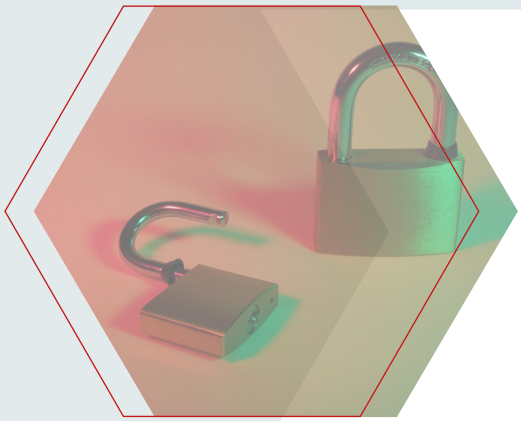
Obserwuj nas na:

Nr 5/2021 (26)
Maj 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH



ROLA I ZADANIA PODMIOTU PRZETWARZAJĄCEGO W SYTUACJI WYSTĄPIENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Podmiot przetwarzający musi jedynie ustalić, czy doszło do naruszenia ochrony danych osobowych, a następnie niezwłocznie zgłosić to naruszenie administratorowi. To istotne, by administrator mógł należycie wywiązać się z ciążących na nim obowiązków, m.in. takich jak dokonanie oceny ryzyka naruszenia praw lub wolności osób fizycznych, które wynika z naruszenia, a w stosownych przypadkach poinformowanie o naruszeniu Prezesa UODO i osób, których ono dotyczy.

Kwestia stwierdzenia przez administratora naruszenia ochrony danych osobowych jest kluczowa dla uruchomienia wszelkich procesów i działań zmierzających do minimalizacji negatywnych konsekwencji tego naruszenia. Stosownie do dyspozycji art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin od stwierdzenia naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Jak zaś stanowi art. 34 ust. 1 RODO, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Zatem dla prawidłowej i szybkiej realizacji tych obowiązków istotne znaczenie ma prawidłowe działanie podmiotu przetwarzającego. Artykuł 33 ust. 2 RODO zobowiązuje go, by po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłaszał je administratorowi. Jak natomiast wskazuje Grupa Robocza Art. 29 w „Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem2016/679", podmiot przetwarzający, po stwierdzeniu naruszenia, a przed zgłoszeniem go administratorowi, nie musi oceniać prawdopodobieństwa wystąpienia, wynikającego z naruszenia ochrony danych osobowych, ryzyka naruszenia praw lub wolności osób fizycznych. Odpowiedzialność za przeprowadzenie takiej oceny spoczywa na administratorze. Podmiot przetwarzający musi jedynie ustalić, czy doszło do naruszenia ochrony danych osobowych, a następnie bez zbędnej zwłoki zgłosić je administratorowi.

KIEDY MOŻNA POZYSKAĆ ADRES ZAMIESZKANIA ZATRUDNIANEGO PRACOWNIKA?

Pracodawca ma prawo pozyskiwać adres zamieszkania od osoby, co do której została podjęta decyzja o zatrudnieniu, gdyż jest to niezbędne do skierowania jej na obowiązkowe, wstępne badania lekarskie.

Ponieważ w obowiązujących przepisach nie ma formy pośredniej między kandydatem do pacy a pracownikiem, tj. kandydata na pracownika, co do którego została podjęta decyzja o zatrudnieniu, powstały wątpliwości, na jakim etapie rekrutacji możliwe jest pozyskiwanie adresu zamieszkania takiej osoby. O ich rozstrzygnięcie zwrócono się do Prezesa UODO.

W przesłanych w tej sprawie wyjaśnieniach Prezes UODO wskazał, że o tym, jakie dane osobowe

pracownika mogą być przetwarzane przez pracodawcę, przesądzają art. 221 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (k.p.) oraz przepisy szczególne, do których odsyła wspomniany kodeks.

Zgodnie z art. 221 k.p., pracodawca, prowadząc rekrutację, żąda od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko; datę urodzenia; dane kontaktowe wskazane przez taką osobę; wykształcenie; kwalifikacje zawodowe; przebieg dotychczasowego zatrudnienia. Natomiast zgodnie z art. 221 § 3 k.p., pracodawca żąda od pracownika podania dodatkowo danych osobowych obejmujących: adres zamieszkania; PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość; inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy; wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie; numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Jednocześnie Kodeks pracy zobowiązuje pracodawcę do kierowania pracowników na wstępne, okresowe i kontrolne badania lekarskie. Artykuł 229 § 1 pkt 1 wskazuje, że wstępnym badaniom lekarskim podlegają osoby przyjmowane do pracy. Badania lekarskie przeprowadza się zaś na podstawie skierowania wydanego przez pracodawcę (art. 229 § 4a k.p.). Wzór skierowania na badania profilaktyczne, okresowe i kontrolne został określony w załączniku nr 3a do rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 r. w sprawie przeprowadzenia badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy, który przewiduje przetwarzanie adresu zamieszkania podejmującego pracę lub zatrudnionego pracownika.

Zatem przyjąć należy, że dopuszczalne jest pozyskiwanie adresu zamieszkania od osoby, która ma zostać zatrudniona, gdyż jest to niezbędne do wypełnienia ciążącego na pracodawcy (zgodnie z art. 229 § 1 pkt 1) obowiązku skierowania takiej osoby na wstępne badania lekarskie.

ZAWIERANIE UMOWY O ZAOPATRZENIE W WODĘ LUB ODPROWADZANIE ŚCIEKÓW BEZ KOPII AKTU NOTARIALNEGO

Przedsiębiorstwo wodociągowo-kanalizacyjne nie ma podstaw prawnych, by na potrzeby zawarcia umowy o zaopatrzenie w wodę lub odprowadzanie ścieków przechowywać kopie aktów notarialnych potwierdzających własność nieruchomości.

RODO stanowi, że dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a), zbierane w konkretnych, wyraźnie i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b), oraz adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c).

Jednocześnie przedsiębiorstwo wodociągowo-kanalizacyjne, zgodnie z art. 6 ust. 2 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, jest obowiązane do zawarcia umowy o zaopatrzenie w wodę lub odprowadzanie ścieków z osobą, której nieruchomość została przyłączona do sieci i która wystąpiła z pisemnym wnioskiem o zawarcie umowy. Umowa, o której mowa w ust. 1, może być zawarta z osobą, która posiada tytuł prawny do korzystania z nieruchomości, do której ma być dostarczana woda lub z której mają być odprowadzane ścieki, albo z osobą, która korzysta z nieruchomości o nieuregulowanym stanie prawnym (art. 6 ust.4).

Zatem w świetle przepisów ustawy o zbiorowym zaopatrzeniu w wodę brak jest podstaw prawnych do pozyskiwania kopii aktów notarialnych potwierdzających własność nieruchomości i dalszego ich przechowywania. Wystarczające na te potrzeby jest bowiem przed-

stawienie stosownego dokumentu, co potwierdza orzecznictwo sądów administracyjnych. Przykładowo, Wojewódzki Sąd Administracyjny w Gliwicach w wyroku z 27 stycznia 2020 r. (sygn. akt II SA/Gl 1496/19) wskazał, że „(...) osoba ubiegająca się o zawarcie umowy o zaopatrzenie w wodę lub odprowadzenie ścieków powinna wykazać, że jest jednym z podmiotów o jakich mowa w art. 6 ust. 4-7 ustawy. Nie może ulegać zatem wątpliwości, że aby to uczynić powinna przedstawić dokument określający stan prawny nieruchomości, bo z niego będzie wynikać czy jest takim podmiotem, względnie będzie wynikać, kto jest uprawniony do potwierdzenia jej tytułu do władania nieruchomością lub lokalem do którego ma być dostarczana woda lub z którego mają być odprowadzane ścieki. Zdaniem Sądu nie może ulegać wątpliwości, że takim dokumentem powinna legitymować się również osoba ubiegająca się o określenie warunków przyłączenia nieruchomości do sieci".

ZAKUPY W WIĘZIENNEJ KANTYNIE

Osadzeni muszą realizować swoje prawo do dokonywania zakupów w więziennej kantynie na warunkach określonych przez podmiot, który ją prowadzi. Natomiast podmiot ten jest zobowiązany do przetwarzania ich danych osobowych w zakresie niezbędnym dla zapewnienia prawidłowego przeprowadzenia i rozliczenia tych zakupów.

Kwestię tę Prezes UODO analizował w związku z pytaniem pewnego więźnia, który miał wątpliwości, czy podmiot prowadzący więzienną kantynę ma prawo do tego, by podczas dokonywanych przez więźniów zakupów wprowadzać do komputera takie dotyczące ich dane, jak: imię i nazwisko, imię ojca, kwotę, jaką osadzeni mają do dyspozycji, oraz dane dotyczące tego, co kupują.

W odpowiedzi Prezes UODO wskazał, że wprawdzie dokonywanie zakupów w kantynie więziennej jest prawem osoby pozbawionej wolności (art. 113a § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy, dalej: k.k.w.), ale nie może być ono realizowane inaczej niż za pośrednictwem zakładu karnego, co jednoznacznie wynika z powołanego przepisu k.k.w. Jednak osadzony może być pozbawiony tego prawa orzeczoną wobec niego karą dyscyplinarną (art. 143 § 1 pkt 5 k.k.w.).

Jednocześnie w tym przypadku zastosowania nie mają przepisy RODO. W myśl bowiem art. 2 ust. 2 lit. d RODO, ten akt prawa unijnego nie ma zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Skoro organizowanie zakupów w kantynie więziennej przez osoby pozbawione wolności pozostaje w związku z wykonywaniem tymczasowego aresztowania, kar pozbawienia wolności, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności, to do przetwarzania danych osobowych osób pozbawionych wolności przez podmioty organizujące takie zakupy powinny być stosowane przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Jednocześnie więzień nie może być uznany za klienta podmiotu organizującego zakupy w kantynie więziennej, ponieważ w tej sytuacji nie występuje, charakterystyczny dla prawa cywilnego, stosunek równości stron. Zatem osadzony, korzystając ze swojego prawa do dokonywania zakupów w kantynie więziennej, musi korzystać z usług podmiotu ją prowadzącego i może realizować swoje prawo jedynie na warunkach przez ten podmiot określonych, co jest jedną z konsekwencji – wykonywanej wobec niego – kary pozbawienia wolności.

Jednocześnie podmiot prowadzący kantynę więzienną jest prawnie zobowiązany do przetwarzania danych osobowych osób pozbawionych wolności dokonujących zakupów w tej kantynie więziennej jedynie w zakresie niezbędnym dla zapewnienia prawidłowego przeprowadzenia i rozliczenia tych zakupów (art. 13 ust. 1 ustawy

z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości).

Zgodnie z § 30 rozporządzenia Ministra Sprawiedliwości z dnia 28 grudnia 2017 r. w sprawie prowadzenia depozytu przedmiotów wartościowych i środków pieniężnych osób pozbawionych wolności, osadzeni dokonują zakupów w kantynie w sposób określony w porządku wewnętrznym, na podstawie paragonów. Depozytor umieszcza na paragonach następujące dane: 1) imię, nazwisko i imię ojca osadzonego; 2) numer ewidencyjny osadzonego; 3) wysokość depozytu pieniężnego pozostającego do dyspozycji osadzonego, według stanu na dzień dokonywania wydruku; 4) nazwę kary dyscyplinarnej związanej z prawem do dokonywania zakupów. Wymienione dane depozytor potwierdza na paragonie podpisem i imienną pieczątką. Z kolei dokonanie zakupów potwierdza podpisem na paragonach osadzony, osoba wydająca towary z kantyny oraz funkcjonariusz lub pracownik. Powołane przepisy stanowią też, że dział finansowy otrzymuje z kantyny oryginały paragonów wraz z ich zestawieniem, zawierającym w szczególności numer ewidencyjny osadzonego oraz wartość dokonanych przez niego zakupów.

W opinii organu nadzoru, opisane w pytaniu więźnia przetwarzanie danych osób dokonujących zakupów w kantynie więziennej przez podmiot ją prowadzący nie narusza obowiązujących przepisów, gdyż zakres przetwarzanych danych mieści się, w tym wskazany, w powołanych przepisach, a jednocześnie wydaje się adekwatny do realizowanego celu, tj. właściwej identyfikacji więźnia i rozliczenia dokonywanych przez niego zakupów ze środków pozostających do jego dyspozycji w więziennym depozycie.

Jednocześnie warto zaznaczyć, że na podmiocie prowadzącym kantynę i jego pracownikach ciąży obowiązek odpowiedniego zabezpieczenia danych osobowych pozyskiwanych w związku z zakupami w kantynie – zgodnie z art. 31 ust. 1 pkt 1 oraz art. 43 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

EDUKACJA

W ostatnim czasie Urząd Ochrony Danych Osobowych podjął szereg inicjatyw edukacyjnych, które wpisują się misję organu nadzorczego. Poprzez edukację i informację upowszechnia w społeczeństwie wiedzę o ochronie danych osobowych i ryzyku, a także o przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych oraz rozumienia tych zjawisk (ze szczególną uwagą poświęconą działaniom skierowanym do dzieci).

Raport „Ochrona danych osobowych w dobie pandemii”

Badanie pt. „Ochrona danych osobowych w czasie pandemii” zostało przeprowadzone na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów Biura Informacji Gospodarczej SA, którzy są organizatorami tego przedsięwzięcia, pod patronatem Urzędu Ochrony Danych Osobowych. Opracowanie ma na celu podniesienie świadomości społeczeństwa oraz jego dalsze edukowanie w zakresie ochrony danych osobowych. W prezentowanej publikacji zostały podniesione także kwestie ochrony danych osobowych, a także przedstawione problemy, z jakimi polskie społeczeństwo spotkało się w okresie między marcem 2020 r. a marcem 2021 r. w kontekście ochrony danych osobowych.

67 proc. badanych uważa, że w czasie pandemii jesteśmy bardziej narażeni na wyłudzenie naszych danych osobowych. Porównując odpowiedzi kobiet i mężczyzn, można zauważyć, że działalności oszustów znacznie bardziej obawiają się przedstawicielki płci pięknej (70 proc. do 65 proc.). Największe obawy mają młodzi ludzie między 25. a 34. r.ż. – prawie 72 proc.

Zdecydowana większość osób (84 proc.) zadeklarowała, że wie, jak zadbać o bezpieczeństwo swoich danych. W tym temacie panowie są pewniejsi niż panie – 85 proc. do 82 proc. Najwięcej wątpliwości mają osoby w wieku 35–44 (18 proc. nie wie) i 45-54 (ponad 19 proc. nie wie). Najpewniejsi są najmłodsi (18–24 lata) – blisko 89 proc.

Prawie 30 proc. badanych twierdzi, że w czasie pandemii otrzymała podejrzaną wiadomość skłaniającą do podjęcia czynności związanych z udostępnieniem danych. Najczęściej dotyczyło to osób w wieku 25–35 lata – prawie 38 proc.

Za pośrednictwem podejrzanych wiadomości respondenci byli proszeni zazwyczaj o kliknięcie w przesłany link (49 proc.), pobranie załącznika (44 proc.), wykonanie przelewu lub płatności (28 proc.) lub przekazania danych osobowych (26 proc.).

83 proc. badanych twierdzi, że wie, jak rozpoznać fałszywą wiadomość. Najpewniejsi własnych umiejętności są młodzi ludzie w wieku 18–24 (ponad 91 proc.) i 25–34 (89 proc.). Weryfikując otrzymane wiadomości, respondenci najczęściej sprawdzają adres mailowy nadawcy (66 proc.) lub numer telefonu w Internecie (55 proc.) i dokładnie czytają przysłaną wiadomość (53 proc.). W przypadku, gdy zorientują się, że otrzymana wiadomość jest próbą oszustwa, 60 proc. badanych po prostu ją usunie. Na policję sprawę zgłosiłoby ponad 54 proc. respondentów.

Co trzeci Polakach obawia się utraty danych w wyniku wycieku z bazy instytucji publicznych lub prywatnych firm. Co ciekawe, wśród najmłodszych (18–24 lata), tę obawę podziela tylko 19 proc. badanych. Znacznie bardziej boją się oni kradzieży danych w wyniku ataku hakerskiego na komputer lub telefon (32,5 proc. do 23 proc. ogółu). Największą obawą Polaków jest jednak utrata danych w wyniku wyłudzenia poprzez oszustwo (fałszywe telefony, e-maile, SMS-y). Boi się tego ponad 43 proc. obywateli.

Ponad 36 proc. badanych wykorzystuje jedno hasło do logowania w wielu miejscach. Co ciekawe, im starsi byli badani, tym ten odsetek był niższy.

Poznaj pełną treść raportu dostępną pod linkiem: https://uodo.gov.pl/pl/138/2021

Webinarium „Bezpieczeństwo cyfrowe dzieci i młodzieży a odpowiedzialność”

Urząd Ochrony Danych Osobowych wraz z Komendą Stołeczną Policji zorganizował wykład on-line, który odbył się 9 kwietnia 2021 r.. Spotkanie było okazją do przybliżenia zasad ochrony naszych danych w Internecie i zagrożeń, których musimy być świadomi.

Wykład ten był adresowany przede wszystkim do uczestników XI edycji programu edukacyjnego UODO dla szkół „Twoje dane – Twoja sprawa”. Podczas webinarium eksperci odpowiadali m.in. na pytania, jak odpowiedzialnie i świadomie korzystać z dostępnych narzędzi w celu ochrony siebie, swojego wizerunku i danych osobowych, a także opowiadali o konsekwencjach nierozważnych decyzji w cyfrowej rzeczywistości.

Zapis webinarium możesz obejrzeć pod linkiem: https://uodo.gov.pl/pl/458/1993

Seminarium naukowe „Sztuczna inteligencja – w kontekście ochrony danych osobowych”

Urząd Ochrony Danych Osobowych zorganizował seminarium naukowe na temat sztucznej inteligencji (SI). Temat ten jest niezwykle istotny z punktu widzenia ochrony danych osobowych w kontekście szybkiego rozwoju technologicznego, który dąży do zrewolucjonizowania otaczających nas realiów. Podczas wydarzenia zaznaczono, że ochrona danych osobowych nie jest przeciwnikiem sztucznej inteligencji, a jedynie wymaga legalności przetwarzania danych. Uczestnicy spotkania podjęli się także analizy przepisów rozporządzenia w sprawie wykorzystania SI.

Zobacz nagranie z seminarium naukowego dostępne pod linkiem: https://uodo.gov.pl/pl/138/2010

„RODO w szkolnej ławce. Przetwarzanie danych biometrycznych”

Pod koniec kwietnia 2021 r. odbyło się webinarium dotyczące przetwarzania danych biometrycznych, które służyło wyjaśnieniu definicji i pojęć, a także wytłumaczeniu, dlaczego należy zachować wzmożoną ostrożność przy przetwarzaniu danych, które powinny być szczególnie chronione – tym bardziej w odniesieniu do przetwarzania danych osobowych dzieci i młodzieży przez szkołę. Na podstawie analizy bieżących spraw oraz przepisów i wytycznych, eksperci UODO wskazali, na co należy zwracać uwagę przy przetwarzaniu danych biometrycznych.

Holandia: kara dla Booking.com za opóźnienie w zgłoszeniu naruszenia

Holenderski organ ochrony danych nałożył na Booking.com karę w wysokości 475 tys.euro, ponieważ spółka zbyt długo zwlekała ze zgłoszeniem naruszenia ochrony danych osobowych organowi nadzorczemu.

Gdy doszło do naruszenia, przestępcy uzyskali dane osobowe ponad 4 tys. klientów. W ręce oszustów wpadły również informacje o kartach kredytowych prawie 300 osób.

W oszustwie telefonicznym, wymierzonym w 40 hoteli zlokalizowanych w Zjednoczonych Emiratach Arabskich, w grudniu 2018 roku, wzięli udział pracownicy hoteli, którzy zostali nakłonieni przez przestępców do ujawnienia danych logowania do ich kont w systemie Booking.com. W ten sposób przestępcy uzyskali dostęp do danych 4109 osób, które zarezerwowały pokoje hotelowe w Zjednoczonych Emiratach Arabskich. Dane zawierały ich imiona, nazwiska, adresy i numery telefonów, a także szczegóły ich rezerwacji.
Ponadto przestępcy zdołali również uzyskać dostęp do informacji o kartach kredytowych 283 osób. W 97 przypadkach uzyskano również kod zabezpieczający kartę kredytową. Przestępcy, podając się za pracowników Booking.com, próbowali również uzyskać w e-mailach lub podczas rozmów telefonicznych informacje o kartach kredytowych innych ofiar.

Naruszenie zgłoszone o 22 dni za późno

Booking.com został poinformowany o naruszeniu ochrony danych osobowych 13 stycznia 2019 r., ale nie zgłosił organowi nadzorczemu tego zdarzenia do 7 lutego 2019 r., co stanowi 22-dniowe opóźnienie. Tymczasem naruszenia ochrony danych osobowych muszą być zgłaszane w ciągu 72 godzin. Z kolei 4 lutego 2019 r. Booking.com poinformował o naruszeniu tych klientów, których dotyczyło naruszenie. Spółka podjęła również inne środki w celu zrekompensowania spowodowanych jej działaniem szkód, np. zaoferowała odszkodowania za wszelkie poniesione straty.

Międzynarodowe postępowanie

Postępowanie w sprawie naruszenia w Booking.com miało charakter międzynarodowy. Sytuacja dotyczyła spółki międzynarodowej, którego klienci pochodzą z wielu państw. Ponieważ główna siedziba Booking.com znajduje się w Holandii, dlatego też postępowanie prowadził holenderski organ nadzorczy. Ponieważ sprawa miała charakter międzynarodowy, organ nadzorczy koordynował postępowanie z innymi europejskimi organami nadzorczymi.

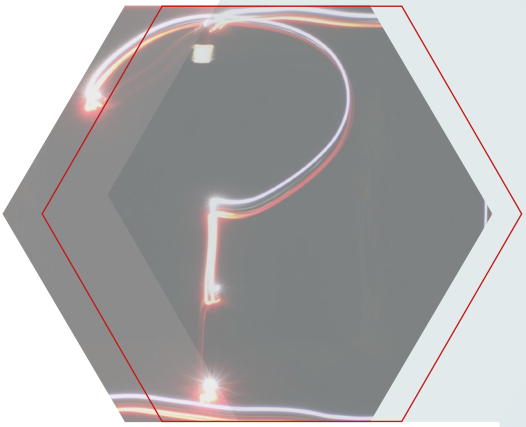
Obowiązek zgłaszania naruszeń ochrony danych osobowych

Obowiązek zgłaszania naruszeń ochrony danych osobowych oznacza, że zarówno przedsiębiorstwa prywatne, jak i organy publiczne muszą bez zbędnej zwłoki (a w każdym razie nie później niż w przeciągu 72 godzin) poinformować organ nadzorczy, jeśli dojdzie do poważnego naruszenia ochrony danych. W niektórych przypadkach muszą one również poinformować osoby, których dane osobowe zastały naruszone. Naruszenia danych należy zgłaszać do wskazanego punktu ds. naruszeń w organie nadzorczym.

Źródło: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-bookingcom-delay-reporting-data-breach_en

O obowiązkach administratora odnoszących się do naruszeń ochrony danych osobowych przeczytasz więcej w artykule pt. „O obowiązkach administratora odnoszących się do naruszeń ochrony danych osobowych". Patrz str. 2.

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW



Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych" w sekcji „Zadania IOD" została wzbogacona o kolejne zagadnienia.

Wyjaśnienia dotyczą takich kwestii, jak:

Która przesłanka jest podstawą przetwarzania danych przez pracodawcę stosującego monitoring?

Czy w jednostkach organizacyjnych samorządu terytorialnego funkcjonuje kilku odrębnych administratorów?

Jaka jest podstawa przetwarzania danych studentów, którym udziela się pomocy materialnej?

URZĄD OCHRONY DANYCH OSOBOWYCH