Nr 5/2022 (38)
Maj 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

PREZES UODO NIE MOŻE NAKAZAĆ UJAWNIENIA DANYCH OSOBOWYCH OSOBIE TRZECIEJ

W aktualnym stanie prawnym Prezes UODO nie ma uprawnień do nakazania administratorowi lub podmiotowi przetwarzającemu udostępnienia danych osobowych osobie trzeciej.

Na mocy RODO (art. 58) każdemu organowi nadzorczemu, a więc również Prezesowi UODO, przysługują uprawnienia do prowadzenia postępowań, naprawcze, do nakładania kar, do udzielania zezwoleń, doradcze, do zgłaszania naruszeń organom wymiaru sprawiedliwości oraz do udziału w postępowaniu sądowym.

Brak wśród uprawnień żądania udostępnienia danych osobowych osoby trzeciej

Wśród ww. nie ma uprawnienia do nakazania administratorowi lub podmiotowi przetwarzającemu ujawnienia danych osobowych osobie trzeciej.

Takiego uprawnienia nie można też wywieść z art. 58 ust. 2 lit. c RODO. Na jego podstawie organ nadzorczy ma prawo do nakazania administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO. Tym żądaniem może więc być prawo dostępu do danych, prawo do sprostowania danych, prawo do usunięcia danych, prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych oraz prawo do sprzeciwu i niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu. Podkreślić jednak należy, że przepisy RODO ujmują prawa osób, których dane dotyczą, w sposób wyczerpujący. Nie ma wśród nich żądania udostępnienia danych osobowych osoby trzeciej.

Nie ma także przepisów krajowych, które umożliwiałyby organowi nadzorczemu takie działanie.

Wspólne stanowisko organów nadzorczych innych państw UE

Jednocześnie warto dodać, że biorąc pod uwagę zasadę jednolitości prawa Unii Europejskiej, organy nadzorcze innych państw UE (hiszpański, rumuński, francuski, bułgarski, estoński, włoski i szwedzki) zgodnie uznały, że nie mają możliwości wydawania rozstrzygnięć nakazujących udostępnienie danych osobowych osób trzecich w oparciu o przepisy RODO.

Zatem gdy do UODO wpływają skargi na nieudostępnienie danych osobowych osoby trzeciej, a które zawierają wniosek o nakazanie udostępnienia takich danych, organ nadzorczy wydaje postanowienia o odmowie wszczęcia postępowania. Działania podejmowane przez Prezesa UODO nie mogą bowiem wykraczać poza jego kompetencje.

Potwierdzone orzecznictwem

Stanowisko takie zostało potwierdzone w orzecznictwie. Przykładem jest m.in. sprawa, w której Prezes UODO odmówił wszczęcia postępowania w związku ze skargą na odmowę udostępnienia przez pracodawcę danych osobowych pracownika (m.in. jego adresu zamieszkania oraz numeru PESEL) osobie, która potrzebowała ich,

by spełnić wszystkie wymogi formalne pozwu o ochronę dóbr osobistych.

W zapadłym na jej kanwie 11 czerwca 2021 r. wyroku (sygn. akt II SA/Wa 456/21) Wojewódzki Sąd Administracyjny w Warszawie wskazał, że: „z punktu widzenia gwarancyjnego, jedynym celem RODO jest zagwarantowanie osobie fizycznej odpowiedniej ochrony jej danych osobowych, a nie przyznawanie uprawnień informacyjnych innym podmiotom.

W szczególności przepisy RODO nie dają uprawnień informacyjnych podmiotom, które zamierzają wytaczać powództwa osobom fizycznym, których dane osobowe objęte są ochroną. Co szczególnie istotne w aspekcie rozstrzyganej sprawy, przepisy analizowanej regulacji nie dają takich uprawnień także organowi nadzoru. Prezes UODO nie może więc żądać od administratora danych osobowych ich ujawnienia osobie trzeciej, na potrzeby ewentualnego postępowania sądowego.

Wbrew twierdzeniom Skarżącej takiego uprawnienia nie sposób też wywieść z art. 6 ust. 1 pkt. f) RODO. Ten przepis stanowiłby dla strony postępowania podstawę prawną do przetwarzania konkretnych danych osobowych w sytuacji, gdyby strona skarżąca była już w posiadaniu tych danych. Powyższa norma nie daje jednak Skarżącej uprawnienia do pozyskania takich danych osobowych bezpośrednio, czy też za pośrednictwem Prezesa UODO. Uprawnienie takie nie wynika też z treści art. 58 ust. 1 pkt. a) RODO. Ten przepis dotyczy wyłącznie zakresu zadań organu nadzorczego. Nie precyzuje jednak tych zadań, a w szczególności, nie sposób z niego wywieść, by organ nadzorczy mógł zobowiązywać administratora danych do ich ujawniania osobom trzecim.

W ocenie tut. Sądu, omawianego uprawnienia nie sposób również odkodować z treści art. 58 ust. 2 pkt. c) RODO. Mianowicie zgodnie z tym przepisem, Prezesowi UODO przysługuje uprawnienie naprawcze w postaci prawa do nakazania administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia. (…)

Żądanie udostępnienia danych osobowych osoby trzeciej nie zostało ujęte także wśród praw osób, których dane dotyczą. (…)

Zmiany w przepisach po 25 maja 2018 r.

Jednocześnie zauważyć należy, że przed 25 maja 2018 r. polski organ nadzorczy uznawał się za kompetentny do wydawania ww. nakazów w zakresie udostępnienia danych osobowych osoby trzeciej, na podstawie art. 18 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.). Artykuł ten wskazywał, że polski organ ochrony danych osobowych, w przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych, „w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem", w tym mógł nakazać „uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych". Obecnie polska ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2019 r. poz. 1781 t.j.) nie zawiera podobnych przepisów i takich kompetencji nie przewiduje. (…)

W świetle powyższego, jako poprawną należało przyjąć konkluzje organu o niemożliwości wszczęcia niniejszego postępowania. Skoro bowiem przepisy prawa uniemożliwiały organowi merytoryczne rozpoznanie wniosku inicjującego postępowanie, to oczywistym było, że organ nie mógłby wydać decyzji zobowiązującej Spółki jako administratora danych osobowych do podjęcia działań żądanych przez Stronę".

Podobne stanowisko Wojewódzki Sąd Administracyjny w Warszawie wyraził w wyroku z 27 listopada 2020 r. (sygn.. akt II SA/Wa 1542/20).

WYKORZYSTYWANIE ZWOLNIENIA LEKARSKIEGO PRZEZ PRACOWNIKA – KONTROLA FIRMY ZEWNĘTRZNEJ

Pracodawca ma możliwość zlecenia podmiotowi zewnętrznemu przeprowadzenia kontroli wykorzystania zwolnienia lekarskiego przez pracownika. Ważne jest jednak, by udostępnienie jego danych osobowych odbyło się na podstawie umowy powierzenia i z poszanowaniem zasady minimalizacji danych. Osoby przeprowadzające kontrolę powinny też mieć imienne upoważnienie, które uprawnia do jej wykonywania.

Kwestię kontroli przez pracodawcę nieobecności pracowników w pracy z powodu choroby lub konieczności sprawowania opieki nad chorym dzieckiem lub innym chorym członkiem rodziny regulują ustawa z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa oraz rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu kontroli prawidłowości wykorzystywania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich.

Stosownie do art. 68 ust. 1 powołanej ustawy Zakład Ubezpieczeń Społecznych oraz płatnicy składek, o których mowa w art. 61 ust. 1 pkt 1 (tj. tacy, którzy zgłaszają do ubezpieczenia chorobowego powyżej 20 ubezpieczonych), są uprawnieni do kontrolowania ubezpieczonych co do prawidłowości wykorzystywania zwolnień od pracy zgodnie z ich celem oraz są upoważnieni do formalnej kontroli zaświadczeń lekarskich.

Przeprowadzenie kontroli ws. zwolnień lekarskich przez pracodawcę

Pracodawca uprawniony do kontroli prawidłowości wykorzystywania zwolnień lekarskich od pracy może taką kontrolę przeprowadzić sam lub upoważnić do tego swoich pracowników bądź zlecić jej przeprowadzenie podmiotowi zewnętrznemu. Jeśli korzysta z tego ostatniego rozwiązania, ważne jest, by z podmiotem, któremu zleca takie zadanie, zawarł umowę powierzenia przetwarzania danych osobowych.

Pamiętać przy tym trzeba o poszanowaniu zasady minimalizacji danych w rozumieniu art. 5 ust. 1 lit. c RODO. W praktyce oznacza to m.in., że osobie kontrolującej nie można przekazać informacji o przyczynie wydania zwolnienia lekarskiego, a także nie ma ona prawa wymagać od osoby kontrolowanej podania informacji na temat swojego stanu zdrowia.

Co ważne, pracodawca, który zlecił podmiotowi zewnętrznemu przeprowadzenie kontroli, nadal pozostaje administratorem danych osobowych swoich pracowników i jest odpowiedzialny za to, by były one przetwarzane zgodnie z przepisami o ochronie danych osobowych.

Zaznaczyć też należy, że godnie z § 8 wymienionego rozporządzenia Ministra Pracy i Polityki Socjalnej osobie kontrolującej prawidłowość wykorzystywania zwolnień lekarskich od pracy płatnik składek wystawia imienne upoważnienie według wzoru stanowiącego załącznik nr 1 do rozporządzenia. Upoważnienie jest ważne łącznie z legitymacją pracowniczą albo dokumentem tożsamości, których numery powinny być podane

w upoważnieniu. Uprawnia ono do wykonywania kontroli w miejscu zamieszkania, miejscu czasowego pobytu lub miejscu zatrudnienia osoby kontrolowanej.

Prowadzenie tego typu kontroli nie wymaga zgody pracowników

Dopuszczalność takiego postępowania została potwierdzona w decyzji Prezesa UODO (ZSZZS.440.727.2018), który po rozpoznaniu wniesionej skargi uznał, że pracodawca, zlecając firmie zewnętrznej przeprowadzenie kontroli zasadności wykorzystania zwolnienia lekarskiego przez Skarżącą skorzystał z przysługującego mu uprawnienia określonego w art. 68 ust. 1 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa oraz w § 1 rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu kontroli prawidłowości wykorzystania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich. Jak podkreślił, „kontrola została przeprowadzona przez podmiot, z którym Spółka [tj. pracodawca] (...) zawarła umowę określającą warunki współpracy w zakresie realizacji usług związanych z kontrolą dotyczącą absencji chorobowych pracowników i doradztwa w tym zakresie oraz umowę powierzenia przetwarzania danych osobowych. (...) W ocenie Prezesa Urzędu Ochrony Danych Osobowych nie ma podstaw do stwierdzenia, iż dane osobowe Skarżącej były przetwarzane przez Spółkę [tj. pracodawcę] w sposób niezgodny z RODO. Skarżony proces znajdował bowiem oparcie w art. 28 RODO w zw. z przesłankami określonymi w art. 6 ust. 1 lit. b) i c) RODO w zakresie tzw. zwykłych danych tj. imienia, nazwiska i adresu zamieszkania oraz art. 9 ust. 2 lit. b) RODO w zakresie danych dot. stanu zdrowia Skarżącej”.

DO PRACY PRZY WYTWARZANIU LUB HANDLU BRONIĄ I AMUNICJĄ POTRZEBNA POZYTYWNA OPINIA POLICJI

Przepisy szczególne nakładają na przedsiębiorców obowiązek weryfikacji pracowników dopuszczonych do pracy przy wytwarzaniu materiałów wybuchowych, broni, amunicji oraz wyrobów o przeznaczeniu wojskowym lub policyjnym, jak również przy ich obrocie.

Zasady podejmowania i wykonywania przez przedsiębiorców działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym oraz kontroli tej działalności regulują przepisy ustawy z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym.

Stanowią one m.in., że bezpośrednio do pracy, zarówno przy wytwarzaniu materiałów wybuchowych, broni, amunicji oraz wyrobów o przeznaczeniu wojskowym lub policyjnym, jak również przy ich obrocie, może być

dopuszczona jedynie osoba, która posiada pozytywną opinię Policji, a w przypadku obywatela innego państwa – organu odpowiedniego szczebla i kompetencji w tym państwie właściwego ze względu na miejsce stałego pobytu (art. 28 ust. 1 pkt 3 i art. 29 ust. 1 pkt 3). Opinię Policji wydaje, w drodze postanowienia, komendant powiatowy Policji właściwy ze względu na miejsce stałego pobytu osoby opiniowanej. Od postanowienia w sprawie opinii służy zażalenie do właściwego komendanta wojewódzkiego Policji (art. 28 ust. 2 oraz art. 29 ust. 2).

Przy zatrudnieniu oraz w trakcie trwania zatrudnienia przedsiębiorca jest obowiązany weryfikować spełnianie przez pracownika wymagań, o których mowa w art. 28 ust. 1 i art. 29 ust. 1 (art. 30 ust. 1). Natomiast raz na 5 lat występuje o aktualną opinię Policji (lub w przypadku obywatela innego państwa – organu odpowiedniego szczebla i kompetencji w tym państwie) dotyczącą pracownika (art. 30 ust. 4). Powołane przepisy nakładają zatem na przedsiębiorcę obowiązek dokonywania weryfikacji pracowników dopuszczonych do pracy przy wytwarzaniu materiałów wybuchowych, broni, amunicji oraz wyrobów o przeznaczeniu wojskowym lub policyjnym, jak również przy ich obrocie. Przejawem tej weryfikacji jest m.in. wystąpienie z wnioskiem o wydanie opinii przez Policję.

KARY

Belgia: kara za kontrole temperatury na lotnisku w Brukseli w ramach walki z COVID-19

Izba odwoławcza belgijskiego organu nadzorczego nałożyła na Port Lotniczy Bruksela i Ambuce Rescue Team administracyjne kary pieniężne w wysokości odpowiednio 200 tys. euro i 20 tys. euro. Oba podmioty ukarano za przeprowadzanie kontroli temperatury pasażerów oraz za przetwarzanie szczególnych kategorii danych osobowych (danych dotyczących zdrowia).

Kamery termowizyjne zostały użyte do sprawdzenia, czy pasażerowie na lotnisku w Brukseli mieli temperaturę ciała 38 stopni Celsjusza lub wyższą. Jeśli temperatura okazała się wyższa, byli poddawani drugiej kontroli (przeprowadzonej przez organizację o nazwie Ambuce Rescue Team). Wówczas musieli wypełnić kwestionariusz dotyczący ewentualnych objawów koronawirusa i innych danych dotyczących zdrowia.

To przetwarzanie szczególnych kategorii danych osobowych (danych o zdrowiu) miało miejsce w okresie od czerwca 2020 r. do stycznia 2021 r. i miało związek z pandemią Covid-19.

Belgijski organ nadzorczy ustalił w trakcie postępowania, że administratorzy nie dysponowali ważną podstawą prawną (art. 6 ust. 1 i 9 ust. 2 RODO). Przetwarzanie danych opierało się głównie na protokole, który zdaniem organu nadzorczego nie spełniał wymogów wyżej wymienionych przepisów – ani reżimu art. 6 ust. 3 RODO, ani orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej („Privacy International"). W szczególności organ podkreślił, że protokół nie jest wiążący w świetle prawa krajowego.

Zwrócił też uwagę, że nie wykazano konieczności przetwarzania gromadzonych danych osobowych w celu wypełnienia obowiązku prawnego lub zadania realizowanego w interesie publicznym. Ponadto stwierdzono, że powołana podstawa prawna nie była jasna, precyzyjna i przewidywalna oraz nie określała wyraźnie celu i innych warunków przetwarzania.

Jeden z administratorów naruszył art. 12–14 RODO z powodu braku zapewnienia przejrzystości wobec osób, których dane dotyczą. W polityce prywatności administratora nie wymieniono podstawy prawnej przetwarzania danych.

Co więcej, administratorzy nie przeprowadzili oceny skutków dla ochrony danych w odniesieniu do drugiej części przetwarzania, tj. gromadzenia danych dotyczących zdrowia za pomocą pisemnego kwestionariusza i przechowywania tych danych przez okres pięciu lat. Belgijski organ nadzorczy uznał, że tę drugą część przetwarzania należy uznać za przetwarzanie na dużą skalę szczególnych kategorii danych. W związku z tym – w ocenie organu – wymagane jest przeprowadzenie oceny skutków dla ochrony danych.

Źródło: decyzja belgijskiego organu (w języku niderlandzkim)

Irlandia: kara dla banku m.in. za zaniedbania w zakresie bezpieczeństwa przetwarzania

Irlandzki organ nadzorczy nałożył na Bank of Ireland Group plc administracyjne kary pieniężne za naruszenie art. 32 ust. 1 RODO oraz za niektóre naruszenia art. 33 i 34 RODO. Łączna kwota nałożonych administracyjnych kar pieniężnych wyniosła 463 tys. euro.

Bankowi nakazano również dostosowanie przetwarzania danych do art. 32 ust. 1 RODO, poprzez wprowadzenie zmian w środkach technicznych i organizacyjnych. W przedmiotowej decyzji Bankowi udzielono upomnienia w odniesieniu do wszystkich naruszeń art. 33, 34 i 32 ust. 1 RODO w niej wskazanych. Przedmiotowe postępowanie zostało wszczęte w związku z 22 zgłoszeniami naruszeń ochrony danych osobowych, które Bank przekazał Komisji Ochrony Danych (Data Protection Commission) w okresie od listopada 2018 r. do czerwca 2019 r. Zgłoszenia dotyczyły nieprawidłowości w przekazie danych Banku do Centralnego Rejestru Kredytowego (CCR), tj. scentralizowanego systemu, który gromadzi i bezpiecznie przechowuje informacje kredytowe. Incydenty obejmowały nieuprawnione ujawnienie danych osobowych klientów poprzez przekazanie ich do CCR oraz przypadkowe zmiany danych osobowych klientów w samym CCR.

W decyzji stwierdzono:
- naruszenie przez Bank art. 33 RODO w 17 przypadkach. W niektórych z nich art. 33 ust. 1 został naruszony poprzez brak zgłoszenia przez Bank naruszenia ochrony danych osobowych bez zbędnej zwłoki. Naruszeniem art. 33 ust. 3 było również nieprzekazanie przez Bank do DPC wystarczających szczegółów dotyczących niektórych naruszeń ochrony danych osobowych;

- naruszenie przez Bank art. 34 RODO w 14 przypadkach. Naruszenia te dotyczyły nieprzekazania przez Bank komunikatów osobom, których dane dotyczą, bez zbędnej zwłoki w okolicznościach, w których naruszenia danych osobowych mogły spowodować wysokie ryzyko dla praw i wolności osób, których dane dotyczą; oraz

- naruszenie art. 32 ust. 1 RODO, ponieważ Bank nie wdrożył odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka, jakie stanowiło przetwarzanie przez niego danych klientów podczas przekazywania informacji do CCR.

Źródło: decyzja organu irlandzkiego

Szwecja: problemy z komunikacją doprowadziły do ukarania banku

Szwedzki organ nadzorczy nałożył na Klarna Bank AB administracyjną karę pieniężną w wysokości ok. 724 tys. euro za uchybienia stwierdzone podczas postępowania.

W trakcie prowadzonego przez organ postępowania wyjaśniającego Spółka dokonywała ciągłych zmian w informacjach na temat sposobu przetwarzania danych osobowych. Decyzja szwedzkiego organu nadzorczego dotyczy informacji przekazanych wiosną 2020 roku.

Spółka nie dostarczyła informacji dotyczących celu i podstawy prawnej przetwarzanych danych w związku z jedną z usług firmy, jak również przekazywała niepełne i wprowadzające w błąd informacje o tym, kto był odbiorcą różnych kategorii danych osobowych, gdy dane były udostępniane szwedzkim i zagranicznym podmiotom zajmującym się informacją kredytową.
Spółka nie poinformowała również o tym, do których krajów poza UE/EOG dane osobowe były przekazywane oraz gdzie i w jaki sposób osoby fizyczne mogły uzyskać informacje o zabezpieczeniach stosowanych przy przekazywaniu danych do państw trzecich. Szwedzki organ nadzorczy wskazał również, że Spółka dostarczyła niepełne informacje na temat praw osób, których dane dotyczą, w tym prawa do usunięcia danych, prawa do przenoszenia danych oraz prawa do sprzeciwu wobec sposobu przetwarzania danych osobowych.

Spółka naruszyła podstawową zasadę przejrzystości oraz prawa do informacji przysługującego osobom, których dane dotyczą, tj. art. 5 ust. 1 lit. a), art. 5 ust. 2, art. 12 ust. 1, art. 13 ust. 1 lit. c, e, f i art. 13 ust. 2 lit. a), b) i f) oraz 14 ust. 2 lit. g) RODO. Szwedzki organ nadzorczy stoi na stanowisku, że nie są to drobne naruszenia i na Spółkę musi zostać nałożona administracyjna kara pieniężna za wspomniane naruszenia.

Źródło: decyzja szwedzkiego organu nadzorczego

Hiszpania: operatorów telefonii komórkowej ukarano za utratę poufności związaną z duplikowaniem kart SIM

Hiszpański organ nadzorczy dowiódł, że środki zastosowane przez kilku operatorów telefonii komórkowej były niewystarczające, co doprowadziło do utraty poufności danych i przekazania danych osobowych osobom trzecim. W rezultacie operatorzy zostali ukarani administracyjnymi karami pieniężnymi.

Do hiszpańskiego organu nadzorczego (dalej: „AEPD") wpłynęły skargi w związku z wydawaniem duplikatów kart SIM (Subscriber Identity Module) osobom trzecim, niebędącym abonentami. W wyniku tego abonenci nie tylko zostali pozbawieni dostępu do usług, ale również osoby trzecie uzyskały dostęp do ich kont bankowych.

AEPD ustalił, że dochodziło do popełniania czynów zabronionych, które polegały na tworzeniu duplikatów kart SIM bez wiedzy ich uprawnionych posiadaczy, co skutkowało uzyskaniem dostępu do poufnych informacji przez osoby trzecie i możliwością popełniania przez te osoby przestępstw na szkodę osób, do których numer karty był zgodnie z prawem przypisany (tzw. SIM Swapping).

AEPD przeprowadził postępowania, mające na celu przeanalizowanie procedur stosowanych przy zarządzaniu wnioskami o zmianę karty SIM przez skarżonych operatorów telefonii komórkowych.

Przedmiotem tych postępowań była identyfikacja słabych punktów we wdrożonych procedurach operacyjnych, wykrycie przyczyn, dla których takie przypadki mogą mieć miejsce, jak również znalezienie punktów niezgodności, wymagających poprawy lub dostosowania, w celu ustalenia odpowiedzialności, zmniejszenia ryzyka i zwiększenia bezpieczeństwa przetwarzania danych osobowych osób, których dotyczą.

Dane, które są przetwarzane w celu wydania duplikatu karty SIM oraz karty SIM, która jednoznacznie

identyfikuje abonenta w sieci, są danymi osobowymi, a ich przetwarzanie musi podlegać przepisom o ochronie danych osobowych.

Stwierdzono, że środki zastosowane przez operatorów były niewystarczające, co doprowadziło do utraty poufności danych i przekazania danych osobowych osobom trzecim.

W związku z powyższym AEPD nałożył administracyjne kary pieniężne za naruszenie poufności danych na:

- XFERA MÓVILES, S.A., w wysokości 200 tys. euro;
- ORANGE ESPAGNE, S.A.U. w wysokości 700 tys. euro;
- TELEFÓNICA MÓVILES ESPAÑA, S.A.U. w wysokości 900 tys. euro;
- ORANGE ESPAÑA VIRTUAL, S.L w wysokości 70 tys. euro.

Za naruszenia poufności danych oraz zasady rozliczalności organ nadzorczy nałożył na VODAFONE ESPAÑA, S.A.U. administracyjną karę pieniężną w wysokości 3,9 mln euro.

Decyzje w języku hiszpańskim:

Xfera Móviles

Orange Espagne

Telefónica Móviles España

Orange España Virtual

Vodafone España

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

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

Wyjaśnienia dotyczą takich kwestii, jak:

Czy administrator może przerzucać swoje obowiązki na IOD?

Czy okręgowa izba inżynierów budownictwa może udostępnić inwestorowi dane projektanta?

Na co zwrócić szczególną uwagę przy powierzeniu danych osobowych w sektorze medycznym?

URZĄD OCHRONY DANYCH OSOBOWYCH