzania danych, ustalenie aktywów wykorzystywanych do przetwarzania danych, tj. systemów informatycznych, dokumentów, nośników danych i ustalenie zakresów danych, które są przetwarzane wraz z ich kategoryzacją.

  Etap analizowania i sprawdzania zgodności przetwarzania z przepisami rozporządzenia 2016/679 powinien być wykonany pod względem formalnoprawnym, jak i zgodności systemów informatycznych.

  Etap informowania, doradzania i rekomendowania określonych rozwiązań powinien być zakończony opracowaniem raportu, w którym wskazane są rekomendacje.

- ☑ Monitorowanie przepisów o ochronie danych osobowych przez Inspektora Ochrony Danych.
- ☑ Dostosowanie szkoleń realizowanych przez Inspektora Ochrony Danych do specyfiki podmiotu oraz specyfiki poszczególnych działów/wydziałów.
- ☑ Zapewnienie Inspektorowi Ochrony Danych szkoleń podnoszących jego kwalifikacje, monitorowanie procesu szkolenia, w tym dysponowanie potwierdzeniem odbycia szkolenia przez Inspektora Ochrony Danych.
- ☑ Włączanie Inspektora Ochrony Danych we wszystkie sprawy dotyczące ochrony danych osobowych.
- ☑ Wyznaczenie Inspektora Ochrony Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań związanych z ochroną danych osobowych.
- ☑ Unikanie częstej zmiany Inspektora Ochrony Danych.

Data wydania decyzji

03.12.2020 r.

Podmiot kontrolowany

Virgin Mobile Polska Sp. z o.o.

Wysokość kary

1 968 524 PLN

Rodzaj naruszenia

Naruszenie Art. 5 (1) f), Art. 5 (2), Art. 25 (1), Art. 32 (1) b), Art. 32 (1) d), Art. 32 (2) RODO. Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

W grudniu 2019 roku Virgin Mobile Polska Sp. z o.o. zgłosiła do Prezesa UODO naruszenie polegające na uzyskaniu przez osobę nieuprawnioną dostępu do danych osobowych abonentów usług przedpłaconych i pozyskaniu 142 222 rekordów potwierdzeń ich rejestracji. Naruszenie pełnego zakresu danych osobowych wystąpiło wyłącznie w 4522 przypadkach. Odnosiło się do imion i nazwisk, numerów PESEL i numerów dokumentów abonentów. W pozostałym zakresie, naruszenie odnosiło się do: imion, nazwisk oraz numerów PESEL (108702 przypadków) lub numerów dokumentu abonenta (10167 przypadków). W związku ze zgłoszonym naruszeniem pracownicy UODO dokonali w Spółce kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Zakresem kontroli objęty został sposób przetwarzania danych, w tym sposób zabezpieczenia danych, w ramach świadczenia usług telekomunikacyjnych abonentom usług przedpłaconych. Na podstawie informacji i dowodów zgromadzonych w toku kontroli pracownicy UODO ustalili, iż Spółka naruszyła zasadę poufności danych poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych służących do rejestracji danych osobowych abonentów usług przedpłaconych, co doprowadziło do uzyskania przez osobę nieuprawnioną dostępu do tych danych.

Kompas FORSAFE

JAK ZAPOBIEGAĆ TAKIM NARUSZENIOM?

1) Regularnie testuj, mierz i oceniaj skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

2) Uwzględnij w Polityce Ochrony Danych Osobowych kwestie dotyczące regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

3) Weryfikuj dobór i poziom skuteczności stosowanych środków technicznych na każdym etapie przetwarzania oraz oceniaj je przez pryzmat adekwatności do ryzyk i proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

4) Przeprowadzaj testy nastawione na weryfikację zabezpieczeń programów i aplikacji.

5) Wykonaj i udokumentuj analizę ryzyka uwzględniającą charakter zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

6) Przeglądy, sprawdzenia lub audyty opieraj na kompletnych i rzetelnych informacjach.

7) Realizuj zasadę rozliczalności w kontekście zachowania staranności zarówno przy nadawaniu upoważnień do przetwarzania danych, jak również przy ich cofaniu wobec byłego pracownika, zleceniobiorcy, czy wykonawcy.

8) Odbieraj uprawnienia w systemie informatycznym osobom, którym wygasło upoważnienie.

Data wydania decyzji

09.12.2020 r.

Podmiot kontrolowany

Towarzystwo Ubezpieczeń i Reasekuracji WARTA S.A.

Wysokość kary

85 588 PLN

Rodzaj naruszenia

Naruszenie Art. 33 (1) i Art. 34 (1) RODO
Niewystarczające wypełnienie obowiązków powiadamiania o naruszeniu danych.

Przedmiot decyzji

W maju 2020 r. do Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja o naruszeniu, polegającym na wysłaniu pocztą elektroniczną przez agenta ubezpieczeniowego ds. obsługi Towarzystwa Ubezpieczeń i Reasekuracji WARTA S.A., polisy ubezpieczeniowej zawierającej dane osobowe do nieuprawnionego adresata, w wyniku czego doszło do naruszenia poufności danych dwóch osób w zakresie imion, nazwisk, adresów zamieszkania lub korespondencyjnych, numerów PESEL, numerów telefonów, adresów poczty elektronicznej oraz informacji dotyczących przedmiotu ubezpieczenia (samochód osobowy), zakresu ubezpieczenia, płatności, cesji, a także dodatkowych zapisów wynikających z umowy. O naruszeniu poinformował adresat wiadomości, który wszedł w posiadanie nieprzeznaczonych dla niego dokumentów zawierających ww. dane osobowe. UODO zwrócił się do Spółki o wyjaśnienie, czy w związku z zaistniałym faktem została dokonana analiza ryzyka naruszenia praw i wolności osób fizycznych niezbędna do oceny, czy doszło do naruszenia. W odpowiedzi na pismo Spółka potwierdziła, że doszło do naruszenia ochrony danych osobowych, jednak założyła brak wysokiego prawdopodobieństwa negatywnych skutków dla osób, których dane dotyczą. Wskazała na zastosowany środek naprawczy w postaci skierowania do nieuprawnionego odbiorcy prośby o trwałe usunięcie wiadomości wraz z prośbą o informację zwrotną potwierdzającą jej usunięcie. Swoją decyzję umotywowała faktem, iż klient sam podał błędny adres poczty elektronicznej, na który został wysłany dokument polisy ubezpieczeniowej. UODO nie przyjęło argumentacji Spółki wszczynając wobec niej postępowanie administracyjne.

Kompas FORSAFE

JAK WŁAŚCIWIE POSTĄPIĆ PO WYKRYCIU NARUSZENIA?

1) Wykonaj ocenę naruszenia ochrony danych osobowych pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny weź pod uwagę czy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykładami takich szkód są: utrata kontroli nad własnymi danymi osobowymi, nieuprawnione odwrócenie pseudonimizacji, dyskryminacja, kradzież lub sfałszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

2) Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować ryzyko dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych. Na zgłoszenie masz 72 godziny od momentu stwierdzenia naruszenia.

3) Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, dokonaj zawiadomienia osób fizycznych, których dane dotyczą, o zaistniałym naruszeniu. Zawiadomienia należy wykonać bez zbędnej zwłoki.

4) Dokonaj wdrożenia środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych takich, jak: weryfikacja adresów mailowych wskazywanych przez klientów, szyfrowanie plików zawierających dane osobowe, które są przesyłane w wiadomościach elektronicznych.

5) Kontroluj podmioty przetwarzające m.in. w zakresie wdrożonych środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych.

Data wydania decyzji

17.12.2020 r.

Podmiot kontrolowany

ID Finance Poland Sp. z o.o. w likwidacji

Wysokość kary

1 069 850 PLN

Rodzaj naruszenia

Naruszenie Art. 5 ust. 1 lit. f, Art. 25 ust. 1, Art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. d, art. 32 ust. 2 RODO. Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

W marcu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja o naruszeniu ochrony danych osobowych, polegającym na nieautoryzowanym dostępie do danych osobowych 140 699 klientów i potencjalnych klientów, którzy przeszli przez proces rejestracji w serwisie internetowym moneyman.pl. Powodem naruszenia było błędne działanie serwera związane z jego restartem wykonanym przez IDFT Sp. z o.o. - podmiot odpowiedzialny za realizację usług mających charakter hostingu. W jego trakcie doszło do zresetowania ustawień oprogramowania odpowiadającego za bezpieczeństwo serwera i w konsekwencji do upublicznienia danych osobowych. Wykorzystując ten błąd nieustalony podmiot trzeci pobrał znajdującą się na tym serwerze bazę danych, a następnie ją z niego usunął. Wszedł w posiadanie takich danych jak: imię i nazwisko, poziom wykształcenia, adres e-mail, dane dotyczące zatrudnienia, adres e-mail osoby, której klient chce polecić pożyczkę, dane dotyczące zarobków, dane dotyczące stanu cywilnego, numer telefonu (stacjonarnego, komórkowego, wcześniej używanego numeru telefonu), numer PESEL, narodowość, numer NIP, hasło, miejsce urodzenia, adresy korespondencyjny, zameldowania, numer telefonu do miejsca pracy oraz numer rachunku bankowego. Zwrócił się również do Spółki z żądaniem zapłaty wynagrodzenia w zamian za zwrot pozyskanej bazy danych. W toku kontroli Pracownicy UODO ustalili, że Spółka nie wdrożyła zarówno w fazie projektowania procesu przetwarzania jak i w czasie samego przetwarzania, odpowiednich środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemu przetwarzania danych osobowych, a także zapewniających zdolność skutecznego i szybkiego stwierdzenia naruszenia ochrony danych osobowych oraz zapewniających regularną ocenę skuteczności tych środków. Brak tych działań skutkowało uzyskaniem przez osoby trzecie nieuprawnionego dostępu do przetwarzanych danych osobowych.

Kompas FORSAFE

JAK WŁAŚCIWIE POSTĄPIĆ PO WYKRYCIU NARUSZENIA?

1) Swoje działania opieraj na podejściu proaktywnym i prewencyjnym polegającym na zapewnianiu bezpieczeństwa danym osobowym na każdym etapie ich przetwarzania.

2) Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności określ poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych, a potem ustal, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

3) Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

4) Wykonując restart serwera pamiętaj, by sprawdzić prawidłowość konfiguracji zabezpieczeń.

5) Przechowuj hasła w systemach informatycznych w postaci niejawnej (np. poprzez zastosowanie funkcji skrótu, zwanej też haszowaniem), aby zapewnić poufność hasła i ograniczyć jego znajomość wyłącznie do osoby, która się nim posługuje.

6) Opracuj i wdróż procedury zgłaszania naruszeń bezpieczeństwa danych osobowych, które będą uwzględniały kwestie związane ze sprawnym i szybkim stwierdzeniem naruszenia ochrony danych.

7) Nie ignoruj informacji o potencjalnym naruszeniu ochrony danych osobowych otrzymanych od osoby fizycznej lub z innego źródła. Każdy sygnał o ewentualnych nieprawidłowościach powinien być przedmiotem wnikliwej analizy.

8) W sytuacji wystąpienia naruszenia ochrony danych osobowych wykonaj jego ocenę pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny weź pod uwagę czy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykładami takich szkód są: utrata kontroli nad własnymi danymi osobowymi, nieuprawnione odwrócenie pseudonimizacji, dyskryminacja, kradzież lub sfałszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

9) Wykonaj analizę ryzyka, gdy w związku z naruszeniem ochrony danych osobowych zostanie ujawnione ryzyko nie rozpatrywane we wcześniejszej analizie.

10) Zawierając umowę powierzenia uwzględnij w niej zapisy odnoszące się do postępowania w sytuacji, gdy doszło do naruszenia bezpieczeństwa danych osobowych, ale również do sytuacji jego potencjalnego wystąpienia.

11) Kontroluj podmioty przetwarzające m.in. w zakresie wdrożonych środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych.

KOMPAS FORSAFE

Materiał edukacyjny
przygotowany przez FORSAFE

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

FORSAFE Sp. z o.o.
ul. 1 Maja 31/33
90-739 Łódź
+48 600 005 880
biuro@forsafe.pl