Obserwuj nas na:

Nr 8/2020 (17)
Sierpień 2020

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH



str. 2 ..... **NEWSLETTER JEST SKUTECZNĄ FORMĄ PRZEKAZYWANIA WIEDZY - WYNIKI ANKIETY**

str. 3 ..... **OŚWIADCZENIA O NIEKARALNOŚCI WYMAGANE W POSTĘPOWANIACH PRZETARGOWYCH**

str. 4 ..... **KTO JEST ODBIORCĄ DANYCH**

str. 6 ..... **KIEROWCA AUTOBUSU NIE POWINIEN POZNAĆ DANYCH OSOBY, KTÓRA ZŁOŻYŁA NA NIEGO SKARGĘ**

str. 6 ..... **DOTOWANIE PODMIOTÓW PROWADZĄCYCH ŻŁOBEK LUB KLUB DZIECIĘCY**

str. 7 ..... **PROWADZENIE REJESTRU AKCJONARIUSZY**

str. 8 ..... **W JAKIM JĘZYKU PROWADZIĆ KOMUNIKACJĘ WS. OCHRONY DANYCH**

str. 9 ..... **PUBLIKACJA DANYCH OSOBOWYCH ZAWARTYCH W RECENZJACH ROZPRAW DOKTORSKICH**

str. 11 ..... **PODSUMOWANIE KONSULTACJI PROJEKTU WYMOGÓW AKREDYTACJI**

str. 11 ..... **TRZY NOWE WNIOSKI O ZATWIERDZENIE KOLEJNYCH KODEKSÓW POSTĘPOWANIA**

str. 12 ..... **MIĘDZYNARODOWE**

- Co po brexicie? KE przygotowała informacje na ten temat

str. 12 ..... **KARY**

- Belgia: dwie kary za działania marketingowe
- Hiszpania: kara za brak odpowiedzi na wniosek o udzielenie informacji
- Finlandia: trzy kary za niewystarczającą informację o prawach osób

str. 15 ..... **NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW**

NEWSLETTER JEST SKUTECZNĄ FORMĄ PRZEKAZYWANIA WIEDZY – WYNIKI ANKIETY

Szanowni Państwo,
serdecznie dziękujemy za zaangażowanie i czas poświęcony na wypełnienie ankiety ewaluacyjnej „Newsletter UODO dla IOD". Wpłynęło do nas prawie 950 odpowiedzi!

W ankiecie zapytaliśmy Państwa m.in., co sądzicie o newsletterze, w jakim stopniu zwiększył on Państwa wiedzę na temat stosowania zasad ochrony danych osobowych w codziennej pracy, jaki jest poziom merytoryczny prezentowanych artykułów. Ponadto zapytaliśmy Państwa o preferencje dotyczące prezentowanych treści, częstotliwość wydań czy jakość poszczególnych jego elementów.

Poniżej prezentujemy najważniejsze wnioski z badań.

Ogólna ocena newslettera
Prawie ¾ inspektorów ochrony danych wystawiło newsletterowi ocenę wysoką i bardzo wysoką. Jedynie dla ok. 2 proc. nie spełnia on oczekiwań.

Dla prawie 93 proc. odpowiadających newsletter jest skuteczną formą przekazywania wiedzy. Jedynie nieco ponad 6 proc. się z tym nie zgadza.

Dla prawie 60 proc. respondentów publikowane treści informacyjne w newsletterze i na stronie uodo.gov.pl są wystarczające.

Prawie 63 proc. badanych uznało przydatność informacji zawartych w newsletterze za wysoką i bardzo wysoką. Niecałe 4 proc. uznało ją za niską.

Dla niemal 73 proc. ankietowanych merytoryczna treść artykułów jest bardzo wysoka i wysoka. Jedynie nieco ponad 1,5 proc. uważa ją za niską.

Prawie 67 proc. osób odpowiedziało, że newsletter zwiększył ich wiedzę na temat stosowania zasad RODO w codziennej pracy. Tylko nieco ponad 3,5 proc. uznało, że w ogóle nie zwiększył.

Najbardziej interesujące informacje
Badanie pokazało, że dla 9 na 10 respondentów najbardziej interesującymi informacjami podawanymi w newsletterze są kolejno: odpowiedzi na pytania dla IOD (92,5 proc.), porady ekspertów (90 proc.), stanowiska Prezesa UODO (88 proc.) oraz artykuły problemowe (87 proc.). Mniejszym zainteresowaniem cieszą się informacje o karach, nie mniej jedynie 11 proc. uznaje ten temat za mniej interesujący oraz sprawy międzynarodowe.

Częstotliwość wydań newslettera
Dla 6 na 10 pytanych częstotliwość wydań jest dobra. Dla co trzeciej osoby newsletter wydawany jest zbyt rzadko. Państwa odpowiedzi wskazywały potrzebę zwiększenie częstotliwości wydań newslettera do jednego w tygodniu.

Przeanalizowaliśmy także Państwa sugestie odnośnie do zmiany układu i treści zamieszczanych w newsletterze.

Kluczowe wnioski przedstawiamy poniżej.
- równowaga w podziale na sektory: publiczny i prywatny;
- podział informacji wg branż;
- nowe treści, tworzone specjalnie na potrzeby newslettera, niezamieszczane na stronie www.uodo.gov.pl;
- zmniejszenie ilości informacji międzynarodowych.

W pytaniach otwartych sugerowali Państwo konkretne tematy i zagadnienia, na które UODO powinien zwrócić szczególną uwagę. Bardzo za to dziękujemy i z pewnością wykorzystamy je przy okazji kolejnych wydań newslettera. **Zgodnie z Państwa oczekiwaniami, sukcesywnie będziemy odnosić się do Państwa propozycji zmian. Już od tego numeru nieco poprawiliśmy szatę graficzną i zamieszczamy materiały, które w newsletterze mają swoją premierę wydawniczą.**

Bardzo dziękujemy za wszystkie miłe słowa, docenienie naszego wkładu pracy, który ułatwia funkcjonowanie Inspektorów w codziennej pracy. Cieszy nas fakt, że newsletter jest potrzebnym i ważnym źródłem informacji do interpretacji przepisów prawnych, a także przydatną formą poszerzania Państwa wiedzy. Dzięki Państwa pomocy jesteśmy przekonani, że będzie jeszcze lepiej spełniał oczekiwania i odpowiadał na realne problemy, z którymi stykacie się Państwo na co dzień.

Pozdrawiamy
Departament Komunikacji Społecznej UODO



OŚWIADCZENIA O NIEKARALNOŚCI WYMAGANE W POSTĘPOWANIACH PRZETARGOWYCH

Samo oświadczenie, iż wszyscy członkowie zarządu/wspólnicy spełniają wymóg niekaralności, nawet jeśli nie zawiera ono ich imion i nazwisk, uznać należy za dokument zawierający dane osobowe. Dla ich legalnego przetwarzania niezbędne jest spełnienie wymagań określonych w art. 10 RODO.

Niektórzy zamawiający w ramach zapytań ofertowych, które nie są przeprowadzane w trybie przewidzianym ustawą z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych, wymagają od oferentów złożenia oświadczenia, iż członkowie organów/wspólnicy nie zostali prawomocnie skazani za popełnienie niektórych kategorii przestępstw (np. przeciwko obrotowi gospodarczemu). Te wymagane – pod rygorem dopuszczenia do udziału w postępowaniu ofertowym – dokumenty mają mieć formę albo oświadczeń indywidualnych od poszczególnych osób (członków organów/wspólników) lub jednego oświadczenia zbiorczego składanego w imieniu całego zarządu i wspólników.

W związku z tym Prezesowi UODO sygnalizowane są wątpliwości dotyczące podstawy prawnej pozyskiwania tego typu dokumentów, które rodzą się w kontekście art. 10 RODO.

Dane osobowe – definicja, opinie i orzecznictwo

W opinii Prezesa UODO, istotne dla wyjaśnienia powyższych wątpliwości jest ustalenie, czy w tej sytuacji mamy do czynienia z danymi osobowymi. Niekiedy zależy to od wielu czynników i wymaga pogłębionej analizy.

Zgodnie bowiem z art. 4 pkt 1 RODO, danymi osobowymi są „wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej".

W swojej opinii nr 4/2007 w sprawie pojęcia danych osobowych Grupa Robocza Art. 29 podpowiada, że: „w przypadkach gdy celem przetwarzania jest identyfikacja osób, można przypuszczać, że administratorzy lub inne zainteresowane osoby dysponują sposobami, „jakimi można się posłużyć" w celu zidentyfikowania osoby, której dane dotyczą. Twierdzenie, że osoby nie są możliwe do zidentyfikowania, podczas gdy celem przetwarzania danych jest właśnie ich identyfikacja, zawierałoby wewnętrzną sprzeczność. Dlatego informacje takie należy uważać za dotyczące osób możliwych do zidentyfikowania, a przetwarzanie ich powinno podlegać przepisom dotyczącym ochrony danych."

Dla rozstrzygnięcia przedstawianych wątpliwości pomocne może być również orzeczenie TSUE z 20 grudnia 2017 r. w sprawie C-434/16 Peter Nowak przeciwko Data Protection Commissioner. TSUE opowiedział się w nim za szerokim rozumieniem pojęcia danych osobowych: „Użycie w zawartej w art. 2 lit. a) dyrektywy 95/46 definicji danych osobowych wyrażenia wszelkie informacje odzwierciedla bowiem przyświecający unijnemu prawodawcy zamiar przypisania temu pojęciu szerokiego zakresu, nie ograniczając go do informacji wrażliwych czy też prywatnych, lecz rozszerzając go potencjalnie o informacje wszelkiego rodzaju, zarówno obiektywne, jak i subiektywne, w postaci opinii czy oceny, a jedynym warunkiem, które muszą one spełniać, jest to, aby dotyczyły danej osoby. Warunek ten jest zaś spełniony, gdy ze względu na swą treść, cel czy skutek dana informacja jest powiązana z daną osobą".

Możliwa identyfikacja

Wobec powyższego przyjąć należy, że samo oświadczenie, iż wszyscy członkowie zarządu/wspólnicy spełniają wymóg niekaralności, mimo że nie wskazuje wprost ich imion i nazwisk, uznać można za zawierające dane osobowe. Istnieje bowiem możliwość iden-

tyfikacji osób, których ta informacja dotyczy (członków organów osób prawnych czy wspólników spółek osobowych). Łatwo to zrobić zwłaszcza na podstawie informacji zawartych w rejestrach publicznych, np. w KRS, CEIDG czy też w odpisach z tych rejestrów załączanych zazwyczaj do umów lub akt postępowań.

Szczególne rygory przetwarzania

Jednocześnie oświadczenie o niekaralności należy uznać za dokument zawierający dane osobowe, o których mowa w art. 10 RODO, tj. dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa.

Dla przetwarzania tych danych prawodawca unijny przewidział w powołanym przepisie szczególne zasady. Artykuł ten stanowi bowiem, że „przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą".

Zatem, jeśli nie został spełniony któryś z wymienionych w art. 10 RODO dodatkowych wymogów (przetwarzanie pod nadzorem władz publicznych lub na podstawie przepisów prawa), wówczas przetwarzanie danych wymienionych w tym przepisie uznać należy za niezgodne z prawem.

W opinii Prezesa UODO, wewnętrznych procedur administratora, na które powołują się niektórzy zamawiający, wskazując je jako podstawę legalizującą pozyskiwanie takich oświadczeń, a które nie odwołują się bezpośrednio do obowiązku wynikającego z przepisu prawa, nie można uznać za wystarczającą podstawę prawną do przetwarzania danych osobowych, o których mowa w art. 10 RODO.

KTO JEST ODBIORCĄ DANYCH

Za odbiorcę danych w rozumieniu art. 4 pkt 9 RODO należy uznać wyłącznie taki podmiot lub osobę, które są uprawnione do dostępu do nich. Nie jest nim ten, kto wszedł w posiadanie danych w wyniku wystąpienia naruszenia ochrony danych osobowych.



To istotne rozróżnienie, mające wpływ m.in. na poprawne dopełnianie obowiązku informacyjnego z art. 13 i 14 RODO, realizację praw osób, których dane dotyczą (w tym dostępu do danych na mocy art. 15 RODO), a także na prowadzenie rejestru czynności przetwarzania.

Jeśli odbiorca, to tylko uprawniony

Zgodnie z definicją zawartą w art. 4 ust. 9 RODO, „Odbiorca oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania". Powyższa definicja odnosi się jedynie do odbiorców uprawnionych, czyli takich, którym ujawnia się, lub którym zostaną ujawnione dane osobowe zgodnie z RODO i innymi przepisami.

Osoba nieuprawniona nie jest odbiorcą

W przypadku wystąpienia naruszenia ochrony danych osobowych (incydentu) polegającego na ujawnieniu (udostępnieniu) danych osobowych osobie nieuprawnionej, takiej osoby nie należy uznawać za odbiorcę danych. Nie jest ona także stroną trzecią w rozumieniu art. 4 pkt 10 RODO.

Ważne argumenty

Za takim rozumieniem pojęcia „odbiorca" przemawia analiza przyjętych w RODO rozwiązań.

Dla przykładu, zgodnie z art. 19 RODO, administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe oraz informuje osobę, której dane dotyczą (na jej żądanie), o tych odbiorcach. Ponadto Prezes UODO ma prawo nakazać administratorowi poinformowanie odbiorców o usunięciu lub ograniczeniu przetwarzania danych (na mocy art. 58 ust. 2 lit. g RODO). Gdyby osobę nieuprawnioną uznać za odbiorcę danych, to w takich sytuacjach pozyskiwałaby ona kolejne informacje o osobie, której dane zdobyła na skutek naruszenia, np. o usunięciu lub sprostowaniu tych danych przez administratora. Takie podejście skutkowałoby również tym, że w rejestrze czynności przetwarzania jako kategorię odbiorców należałoby umieścić również podmioty nieuprawnione, a zatem przyjąć, iż z założenia będzie dochodzić do pozyskiwania danych przez podmioty nieuprawnione, co jest sprzeczne z celami przyświecającymi zarówno tworzeniu takiego rejestru, jak i ogólnie zasadami ochrony danych.

Uwaga!
Powyższe rozważania zachowują swoją aktualność także w przypadku realizacji obowiązków informacyjnych określonych w art. 13, 14 i 15 RODO. Obowiązek administratora dotyczący podania informacji o odbiorcy danych odnosi się tylko do tego odbiorcy, który legalnie, a więc na podstawie właściwej przesłanki legalizującej i konkretnego celu przetwarzania, otrzymał lub otrzyma dane osobowe. Wobec powyższego stwierdzić należy, że definicja odbiorcy danych, biorąc pod uwagę wykładnię systemową i funkcjonalną, nie obejmuje podmiotu/osoby fizycznej, któremu bezprawnie ujawniono dane.

Wobec tego administrator nie jest uprawniony do podawania danych takich osób podczas realizacji prawa dostępu do danych przysługującego osobie, której dane dotyczą, na mocy którego ma ona prawo do otrzymania m.in. informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione (art. 15 ust. 1 lit. c).

Zakres informacji o naruszeniu

Administrator nie powinien udostępniać danych osobowych osoby fizycznej, której w wyniku naruszenia ochrony danych osobowych (incydentu), bezprawnie ujawniono dane, także wówczas, gdy realizuje obowiązek zawiadamiania o naruszeniu osoby, której dane dotyczą.

Artykuł 34 RODO zobowiązuje administratora m.in. do przekazania osobie, której dane dotyczą, informacji o środkach zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych – w tym w stosownych przypadkach – środków mających na celu zminimalizowanie jego ewentualnych negatywnych skutków. To administrator ma pełną wiedzę o zdarzeniu oraz o działaniach, jakie może podjąć osoba, której dane dotyczą, w celu zminimalizowania negatywnych skutków naruszenia.

Jednocześnie należy wskazać, że administrator ma znaczne możliwości, by wpłynąć na osobę, która na skutek incydentu weszła w posiadanie danych osobowych, choć nie jest do tego uprawniona. Może chociażby zażądać zwrotu nieprawidłowo zaadresowanej korespondencji czy poinformować ją, że dalsze przetwarzanie danych osobowych, do których przetwarzania nie jest uprawniona, może narazić ją na odpowiedzialność karną wynikającą z art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Artykuł 34 RODO nie zobowiązuje wprost administratora do podawania szczegółowych informacji o zdarzeniu, takich jak np. podatność w systemie informatycznym wykorzystana do uzyskania nieuprawnionego dostępu do danych osobowych czy dane osobowe „przypadkowego", nieuprawnionego odbiorcy. Wręcz przeciwnie – opis ma być sformułowany prostym i jasnym językiem, w sposób zwięzły przedstawiający zaistniałe zdarzenie. Ponadto o konieczności udzielania takich informacji nie wspominają zarówno wytyczne Grupy Roboczej Art. 29, jak i wskazówki Prezesa UODO dotyczące naruszeń ochrony danych osobowych.

Należy również zauważyć, że konieczność udostępnienia danych osoby fizycznej, której bezprawnie ujawniono dane, prowadziłaby do ograniczenia jej prawa do prywatności, a podstawą tego udostępnienia byłoby pierwotne, naruszające przepisy, zdarzenie zaistniałe u administratora.



KIEROWCA AUTOBUSU NIE POWINIEN POZNAĆ DANYCH OSOBY, KTÓRA ZŁOŻYŁA NA NIEGO SKARGĘ

Miejskiemu przedsiębiorstwu komunikacyjnemu (MPK), którego pracownik nie w pełni zanonimizował skargę i udostępnił ją kierowcy, Prezes UODO udzielił upomnienia za naruszenie zasady poufności danych.

W toku prowadzonego w tej sprawie postępowania Prezes UODO ustalił, że pasażer złożył w MPK skargę na kierowcę autobusu. Wykorzystał do tego elektroniczny formularz kontaktowy udostępniony przez MPK. Podał w nim swoje imię i nazwisko oraz adres e-mail.

W skutek niedopatrzenia pracownika, który przekazał kierowcy kopię skargi, dane skarżącego pasażera nie zostały zanonimizowane we wszystkich miejscach. Kierowca mógł więc je poznać, choć nie był do tego uprawniony. Realizacja celu, jakim było rozpatrzenie skargi była możliwa bez przekazania danych osobowych.

W wydanej w tej sprawie decyzji, Prezes UODO podkreślił, że MPK, z chwilą otrzymania formularza skargi, stało się administratorem zawartych w niej danych osobowych. Jego obowiązkiem – zgodnie z art. 5 ust. 1 lit. f RODO – było przetwarzanie danych w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Powinien w tym celu wdrożyć należyte środki techniczne i organizacyjne, odpowiednie do ryzyka związanego z przetwarzaniem tych danych.

Bezsprzecznie w analizowanym przypadku doszło do naruszenia przez MPK zasady poufności danych, gdyż dopuściło ono, by z danymi pasażera, który złożył skargę, zapoznała się osoba nieuprawniona, tj. kierowca autobusu.

Niemniej Prezes UODO, stwierdzając naruszenie, uznał upomnienie za wystarczającą reakcję w tej sprawie. Wziął bowiem pod uwagę jego incydentalny charakter oraz późniejsze działania MPK, tj. dodatkowe przeszkolenie pracowników oraz dokonanie analizy procedury rozpatrywania skarg pod kątem możliwości wprowadzenia anonimizacji danych osobowych osób składających skargi jeszcze przed ich przekazaniem do komórki organizacyjnej, rozpatrującej sprawę zgodnie z właściwością.

DOTOWANIE PODMIOTÓW PROWADZĄCYCH ŻŁOBEK LUB KLUB DZIECIĘCY

Gmina przekazująca ze swojego budżetu dotację oraz otrzymujące ją podmioty, jak prowadzący żłobek lub klub dziecięcy lub zatrudniający dziennych opiekunów oraz osoby prowadzące działalność na własny rachunek, to odrębni administratorzy.



Żeby określić status danego podmiotu w procesie przetwarzania danych osobowych trzeba kierować się zawartymi w RODO definicjami administratora i podmiotu przetwarzającego oraz uwzględniać to, w jakich celach (dla realizacji jakich zadań), w jaki sposób i na jakich podstawach prawnych określony podmiot te dane przetwarza. Zgodnie z art. 4 pkt 7 RODO, „administratorem danych osobowych jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania

danych osobowych. Podmiotem przetwarzającym jest zaś, jak stanowi art. 4 pkt 8 RODO, osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Zgodnie zaś z art. 28 ust. 1 RODO, z powierzeniem przetwarzania danych osobowych mamy do czynienia wówczas, gdy przetwarzanie jest dokonywane przez zewnętrzny podmiot w imieniu administratora. Podmiot przetwarzający nie działa we własnych celach, bo cele przetwarzania oraz polecenia co do przetwarzania są formułowane przez administratora.

Zatem w myśl przepisów RODO, konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator zleca wykonywanie swoich zadań innemu podmiotowi (podmiotowi przetwarzającemu). Podmiot przetwarzający przetwarza dane w imieniu administratora, a nie w imieniu własnym, a zatem nie staje się ich administratorem. Podmiot przetwarzający nie decyduje bowiem o celach i sposobach przetwarzania, gdyż przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO).

Z taką sytuacją nie mamy do czynienia w przypadku przetwarzania danych osobowych dzieci objętych opieką w żłobku lub klubie dziecięcym, na które gmina przekazuje ze swojego budżetu dotację celową.

W myśl art. 60 ust. 1 ustawy z dnia 4 lutego 2011 r. o opiece nad dziećmi w wieku do lat 3, jednostki samorządu terytorialnego oraz instytucje publiczne, osoby fizyczne oraz osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej, prowadzące żłobek lub klub dziecięcy lub zatrudniające dziennych opiekunów oraz osoby prowadzące działalność na własny rachunek, mogą otrzymać na dziecko objęte opieką w żłobku lub klubie dziecięcym, lub przez dziennego opiekuna, dotacje celową z budżetu gminy. Wysokość i zasady ustalania oraz rozliczania tej dotacji, w tym kategorie dzieci, na które przyznawana jest dotacja, określa rada gminy w drodze uchwały (art. 60 ust. 2 tej ustawy). Może w niej ustalić, że wraz z wnioskiem o udzielenie dotacji gminie przekazać należy dane osobowe dzieci objętych opieką.

W opisanej sytuacji mamy jednak do czynienia z odrębnymi administratorami, a przekazywanie danych następuje na postawie właściwych przepisów ustawowych i uchwały rady gminy, nie zaś z wykorzystaniem konstrukcji, o której mowa w art. 28 RODO, tj. z powierzeniem przetwarzania danych osobowych. Dane te są bowiem przekazywane gminie w celu realizacji przez nią jej własnych zadań.



PROWADZENIE REJESTRU AKCJONARIUSZY

Podmioty ustawowo uprawnione do prowadzenia rejestru akcjonariuszy spółek niebędących spółkami publicznymi, jak np. domy maklerskie czy banki powiernicze, są jednocześnie administratorami pozyskanych w tym celu danych. Dysponują one bowiem własnymi, określonymi w Kodeksie spółek handlowych, celami przetwarzania danych zawartych w rejestrze.

Wiele podmiotów już teraz podejmuje działania mające na celu przygotowanie ich do obowiązkowej dematerializacji akcji i rejestracji w rejestrze akcjonariuszy spółek. To efekt nowelizacji przepisów Kodeksu spółek handlowych wprowadzonych ustawą z 30 sierpnia 2019 r.

Czas na wybór podmiotu i wezwania do złożenia akcji

Obecnie spółki, po zmianach terminów wprowadzonych tzw. Tarczą Antykryzysową 3.0 (ustawa z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2), mają obowiązek do 30 września 2020 r. dokonać wyboru i zawarcia umowy z podmiotem dokonującym dematerializacji akcji i prowadzącym następnie rejestr akcjonariuszy spółki, a także dokonać pierwszego wezwania akcjonariuszy do złożenia w spółce akcji, będących w formie dokumentowej. Muszą też pamiętać, że 1 marca 2021 r. upływa termin ważności akcji w formie dokumentowej. To również ostateczny termin na ukonstytuowanie się rejestru akcjonariuszy.

Status spółek i podmiotów prowadzących rejestr akcjonariuszy

W związku z tymi pracami Prezesowi UODO sygnalizowane są wątpliwości co do ról poszczególnych podmiotów.

W opinii Prezesa UODO, spółki oraz podmioty ustawowo uprawnione do prowadzenia rejestru akcjonariuszy spółek to odrębni administratorzy. Za takim podejściem przemawiają rozwiązania zawarte w art. 328^{1}–328^{15} Kodeksu spółek handlowych.

Rejestr akcjonariuszy – zgodnie z art. 328^{1} § 2 Kodeksu spółek handlowych – prowadzą podmioty, które na podstawie ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, są uprawnione do prowadzenia rachunków papierów wartościowych. Ponadto to podmioty uprawnione do prowadzenia rejestru akcjonariuszy wystawiają świadectwa rejestrowe. Jest to ich wyłączna kompetencja, nie zaś zadanie zlecone przez spółkę, co także przemawia za uznaniem tych podmiotów za odrębnych administratorów. Podmiot prowadzący rejestr akcjonariuszy, któremu spółka przekaże dane akcjonariuszy, dysponuje bowiem własnymi, określonymi w Kodeksie spółek handlowych celami przetwarzania danych zawartych w rejestrze.

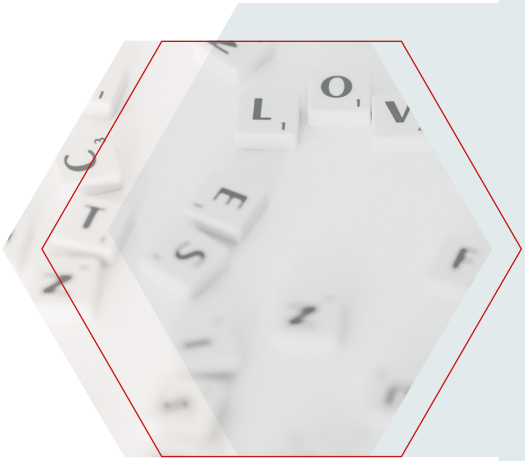
Zauważyć także należy, że zgodnie z art. 328^{4} § 1 Kodeksu spółek handlowych, podmiot prowadzący rejestr akcjonariuszy dokonuje wpisu w rejestrze akcjonariuszy, na żądanie spółki lub osoby mającej interes prawny w dokonaniu wpisu. Tym samym trudno uznać spółkę za administratora, który autonomicznie ustala cele przetwarzania danych osobowych w rejestrze akcjonariuszy, jeżeli własne cele ustalają też osoby mające interes prawny w dokonywaniu wpisu do tego rejestru.

Bez umowy powierzenia przetwarzania danych

Niewłaściwą praktyką byłoby zatem zawieranie przez spółki oraz podmioty prowadzące rejestr akcjonariuszy umów powierzenia przetwarzania danych osobowych.

W JAKIM JĘZYKU PROWADZIĆ KOMUNIKACJĘ WS. OCHRONY DANYCH

W jakim języku należy realizować obowiązek informacyjny wobec klientów, jeżeli zagraniczna firma mająca oddziały w Polsce, posługuje się językiem angielskim?



Podstawowym wymogiem, jaki nakłada ogólne rozporządzenie o ochronie danych (RODO) na administratora, w zakresie formy, w jakiej mają być przekazywane informacje osobie, której dane dotyczą, jest przejrzystość komunikacji. Zgodnie z art. 12 RODO administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji. Chodzi o informacje podawane w przypadku zarówno zbierania danych od osoby, której dane dotyczą (art. 13 RODO), jak również gdy dane osobowe pozyskiwanie są w inny sposób (art. 14 RODO). Ponadto zasada przejrzystości jest wymagana, aby prowadzić z wszelką dbałością komunikację w sprawie przetwarzania (na mocy art. 15–22 i 34).

Jakiego języka użyć w komunikacji z pracownikami?

Jeśli pracownicy firmy nie posługują się językiem polskim, a zrozumiałą formą przekazu jest dla nich komunikacja w języku angielskim, zasadnym jest, aby administrator przekazywał im wymagane informacje również w języku angielskim. Należy jednak pamiętać, że ustawa z dnia 7 października 1999 r. o języku polskim – dalej ustawa o języku polskim, ustanawia wymóg używania języka polskiego przy wykonywaniu przepisów z zakresu prawa pracy (w art. 7 ust. 1), jeśli osoba świadcząca pracę ma miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej. Tym samym – ponieważ dotyczy to stosunków z zakresu prawa pracy – przekazanie przez administratora odpowiednich informacji w języku angielskim nie zwalnia go z przekazania tych samych informacji również w języku polskim.

W jakim języku prowadzić dokumentację?

Odnosząc się natomiast do języka, w jakim ma być sporządzona wewnętrzna dokumentacja administratora danych (np. polityka bezpieczeństwa danych osobowych),

to podstawową zasadą RODO, przez pryzmat, której powinien być rozpatrywany ten problem, jest zasada rozliczalności. Zgodnie z art. 24 ust. 1 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. Dlatego na administratorze ciąży obowiązek takiego zaprojektowania funkcjonującego u niego systemu ochrony danych osobowych, aby był zgodny z RODO i aby administrator mógł to wykazać. Zgodnie z art. 24 ust. 2 RODO, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

RODO nie narzuca wprost formy, w tym języka, w jakim mają być sporządzone owe polityki – jednak dokumentacja przetwarzania danych osobowych w firmie działającej na terenie Polski powinna być prowadzona w języku polskim, co nie wyklucza również innego języka, jeżeli jest on używany w relacjach wewnętrznych firmy. Mając na uwadze cel jakiemu mają służyć wspomniane polityki, sporządzenie ich wyłącznie w języku angielskim może być niewystarczające dla wykazania przez administratora, funkcjonującego w ramach polskiego porządku prawnego, zgodności z RODO.

Należy pamiętać, że w zakres szerokiego pojęcia bezpieczeństwa przetwarzania danych osobowych nie wchodzą wyłącznie przepisy RODO. Są to również m.in. wymogi ustaw: z dnia 10 maja 2018 r. o ochronie danych osobowych, z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, jak również wiele aktów prawnych odnoszących się do tajemnicy prawnie chronionej oraz ochrony danych w poszczególnych sektorach. Dlatego polityki ochrony danych osobowych muszą oprócz aktów prawnych o charakterze międzynarodowym uwzględniać również polskie ustawodawstwo.

W jakim języku komunikować się z organem nadzorczym?
Ponieważ art. 5 ust. 1 ustawy o języku polskim stanowi, że podmioty wykonujące zadania publiczne na terytorium Rzeczypospolitej Polskiej dokonują wszelkich czynności urzędowych oraz składają oświadczenia woli w języku polskim, chyba że przepisy szczególne stanowią inaczej, to komunikacja administratora z organem nadzorczym jest również prowadzona w języku polskim. Należy pamiętać, że zgodnie z art. 51 ust. 1 RODO, każde państwo członkowskie zapewnia, by za monitorowanie stosowania ogólnego rozporządzenia o ochronie danych odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii. Zgodnie zaś z art. 57 ust. 1 lit. a RODO organ nadzorczy na swoim terytorium monitoruje i egzekwuje stosowanie RODO, jest również władny na podstawie art. 58 ust. 1 lit a RODO nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań. Działania organu nadzorczego zgodnie z wyżej przywoływanymi unormowaniami ustawy o języku polskim, która zobowiązuje organy publiczne do wykonywania czynności urzędowych w języku polskim, będą wykonywane właśnie w tym języku.



PUBLIKACJA DANYCH OSOBOWYCH ZAWARTYCH W RECENZJACH ROZPRAW DOKTORSKICH

Administrator, który przetwarza dane osobowe zwarte w recenzjach w związku z prowadzonymi postępowaniami o nadawania stopnia naukowego doktora powinien sprawdzić czy: przetwarzanie danych osobowych wynika z przepisów prawa, jest niezbędne do zrealizowania konkretnego celu oraz przez czas nie dłuższy, niż jest to konieczne.

Sposób prowadzenia postępowania w sprawach przyznania uprawnienia do nadawania stopnia doktora regulują przepisy sektorowe, tj. ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (dalej: p.s.w.n.) oraz ustawa z dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (dalej: przepisy wprowadzające).

Przed nowelizacją przepisów o szkolnictwie wyższym...
W sytuacji gdy postępowanie w sprawie nadania stopnia doktora zostało wszczęte i niezakończone przed dniem wejścia w życie ww. przepisów, tj. przed

1 października 2018 r., to zgodnie z art. 175 przepisów wprowadzających, prowadzi się je na podstawie przepisów dotychczasowych, tj. ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuk (dalej: ustawa o stopniach naukowych).

Recenzje rozprawy doktorskiej zamieszcza się na stronie internetowej szkoły wyższej lub jednostki organizacyjnej przeprowadzającej przewód doktorski w dniu ich przekazania przez recenzentów, które pozostają na stronie internetowej co najmniej do dnia nadania stopnia doktora (zgodnie z art. 13 ust. 7 ustawy o stopniach naukowych). Oznacza to, że administrator, chcąc dalej publikować dane osobowe zawarte w recenzjach rozpraw doktorskich, już po nadaniu stopnia doktora, ma obowiązek wykazać, że realizuje cel wynikający wprost z przepisów prawa. Powinien on dowieść, że przetwarzanie określonych danych jest zgodne z zasadami wynikającymi z RODO (art. 5 ust. 1), m.in. z zasadą ograniczenia celu (lit. b). Zasada ta stanowi, że dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Oznacza to, że administrator powinien dokonać analizy dalszej retencji danych osobowych, które planuje przetwarzać. Warunek zamieszczenia recenzji rozprawy doktorskiej nie dotyczy natomiast rozprawy, której przedmiot jest objęty ochroną informacji niejawnych.

...po nowelizacji przepisów

Zgodnie z nowymi przepisami – art. 188 p.s.w.n. – podmiot doktoryzujący, nie później niż 30 dni przed wyznaczonym dniem obrony rozprawy doktorskiej, udostępnia w Biuletynie Informacji Publicznej (BIP) na swojej stronie podmiotowej rozprawę doktorską będącą pracą pisemną wraz z jej streszczeniem albo opis rozprawy doktorskiej niebędącej pracą pisemną oraz recenzje. Natomiast, w przypadku rozprawy doktorskiej, której przedmiot jest objęty tajemnicą prawnie chronioną, udostępnia się tylko recenzje z wyłączeniem treści objętych tą tajemnicą. Dokumenty te udostępnia się również w Systemie POL-on (Zintegrowany System Informacji o Szkolnictwie Wyższym i Nauce POL-on). Baza dokumentów w postępowaniach awansowych, w tym systemie, obejmuje w odniesieniu do osób ubiegających się o stopień doktora m.in. recenzje rozprawy doktorskiej i daty ich opracowania (art. 348 ust. 1 pkt 1 lit. e) p.s.w.n.). Powyższe oznacza, że zgodnie z obowiązującymi przepisami – obowiązkiem podmiotu doktoryzującego jest upublicznienie rozprawy doktorskiej wraz z jej streszczeniem oraz recenzjami w terminie i miejscu określonym przez ustawę, a także przekazanie ww. dokumentów do Systemu POL-on. Wyjątek odnoszący się do braku upubliczniania rozprawy doktorskiej, której przedmiot jest objęty tajemnicą prawnie chronioną, dotyczy jedynie obowiązku związanego z udostępnieniem określonych informacji w BIP. Nie dotyczy on natomiast zamieszczenia danych w Systemie POL-on.

Zgodnie z przepisami p.n.s.w. czas publikacji dokumentów przed obroną rozprawy doktorskiej – w porównaniu do ustawy o stopniach naukowych – został wydłużony, ponieważ udostępnia się je 30 dni przed wyznaczonym terminem obrony. Dotychczas recenzje publikowane były w dniu ich przekazania przez recenzentów, a streszczenie rozprawy doktorskiej publikowane było w dniu podjęcia decyzji o jej przyjęciu. Pozostawione były one na stronie internetowej co najmniej do dnia nadania stopnia doktora oraz przekazania ich do Centralnej Komisji ds. Stopni i Tytułów w celu opublikowania w BIP. Obecnie natomiast wszystkie dokumenty muszą być opublikowane 30 dni przed obroną rozprawy doktorskiej.

Potrzebna ciągła analiza przetwarzanych danych

Zarówno dotychczasowe, jak i aktualne przepisy nie regulują obowiązku usuwania recenzji, w tym danych osobowych w nich zawartych, ze strony internetowej podmiotu prowadzącego postępowanie. Obecnie obowiązujące przepisy p.n.s.w. również nie wskazują, jak długo powinny być publikowane ww. treści na stronie internetowej (BIP) podmiotu doktoryzującego.

Uwaga!

Administrator, który przetwarza dane osobowe zawarte w recenzjach w związku z prowadzonymi postępowaniami, zarówno na podstawie ustawy o stopniach naukowych, jak i przepisów p.s.w.n., powinien kierować się przede wszystkim koniecznością spełnienia przesłanek określonych w art. 5 ust. 1 ogólnego rozporządzenia o ochronie danych (RODO). Powinien zwłaszcza dokonać analizy, czy przetwarzanie (upublicznianie) danych osobowych wynika z określonych przepisów prawa, jest niezbędne do zrealizowania konkretnego celu oraz przez czas nie dłuższy, niż jest to konieczne.

Dlatego administrator powinien przy każdym procesie przetwarzania danych badać dalszą retencję określonych danych, wymaganej przez RODO, oraz wprowadzić procedury ich usuwania. Wyniki oceny celowości dalszego przetwarzania na stronach internetowych poszczególnych rodzajów danych osobowych znajdujących się w recenzjach powinny zostać częścią dokumentacji tworzonej przez administratora zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO). Działania te są konieczne, aby mógł wykazać on, że przetwarza dane zgodnie z przepisami sektorowymi, a jednocześnie nie narusza praw osób, których dane dotyczą.



PODSUMOWANIE KONSULTACJI PROJEKTU WYMOGÓW AKREDYTACJI

Zakończyły się konsultacje społeczne projektu wymogów akredytacji podmiotów monitorujących kodeksy postępowania. Dziękujemy za zainteresowanie i udział w prowadzonych przez Prezesa UODO konsultacjach.

Do Urzędu Ochrony Danych Osobowych wpłynęło blisko 230 uwag od twórców kodeksów, instytucji uczestniczących w konsultacjach projektów kodeksów, specjalistów ochrony danych osobowych oraz innych osób zainteresowanych.

Po przeanalizowaniu wszystkich nadesłanych uwag, Prezes Urzędu, zgodnie z art. 41 ust. 3 ogólnego rozporządzenia o ochronie danych (RODO), przedłoży ostateczny projekt proponowanych wymogów akredytacji Europejskiej Radzie Ochrony Danych z wykorzystaniem mechanizmu spójności przewidzianego w art. 63 RODO.

Przypomnijmy, projekt wymogów akredytacji podmiotów monitorujących kodeksy postępowania został przygotowany na podstawie art. 41 RODO, przy uwzględnieniu art. 29 ustawy o ochronie danych osobowych oraz wytycznych Europejskiej Rady Ochrony Danych nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.

Szczegółowe informacje o kodeksach są dostępne pod adresem: https://uodo.gov.pl/pl/426.

TRZY NOWE WNIOSKI O ZATWIERDZENIE KOLEJNYCH KODEKSÓW POSTĘPOWANIA

Rynek badań i opinii, branża retail oraz środowisko bibliotekarzy to kolejne grupy, które podjęły starania o wypracowanie kodeksów postępowania. Wnioski o ich zatwierdzenie czekają na akceptację Prezesa UODO.



W ostatnim czasie wnioski złożyli:

– Związek Pracodawców Organizacja Firm Badania Opinii i Rynku – projekt kodeksu postępowania w zakresie ochrony i przetwarzania danych osobowych w badaniach rynku i opinii;

– Polska Rada Centrów Handlowych – projekt kodeksu RODO dla branży retail;

– Stowarzyszenie Bibliotekarzy Polskich – Kodeks postępowania dla bibliotek wspierający we właściwym stosowaniu RODO.

Więcej informacji na temat złożonych wniosków dostępnych jest pod adresem: https://uodo.gov.pl/pl/426/1109

Ponadto przypominamy o trwających konsultacjach projektów kodeksów postępowania dla fotografów oraz dla oświaty.

Do 31 sierpnia 2020 r. wszystkie podmioty zainteresowane stosowaniem RODO w branży fotograficznej mogą wziąć udział w konsultacjach projektu kodeksu postępowania w tym sektorze. Treść projektu kodeksu oraz więcej informacji na jego temat są dostępne na stronie internetowej: https://bezpiecznywizerunek.pl/.

Z kolei miesiąc później, tj. 30 września 2020 r., zakończą się konsultacje projektu kodeksu postępowania dla oświaty. Aktualna treść projektu tego kodeksu jest dostępna na stronie internetowej: http://rodo-w-oswiacie.pl/kodeks-postepowania-calosc/.



MIĘDZYNARODOWE
CO PO BREXICIE? KE PRZYGOTOWAŁA INFORMACJE NA TEN TEMAT

Komisja Europejska opublikowała materiały informacyjne dotyczące Brexitu pt. „Przygotowania na koniec okresu przejściowego".

Na dedykowanej stronie internetowej Komisji Europejskiej można znaleźć informacje dotyczące wycofania się Zjednoczonego Królestwa z członkostwa w Unii Europejskiej i przepisów unijnych w dziedzinie ochrony danych, które zawierają opis sytuacji prawnej po zakończeniu okresu przejściowego oraz odpowiednie postanowienia dotyczące umowy o wycofaniu.

Więcej materiałów na ten temat dostępnych jest pod adresem: https://ec.europa.eu/info/european-union-and-united-kingdom-forging-new-partnership/future-partnership/getting-ready-end-transition-period_pl



KARY

Belgia: dwie kary za działania marketingowe

Belgijski organ ochrony danych ukarał w niezależnych postępowaniach dwa podmioty za prowadzenie marketingu bezpośredniego z naruszeniem zasad ogólnego rozporządzenia o ochronie danych (RODO).

1000 euro za nieprzestrzegania prawa osoby, której dane dotyczą

Pierwszą z kar w wysokości tysiąca euro nałożono na stowarzyszenie, które, na podstawie prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f) RODO), wysyłało wiadomości marketingu bezpośredniego do (byłych) darczyńców w swoich akcjach pozyskiwania funduszy. Kara administracyjna została nałożona po skardze złożonej w belgijskim organie ochrony danych przez dawnego darczyńcę stowarzyszenia, które to nie zrealizowało wniosku o usunięcie danych, skierowanego przez tę osobę, do administratora danych (w związku z art. 17 ust. 1 RODO) oraz z prawem do sprzeciwu (zgodnie z art. 21 ust. 2 RODO).

Izba sporów sądowych zadecydowała, że administrator danych naruszył artykuły 6 ust. 1, 17 ust. 1 lit. c) i d), 23 ust. 1 oraz 21 ust. 4 RODO.

Po pierwsze izba stwierdziła, że administrator nie zastosował się do wniosku o usunięcie danych oraz prawa osoby, której dane dotyczą, do sprzeciwu. Po drugie, izba uznała, że stowarzyszenie nie mogło stosować swojego prawnie uzasadnionego interesu jako podstawy prawnej przetwarzania danych w tym przypadku, gdyż nie dopełniło skumulowanych warunków nałożonych przez orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej – w szczególności wyroku ws. Rigas satiksme (C-13/16). Zgodnie z tym orzeczeniem, aby powołać się na art. 6 ust. 1 lit. f) RODO administrator powinien udowodnić, że:

- interesy, realizowane poprzez przetwarzanie, mogą zostać uznane za prawnie uzasadnione („test celu”);

- zamierzone przetwarzanie jest niezbędne dla celów zamierzonego przetwarzania („test niezbędności”)

- ważenie tych interesów względem podstawowych praw i wolności osób, których dane dotyczą, przechyla się na korzyść administratora lub strony trzeciej („test równoważenia”).

W tym przypadku izba sporów zadecydowała, że trzeci z warunków art. 6 ust. 1 lit. f) RODO oraz orzeczenia TSUE nie został spełniony.

Izba sporów stwierdziła, że istnieją wątpliwości co do tego, czy osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w celu marketingu bezpośredniego lata po zebraniu tych danych (motyw 47 RODO). Ponadto izba uznała, że administrator danych w sposób niewystarczający umożliwił realizację prawa do sprzeciwu.

Decyzja ta wdrażana jest w kontekście przyjętego przez belgijski organ ochrony danych strategicznego planu na lata 2020-2025, w którym marketing bezpośredni jest jednym z priorytetowych punktów strategicznych. Izba sporów w związku z tym odwołuje się także do Rekomendacji nr 01/2020 belgijskiego organu ochrony danych.

10 tys. euro za wysyłki marketingowe do niewłaściwego adresata

Jeśli chodzi o drugą z kar, to belgijski organ ochrony danych ukarał administratora za wysłanie wiadomości marketingu bezpośredniego do niewłaściwej osoby i za niewłaściwą odpowiedź na późniejszy wniosek tej osoby o dostęp danych, które jej dotyczą. Tym razem kara wyniosła 10 tys. euro.

W tym przypadku wiadomość marketingowa została wysłana do powoda zamiast do innej osoby o tym samym nazwisku, lecz innym adresie e-mail. Do niewłaściwego przetwarzania doszło z powodu błędu ludzkiego. Osoba, która otrzymała wiadomość skorzystała z prawa dostępu do danych, co nie przebiegło w sposób płynny. Belgijski organ ochrony danych stwierdził, że administrator nieodpowiedział w sposób wystarczający na wniosek powoda (art. 15 RODO), ponadto nie udzielił odpowiedzi w terminie określonym w RODO (art. 12 ust. 3) i nie wykazał się wystarczającą przejrzystością (art. 12 ust. 1 RODO). Z tych przyczyn belgijski organ uznał, że wykonanie praw tej osoby nie było wystarczająco ułatwione, jak tego wymaga art. 12 ust. 2 RODO.

Pełne treści decyzji w języku niderlandzkim dostępne są pod adresem:

https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_28-2020_NL_.pdf

https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_33-2020_NL.pdf

Źródła:
https://edpb.europa.eu/news/national-news/2020/belgian-dpa-fines-controller-sending-direct-marketing-message-wrong-person_pl

https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposed-fine-1000-eur-association-sent-direct-marketing-messages_pl

Hiszpania: kara za brak odpowiedzi na wniosek o udzielenie informacji

Hiszpański organ ochrony danych nałożył na przedsiębiorstwo Iberdrola karę w wysokości 4 tys. euro za brak odpowiedzi na wniosek o udzielenie informacji

Procedura sankcyjna została wszczęta w związku z brakiem odpowiedzi na wniosek o udzielenie informacji złożony celem zbadania okoliczności faktycznych zidentyfikowanych w skardze. Skarżący wnioskował wyłączenie dotyczących go danych z kartoteki odnoszącej się do zadłużenia – Asnef – z powodu rzekomego zadłużenia wobec przedsiębiorstwa dostarczającego energię – Iberdrola.

Skarga przekazano do przedsiębiorstwa Iberdrola, które zostało zobowiązane do wydania AEPD (hiszpańskiemu organowi nadzorczemu) informacji i dokumentów, o które wnioskowano w wystąpieniu. Gdy nie otrzymano odpowiedzi, skarga została przyjęta.

Następnie przeprowadzone zostały postępowania, a przedsiębiorstwo zobowiązano do przedstawienia wymaganych faktów. Ten nowy wniosek również pozostał bez odpowiedzi. Przedsiębiorstwo Iberdrola nie podało wymaganych informacji i konsekwentnie utrudniało prowadzenie postępowania, które należy do uprawnień każdego z organów nadzorczych, naruszając art. 58 ust. 1 RODO.

Naruszenie to jest określone w art. 83 ust. 5 lit. e) RODO i zostało sklasyfikowane jako bardzo poważne.

Wzięto również pod uwagę, że Iberdrola jest dużym przedsiębiorstwem, nie zaś nowo utworzonym i dlatego powinno było ustanowić procedury wypełniania obowiązków wynikających z przepisów o ochronie danych, w tym przekazywać wszelkie informacje wymagane przez organ nadzorczy. Z tego powodu ukarano je kwotą 5 tys. euro, zmniejszoną do 4 tys. euro, ponieważ skorzystało z dobrowolnego zmniejszenia płatności zgodnie z hiszpańskim prawem procesowym.

Pełna treść decyzji w języku hiszpańskim dostępna jest pod adresem: https://www.aepd.es/es/documento/ps-00444-2019.pdf

Źródło:
https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-fined-company-iberdrola-not-responding_pl

Finlandia: trzy kary za niewystarczającą informację o prawach osób

Rada ds. sankcji Biura Rzecznika Ochrony Danych nałożyła kary administracyjne na trzy przedsiębiorstwa za naruszenia ochrony danych osobowych. Naruszenia te dotyczyły zapewnienia niewystarczających informacji o prawach do ochrony danych, zaniedbania polegającego na braku przeprowadzenia oceny skutków dla ochrony danych oraz niepotrzebnego gromadzenia danych osobowych.

Są to pierwsze kary, które nałożyła rada ds. sankcji za naruszenie przepisów o ochronie danych.

Braki w informacjach przekazywanych w związku z powiadomieniami o zmianie adresu

Osoby, które złożyły skargę do Rzecznika Ochrony Danych, otrzymały komunikaty i marketing bezpośredni od różnych przedsiębiorstw po przesłaniu informacji o zmianie adresu do przedsiębiorstwa Posti Oy, które jest wiodącym operatorem usług pocztowych w Finlandii. Postępowanie przeprowadzone przez Urząd Rzecznika Ochrony Danych ujawniło, że przedsiębiorstwo to nie poinformowało osób, których dane dotyczą, o ich prawach, w tym o prawie do sprzeciwu wobec ujawnienia danych w związku z przesłaniem informacji o zmianie adresu. Przedsiębiorstwo powinno było wyraźnie poinformować swoich klientów o ich prawie do sprzeciwu wobec przetwarzania ich danych osobowych. Posti przekazało takie powiadomienia tylko klientom, którzy zakupili dodatkowe usługi oprócz powiadomienia o zmianie adresu. Posti już w 2017 r. powiadomiło Rzecznika Ochrony Danych, że zbada możliwości poprawy przejrzystości przetwarzania danych osobowych. Przedsiębiorstwo ostatecznie poprawiło swoje praktyki informowania klientów w 2020 r., po tym jak Biuro Rzecznika Ochrony Danych ponownie się z nim skontaktowało. Naruszenia jedynie w 2019 r. dotknęły 161 tys. klientów. Rada ds. sankcji nałożyła na Posti Oy karę administracyjną w wysokości 100 tys. euro.

Ocena skutków dla ochrony danych przetwarzania danych o lokalizacji pracowników została zlekceważona

Druga decyzja dotyczyła skargi do Rzecznika Ochrony Danych na temat sposobu, w jaki przedsiębiorstwo Kymen Vesi Oy przetwarzało dane o lokalizacji swoich pracowników poprzez śledzenie pojazdów za pomocą systemu informacji o pojeździe. Administrator nie dokonał oceny skutków wymaganej przez RODO przed rozpoczęciem przetwarzania danych o lokalizacji. Dane o lokalizacji wykorzystywano między innymi do monitorowania godzin pracy.

Ocena skutków dla ochrony danych jest wymagana, jeśli przetwarzanie może spowodować wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Ocena jest konieczna na przykład w przypadku przetwarzania danych o lokalizacji osób wymagających szczególnego traktowania lub gdy dane o lokalizacji wykorzystywane są do systematycznego monitorowania. Decyzję w sprawie sytuacji, w których wymagana jest ocena skutków dla ochrony danych przetwarzania danych o lokalizacji, można znaleźć na stronie internetowej Rzecznika Ochrony Danych.

Rada ds. sankcji nałożyła na Kymen Vesi Oy karę administracyjną w wysokości 16 tys. euro.

Dane osobowe osób ubiegających się o pracę zostały zebrane bez potrzeby

W trzecim przypadku Rzecznik Ochrony Danych został powiadomiony o przedsiębiorstwie niepotrzebnie zbierającym dane osobowe od osób ubiegających się o pracę i pracowników. Zgodnie z fińską ustawą o ochronie prywatności w życiu zawodowym pracodawca może przetwarzać jedynie dane, które są niezbędne w związku ze stosunkiem pracy. Niedociągnięcia wykryto również w dokumentacji administratora dotyczącej zgodności z RODO.

Przedsiębiorstwo prosiło o informacje dotyczące takich kwestii, jak przekonania religijne, stan zdrowia, możliwa ciąża i status rodzinny osób, których dane dotyczą. Rzecznik Ochrony Danych nakazał

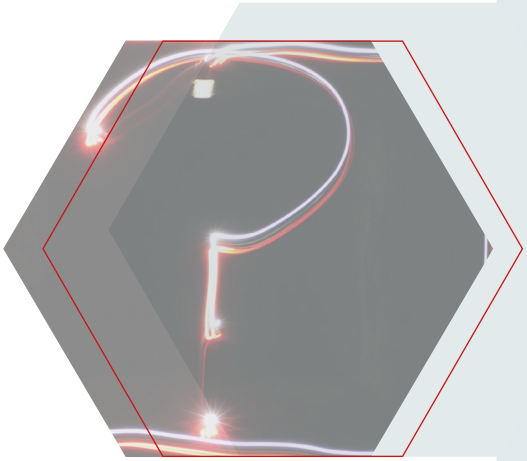
przedsiębiorstwu usunięcie niepotrzebnych danych i wydał upomnienie za braki w dokumentacji. Rada ds. Sankcji nałożyła również na przedsiębiorstwo karę administracyjną w wysokości 12,5 tys. euro.

Po raz pierwszy Rada ds. sankcji nałożyła kary administracyjne za naruszenie przepisów o ochronie danych.

Pełna treść decyzji w języku fińskim dostępna jest na stronie https://tietosuoja.fi/en/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista

Źródło: https://edpb.europa.eu/news/national-news/2020/finnish-dpa-imposed-three-administrative-fines-data-protection-violations_pl

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:

Jaka jest podstawa przetwarzania danych członków rodziny pracownika korzystającego z ZFŚS?
Czy z sołtysem należy zawierać umowę powierzenia?
Kto jest administratorem w przypadku PKZP działającej przy pracodawcy?

URZĄD OCHRONY DANYCH OSOBOWYCH