Obserwuj nas na:

Nr 7/2021 (28)
Lipiec 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

# NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

# PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH W ZWIĄZKU Z ORGANIZACJĄ, NAGRYWANIEM I UDOSTĘPNIANIEM NAGRAŃ Z TELEKONFERENCJI

**Żeby pracodawcy mogli przetwarzać wizerunek pracowników, muszą spełnić przynajmniej jedną z przesłanek, o których mowa w art. 6 RODO, a także muszą być spełnione wszystkie zasady wskazane w jego art. 5. Administrator powinien też stworzyć procedury, z których będzie wynikał termin i sposób usuwania informacji zawierających dane osobowe oraz zasady dokonywania przeglądów przetwarzanych danych.**

Podczas wykonywania pracy zdalnej pracownicy niektórych instytucji, w tym publicznych, korzystają z telekonferencji. W ten sposób przeprowadzane są różne spotkania, konferencje oraz szkolenia, niekiedy z udziałem przedstawicieli podmiotów zewnętrznych. W czasie ich trwania mogą być przetwarzane takie dane osobowe, jak: wizerunek, głos, imię i nazwisko, stanowisko służbowe uczestnika telekonferencji czy nazwa pracodawcy. Niejednokrotnie istnieje też potrzeba nagrywania takich spotkań, a następnie ich udostępniania, co rodzi różne praktyczne problemy, o wyjaśnienie których proszony jest organ ds. ochrony danych osobowych. Wiele z nich dotyczy podstaw prawnych przetwarzania danych osobowych, w tym wizerunku.

## Możliwe przesłanki

W związku z tym warto wskazać, że przetwarzanie danych osobowych, w tym wizerunku, jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z warunków określonych w art. 6 ust. 1 RODO. Należy podkreślić, że przesłanki legalizujące co do zasady są równoprawne. Wobec tego spełnienie co najmniej jednej z nich stanowi już o zgodnym z prawem przetwarzaniu danych osobowych. Zatem dla legalności przetwarzania danych osobowych nie zawsze wymagana jest zgoda osoby, której dane dotyczą. U podstaw tego procesu może znajdować się bowiem inna z przesłanek wymienionych w art. 6 ust. 1 RODO.

W niektórych przypadkach możliwe wydaje się zastosowanie przesłanki, o której mowa w art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą).

Zakres danych, które pracodawca obowiązkowo pozyskuje od pracownika określony został w art. $22^1$ § 1–3 Kodeksu pracy. Dodatkowo w § 4 powołanego artykułu wskazano, że pracodawca żąda podania innych danych osobowych niż określone w § 1 i 3 (jak m.in. imię, nazwisko, adres zamieszkania czy numer PESEL), gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Z przepisów Kodeksu pracy nie wynika wprawdzie wprost, że pracownik musi udostępnić pracodawcy wizerunek, ale w niektórych przypadkach wykorzystanie wizerunku pracownika przez pracodawcę jest immanentnie związane z realizacją stosunku pracy.

W związku z nawiązaniem stosunku pracy na podstawie umowy o pracę, pracownik zobowiązuje się do wykonywania pracy określonego rodzaju na rzecz pracodawcy pod jego kierownictwem oraz w miejscu i czasie wyznaczonym przez pracodawcę, a pracodawca do zatrudnienia pracownika za wynagrodzeniem. Umowa o pracę zwykle zawiera ogólne elementy określające łączące strony postanowienia umowne. Doprecyzowaniem umowy o pracę może być regulamin pracy czy zakres obowiązków.

Powołanie się na wskazaną powyżej przesłankę przetwarzania danych osobowych pracowników (art. 6 ust. 1 lit. b RODO) można rozważać zwłaszcza

w przypadku osób zatrudnionych na stanowiskach, w które wpisane są takie zadania, jak np. wystąpienia publiczne, konferencje, szkolenia (dyrektorzy, rzecznik prasowy, pracownik działu szkoleń).

Należy przy tym zauważyć, że zwłaszcza w czasie pandemii liczba stanowisk wykonujących swoje zadania (podstawowe obowiązki służbowe) w trybie zdalnym, np. poprzez udział w telekonferencji, zwiększyła się, co powinno znaleźć swoje odzwierciedlenie w zakresie obowiązków tych pracowników, w szczególności poprzez ustalenie, których stanowisk to dotyczy oraz modyfikację w zakresach obowiązków trybu wykonywania takich obowiązków.

Powyższe rozważania dotyczą sytuacji, gdy udział pracownika np. w wideokonferencji czy szkoleniu mieści się w zakresie realizacji jego obowiązków służbowych. Natomiast w sytuacji, gdy przetwarzanie wizerunku i innych danych z tą sytuacją związanych następuje w innych celach niż objęte treścią stosunku pracy, wówczas można rozważać zastosowanie przesłanki zgody (art. 6 ust. 1 lit. a RODO).

Wprawdzie EROD w Wytycznych 05/2020 w sprawie zgody na mocy rozporządzenia 2016/679 wskazała, że „w przypadku większości takiego przetwarzania danych w miejscu pracy podstawą prawną nie może i nie powinna być zgoda pracowników (art. 6 ust. 1 lit. a) ze względu na charakter relacji między pracodawcą a pracownikiem". Niemniej dalej dodano, że „nie oznacza to jednak, że pracodawcy nigdy nie mogą polegać na zgodzie jako zgodnej z prawem podstawie przetwarzania. Mogą wystąpić sytuacje, w których pracodawca może wykazać, że zgoda faktycznie jest udzielana swobodnie". Jako przykład takiej sytuacji EROD wskazała filmowanie części biura, w przypadku której, ci pracownicy, którzy nie chcą być filmowani, mogą w czasie realizacji nagrania pracować w innych pomieszczeniach.

Polski ustawodawca kwestię zgody pracownika jako podstawy do przetwarzania danych osobowych uregulował w art. $22^{1a}$ § 1 Kodeksu pracy. Zgodnie z tym przepisem, zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę innych danych osobowych niż wymienione w art. $22^{1}$ § 1 i 3, z wyjątkiem danych osobowych, o których mowa w art. 10 RODO. W § 2 tego przepisu ustawodawca zastrzegł jednak, że brak zgody, o której mowa w § 1, lub jej wycofanie, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę.

Wobec powyższego można zasadnie przyjąć, że przetwarzanie danych pracownika może opierać się na przesłance zgody, o której mowa w art. 6 ust. 1 lit. a RODO oraz $22^{1a}$ Kodeksu pracy, przy czym wobec braku równości stron stosunku pracy trzeba zastrzec, że odbierana od pracownika zgoda nie może być jedynie formalna, iluzoryczna i musi mieć on rzeczywistą możliwość odmowy jej wyrażenia bez poniesienia negatywnych konsekwencji.

## Z poszanowaniem wszystkich zasad

Należy podkreślić, że to na administratorze spoczywa obowiązek każdorazowej oceny podstawy przetwarzania danych. Przede wszystkim należy zwrócić uwagę na zasady określone w art. 5 RODO, które mają charakter podstawowy w odniesieniu do całej regulacji. Zasady te należy traktować jako posiadające nadrzędną moc i wyznaczające kierunek działania administratora w realizacji jego zadań wynikających z przepisów prawa. Podstawową zasadą w ogólnym rozporządzeniu o ochronie danych jest „zasada rozliczalności", o której mowa w art. 5 ust. 2 RODO. Zgodnie z tym przepisem, administrator danych jest odpowiedzialny za przestrzeganie wszystkich zasad przy przetwarzaniu danych osobowych (wskazanych w art. 5 ust. 1 RODO) i musi być w stanie wykazać ich przestrzeganie. Zasada rozliczalności nakłada zatem na administratora ciężar dowodowy, polegający na konieczności wykazania przez niego zarówno przed organem nadzorczym, jak również przed podmiotem danych, dowodów na przestrzeganie wszystkich zasad przetwarzania danych.

## Uwaga na okres retencji

Warto też zwrócić szczególną uwagę na zasadę ograniczonego przechowywania określoną w art. 5 ust. 1 lit. e RODO. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien stworzyć procedury, z których będzie wynikał termin i sposób usuwania informacji zawierających dane osobowe oraz zasady dokonywania przeglądów przetwarzanych danych. Należy zatem mieć na uwadze, że nawet dokonywane na podstawie zgody udostępnienie danych osobowych w określonych celach w sieci nie oznacza bezterminowego ich przechowywania i w związku z tym administrator powinien jasno określić okresy przetwarzania upublicznianych w ten sposób danych.

# WERYFIKACJA TOŻSAMOŚCI OSOBY WNIOSKUJĄCEJ O PRAWO DOSTĘPU DO DANYCH

**W opinii UODO, imię, nazwisko, adres, nazwa zboru Świadków Jehowy, do którego należała dana osoba, oraz własnoręczny podpis to dane wystarczające do zidentyfikowania osoby wnioskującej o dostęp do dotyczących jej danych osobowych. Żądanie przesłania kserokopii urzędowego dokumentu stwierdzającego tożsamość zawierającego podpis oraz zdjęcie prowadziłoby do pozyskania danych nadmiarowych i byłoby niezgodne z zasadą minimalizacji danych.**

Takie rozstrzygnięcie sporu między byłym członkiem Związku Wyznaniowego Świadkowie Jehowy a tym związkiem znalazło się w wydanej niedawno decyzji Prezesa UODO.

Sprawa była rozpatrywana w związku ze skargą osoby, która chciała skorzystać z przysługującego jej na mocy art. 15 ust. 1 RODO prawa dostępu do dotyczących jej danych osobowych.

## Wniosek do zboru

Osoba, której dane dotyczą, zwróciła się ze stosownym wnioskiem w tej sprawie do Związku Wyznaniowego Świadkowie Jehowy, którego wcześniej była członkiem. Poprosiła w nim o przekazanie jej takich informacji, jak:
- od kiedy i jakie jej dane osobowe posiada i przetwarza zbór,
- z jakiego źródła zbór pozyskał jej dane osobowe,
- w jakim celu, zakresie i w jaki sposób dane te są przetwarzane,
- czy zbór przekazał dane osobowe innemu administratorowi, a jeśli tak, to jakiemu i w jakim zakresie,
- jaka jest treść formularza S-77, który stanowi informację na temat wewnątrzwyznaniowego postępowania dyscyplinarnego.

Jednocześnie w podpisanym własnoręcznie wniosku podała takie informacje na swój temat, jak: imię, nazwisko, adres i nazwa zboru.

## Żądanie dodatkowych danych

Związek poinformował jednak osobę wnioskującą, że w związku z koniecznością weryfikacji jej tożsamości, powinna ona przesłać wniosek wraz z kserokopią urzędowego dokumentu stwierdzającego tożsamość, zawierającego podpis oraz zdjęcie. Zdaniem Związku, pozyskanie dodatkowych danych osoby wnioskującej jest konieczne dla właściwego zabezpieczenia danych osobowych przed udostępnieniem osobie nieuprawnionej, co jest tym bardziej istotne, że dotyczy dostępu do szczególnej kategorii danych osobowych.

W wyjaśnieniach kierowanych do UODO Związek podnosił, że jako administrator nie może opierać się na danych osobowych, które każdy może łatwo pozyskać (imię i nazwisko oraz nazwa zboru), na danych osobowych, których nie posiada (adres), ani na danych osobowych, których nie można samodzielnie potwierdzić bez urzędowego dokumentu (w tym przypadku podpis). Wskazywał, że powinien mieć prawo skorzystać z wszelkich rozsądnych środków (motyw 64 preambuły RODO), jeżeli ma uzasadnione wątpliwości (art. 12 ust. 6 RODO) co do tożsamości wnioskodawcy.

## Decyzja Prezesa UODO

W wydanej w tej sprawie decyzji Prezes UODO uznał, że takie informacje przekazane przez osobę chcącą skorzystać z prawa dostępu do dotyczących jej danych, jak: imię, nazwisko, adres, nazwa zboru oraz własnoręczny podpis, były wystarczające do zidentyfikowania jej w prowadzonych przez Związek zbiorach danych i umożliwiały spełnienie wobec niej żądań wymienionych we wniosku. Natomiast pozyskanie danych z dokumentu tożsamości byłoby nadmiarowe i niezgodne z zasadą wyrażoną minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO.

W uzasadnieniu decyzji Prezes UODO wskazał, że choć zgodnie z art. 12 ust. 6 RODO, bez uszczerbku dla art. 11, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21 RODO, może on zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą, to przepis ten należy odczytywać łącznie z motywem 64 RODO, który wskazuje, że administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą. Jeżeli informacje przekazane przez osobę wnioskującą byłyby niewystarczające do ustalenia tego faktu, Związek powinien poprosić ją o dodatkowe informacje, na podstawie których uzyskałby pewność co do posiadania podstawy prawnej przekazania danych. Jednak dokonując wszelkich działań w obszarze przetwarzania danych osobowych, administrator powinien zarazem mieć na uwadze wyrażoną w art. 5 ust. 1 lit. c RODO zasadę minimalizacji danych, zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne, do celów, w których są przetwarzane. Zgodnie z tą zasadą, administrator nie tylko jest zobowiązany do tego, aby ustalić zakres niezbędnych danych, ale również, aby poddać szczegółowej analizie poszczególne ich kategorie, w celu wyeliminowania danych potencjalnie nadmiarowych, czyli takich, których przetwarzanie nie jest niezbędne w danym procesie przetwarzania.

W opinii Prezesa UODO, przesłanie kserokopii urzędowego dokumentu stwierdzającego tożsamość, zawierającego podpis i zdjęcie, nie umożliwiłoby Związkowi dokonania poprawnej weryfikacji personaliów osoby wnioskującej o dostęp do dotyczących jej danych. Ponadto wszystkie dane zawarte w dokumencie tożsamości, z wyjątkiem imienia, nazwiska oraz daty urodzenia, byłyby dla Związku danymi nieadekwatnymi i nadmiarowymi do wykonywanych przez niego czynności przetwarzania.

Prezes UODO podkreślił, że w przypadku gdy dane osobowe przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby fizycznej, nie powinien on mieć prawa uzyskania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do przepisów rozporządzenia. Motyw 64 preambuły RODO stanowi, że administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości osoby żądającej dostępu do dotyczących jej danych, jednak w świetle powyższych regulacji bezsporna jest konieczność maksymalnego ograniczenia zakresu przetwarzanych danych osobowych na każdym etapie tego procesu.

## ODSTĘPSTWA OD DOPEŁNIANIA OBOWIĄZKU INFORMACYJNEGO

**Organ publiczny, pozyskując podczas prowadzonego postępowania administracyjnego lub skargowego dane osobowe nie od osoby, której one dotyczą, nie musi spełniać obowiązku informacyjnego określonego w art. 14 ust. 1 i 2 RODO, gdy podstawą przetwarzania danych osobowych jest obowiązek ciążący na administratorze wynikający z przepisów prawa.**

Do organów administracji publicznej często wpływają różne pisma, w tym skargi, które odnoszą się nie do osób je składających, ale do osób trzecich. W takich sytuacjach rodzą się wątpliwości dotyczące dopełniania obowiązku informacyjnego.

W jednym z wyjaśnień w tej sprawie Prezes UODO przypomniał, że art. 14 RODO nakłada na administratora obowiązek przekazania osobie, której dane dotyczą, określonych informacji w przypadku gdy jej dane są pozyskiwane z innych źródeł niż bezpośrednio od niej samej. Zgodnie z art. 14 ust. 5 lit. c. RODO, z tego obowiązku informacyjnego administrator zwolniony jest w sytuacji, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem (przepisami prawa UE lub prawa państwa członkowskiego, któremu podlega administrator), przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą. Wskazane zwolnienie obejmuje przypadki, w których przepisy zawierają wyraźne

regulacje dotyczące przetwarzania (pozyskiwania lub ujawniania) danych. Ma ono szczególne znaczenie dla podmiotów publicznych (zwłaszcza administracji publicznej), które – zgodnie z zasadą legalizmu – opierają swoje działania na przepisach prawa. Zwrócić należy jednak uwagę, że obejmuje ono jedynie gromadzenie danych z innych źródeł, natomiast nie przewidziano go w odniesieniu do gromadzenia przez administrację publiczną danych od osób, których dane dotyczą. Warunkiem zastosowania tego zwolnienia jest również spełnienie wymogu, aby przepisy regulujące przetwarzanie danych przewidywały odpowiednie środki chroniące prawa osób, których dane poddawane są przetwarzaniu.

Wskazać jednak należy, że zgodnie z art. 14 ust. 5 lit. c RODO, organ publiczny, pozyskując dane osobowe nie od osoby, której one dotyczą, nie jest obowiązany spełniać obowiązku informacyjnego określonego w art. 14 ust. 1 i 2 RODO, gdy podstawą przetwarzania danych osobowych jest obowiązek ciążący na administratorze wynikający z przepisów prawa.

Jeśli podmiot publiczny działający na podstawie i w granicach prawa w związku z wykonywaniem obowiązków określonych w Kodeksie postępowania administracyjnego (k.p.a.) pozyskuje dane osobowe z innych źródeł niż osoba, której dane dotyczą (np. gdy dane te zawarte są w treści skarg lub wniosków), wówczas można zasadnie rozważać zastosowanie wskazanego wyżej zwolnienia z obowiązku informacyjnego.

Jednocześnie szczególną ostrożność zachować należy co do danych osoby, od której pozyskano informacje. W niektórych sytuacjach bowiem przekazanie takich danych może doprowadzić do naruszenia przepisów k.p.a., gdyż zgodnie z zawartym w nim art. 236 § 2, w przypadku wszczęcia albo wznowienia postępowania, stwierdzenia nieważności decyzji, jej uchylenia albo zmiany na skutek skargi, o której mowa w art. 233 zdanie drugie, art. 234 pkt 2 lub art. 235, w stosunku do strony i uczestnika postępowania nie stosuje się art. 15 ust. 1 lit. g RODO (który w przypadku, gdy dane osobowe zostały pozyskane nie od osoby, której dotyczą, przyznaje jej prawo do uzyskania od administratora wszelkich dostępnych informacji o źródle ich pozyskania). Oznacza to, że jeżeli konsekwencją wniesienia skargi czy wniosku będzie uruchomienie postępowania, a skarga czy wniosek pochodzą od innej osoby niż strona, to nie informuje się strony ani uczestnika postępowania o źródle pozyskania informacji. Skarżący może jednak na każdym etapie postępowania zezwolić organowi na udostępnienie swoich danych stronie. Przepis ten skorelowany jest z art. 73 § 1b k.p.a., w świetle którego wgląd w akta sprawy w przypadku, o którym mowa w art. 236 § 2, następuje z pominięciem danych osobowych osoby składającej skargę.

# CZY Z TŁUMACZEM PRZYSIĘGŁYM NALEŻY ZAWRZEĆ UMOWĘ POWIERZENIA?

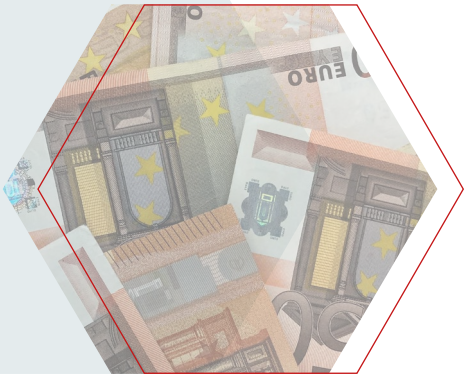
**Organ administracji publicznej, przekazując w związku z prowadzonym postępowaniem, dokumenty do tłumaczenia przez tłumacza przysięgłego, nie musi zawierać z nim umowy powierzania przetwarzania danych osobowych. W tej sytuacji mamy bowiem do czynienia z udostępnieniem danych innemu administratorowi na podstawie przepisów prawa.**

Zgodnie z art. 75 ust. 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (k.p.a.), jako dowód należy dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem. Organ administracji publicznej jest obowiązany w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy (art. 77 ust. 1 k.p.a.). Zatem przedłożenie przed organem administracji publicznej dokumentów w języku obcym jest dopuszczalne i to na tym organie spoczywa obowiązek uzyskania ich tłumaczenia.

Natomiast osobą uprawnioną do sporządzenia tłumaczenia z języka obcego na język polski jest przede wszystkim tłumacz przysięgły (art. 13 pkt 1 ustawy z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego).

Organy administracji publicznej, działając na podstawie przepisów prawa, mogą więc zwrócić się do tłumacza przysięgłego o dokonanie takiego tłumaczenia, a tłumacz przysięgły na podstawie art. 15 powołanej wyżej ustawy, nie może odmówić wykonania takiego tłumaczenia, chyba że zachodzą szczególnie ważne przyczyny uzasadniające odmowę.

Ustawa o zawodzie tłumacza przysięgłego w art. 29a–29c kreuje obowiązki tłumacza jako administratora. W art. 29a ust. 1 ustawy wskazano, że przepisy art. 15 ust. 1 i 3, art. 18 oraz art. 19 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez tłumacza przysięgłego tajemnicy zawodowej, o której mowa w art. 14 ust. 1 pkt 2 tej ustawy. Natomiast w przypadku danych osobowych pozyskanych przez tłumacza przysięgłego w związku z tłumaczeniem nie stosuje się przepisu art. 21 ust. 1 RODO (art. 29a ust. 2 ustawy). Zgodnie bowiem z art. 14 ust. 1 pkt 2 ustawy o zawodzie tłumacza przysięgłego, tłumacz przysięgły jest obowiązany do zachowania w tajemnicy faktów i okoliczności, z którymi zapoznał się w związku z tłumaczeniem. Obowiązek ten nie ustaje w przypadku, gdy z żądaniem ujawnienia informacji uzyskanych w związku z tłumaczeniem występuje Prezes UODO (art. 29b tej ustawy). Z kolei w art. 29c tej ustawy określony został okres przechowywania danych osobowych zgromadzonych przez tłumacza przysięgłego w związku z tłumaczeniem, który wynosi 4 lata od zakończenia roku kalendarzowego, w którym dane zostały zgromadzone. Po upływie tego okresu dane osobowe podlegają usunięciu, chyba że dalsze ich przechowywanie jest niezbędne dla ochrony praw lub dochodzenia roszczeń.



# KARY

## Francja: CNIL nakłada karę pieniężną w wysokości 500 tys. euro na BRICO PRIVÉ

**CNIL ukarał firmę BRICO PRIVÉ za wysyłanie e-maili reklamowych bez zgody osób prywatnych oraz za nieprzestrzeganie kilku obowiązków wynikających z RODO.**

CNIL przeprowadziła trzy kontrole w latach 2018–2021 w przedsiębiorstwie BRICO PRIVÉ, które wydaje stronę internetową sprzedaży prywatnej bricoprive.com poświęconą majsterkowaniu, ogrodnictwu i remontom domów. Firma ta działa we Francji i w trzech innych krajach europejskich (Hiszpania, Włochy i Portugalia).

Podczas kontroli CNIL odnotowała kilka naruszeń dotyczących przetwarzania danych osobowych potencjalnych klientów i klientów spółki. CNIL uznał, że przedsiębiorstwo naruszyło szereg obowiązków przewidzianych we francuskim kodeksie poczty i łączności elektronicznej (CPCE), RODO i ustawie o ochronie danych.

Spółce zarzucono nieprzestrzeganie obowiązku ograniczenia czasu przechowywania danych. Przedsiębiorstwo nie przestrzegało ustalonych przez siebie okresów przechowywania danych. W ten sposób zachowano dane ponad 16 tys. klientów, którzy nie złożyli zamówienia w ciągu ostatnich pięciu lat. To samo dotyczyło ponad 130 tys. osób, które nie logowały się na swoje konto klienta od pięciu lat. Ponadto spółka nie przestrzegała obowiązku informacyjnego. Informacje udostępnione użytkownikom strony internetowej nie zawierały wszystkich elementów wymaganych przez RODO, zarówno w ogólnych warunkach sprzedaży, uwagach prawnych, jak i polityce przechowywania danych osobowych. BRICO PRIVÉ nie wywiązało się także z obowiązku pełnego zastosowania się do otrzymanych wniosków o usunięcie danych, ponieważ nie usunęło danych osobowych klienta, który złożył wniosek (zachowując na przykład jego nazwisko, imię i adres e-mail). Przystąpiła jedynie do dezaktywacji dostępu do konta.

Spółka nie zapewnieniła bezpieczeństwa danych osobowych, wymagając zastosowania silnego hasła przy zakładaniu konta na swojej stronie internetowej ani przy dostępie pracowników do oprogramowania do zarządzania relacjami z klientami. Naruszenia dotyczyły także poszukiwań handlowych i plików cookie, niepodlegające współpracy europejskiej.

Ponadto przedsiębiorstwo nie przestrzegało obowiązku uzyskania zgody osób fizycznych w celu prowadzenia poszukiwań handlowych drogą elektroniczną, które w tym przypadku art. L. 34-5 francuskiego kodeksu poczty i łączności elektronicznej (CPCE) przewiduje, że takie operacje wymagają uprzedniej zgody zainteresowanych osób.

Ponieważ firma działa w kilku krajach na terenie Unii Europejskiej, skład orzekający CNIL współpracował, w odniesieniu do części decyzji, z organami nadzorczymi trzech krajów, w których BRICO PRIVÉ oferuje swoje usługi.

W konsekwencji CNIL nałożył karę pieniężną w wysokości 500 tys. euro oraz nakazał spółce dostosowanie operacji przetwarzania danych do art. L.34-5 CPCE i RODO oraz uzasadnienie tego w ciągu trzech miesięcy od powiadomienia o decyzji, pod groźbą kary w wysokości 500 euro za każdy dzień zwłoki.

Źródło: https://www.cnil.fr/fr/sanction-de-500-000-euros-lencontre-de-la-societe-brico-prive

## Hiszpania: 1,5 mln euro kary za dwa naruszenia

**Hiszpański organ ochrony danych osobowych (AEPD) nałożył na EDP Comercializadora, S.A.U. karę pieniężną w wysokości 1,5 mln euro za dwa naruszenia RODO.**

AEPD uważa, że EDP COMERCIALIZADORA, S.A.U nie przyjęła środków technicznych i organizacyjnych w celu sprawdzenia, czy osoba, która wynajmuje jej usługi w imieniu innej osoby fizycznej, posiada upoważnienie do przeprowadzania zawierania umów.

Firma nie przyjęła również środków technicznych i organizacyjnych pozwalających na weryfikację, czy osoba działająca w imieniu innej osoby fizycznej jest upoważniona przez tę osobę do wyrażenia zgody na inne przetwarzanie danych osobowych w jej imieniu. Zgody te były wymagane podczas procedury zatrudniania, w dwóch celach: wysyłania własnych informacji handlowych i informacji handlowych osób trzecich oraz profilowania z wykorzystaniem informacji z baz danych osób trzecich do zautomatyzowanego podejmowania decyzji w celu wysyłania spersonalizowanych propozycji handlowych i umożliwienia zawierania umów na określone usługi.

W związku z tym AEPD stwierdziła, że EDP COMERCIALIZADORA, S.A.U. naruszyła art. 25 RODO, za co nałożono karę pieniężną w wysokości 500 tys. euro.

Ponadto hiszpański organ uważa, że dokument mający na celu dostarczenie informacji osobom, których dane dotyczą, nie zapewnia wystarczających informacji na temat administratora danych, podstawy prawnej przetwarzania nieopartego na zgodzie, celów przetwarzania związanych z profilowaniem na podstawie prawnie uzasadnionego interesu, ani możliwości sprzeciwu wobec czynności przetwarzania, które administrator danych opiera na swoim prawnie uzasadnionym interesie. Ponadto, w niektórych procedurach zawierania umów o świadczenie usług przez spółkę (np. zawieranie umów przez telefon) forma dostępu do wszystkich informacji wymaganych na podstawie art. 13 nie jest prosta i natychmiastowa. W związku z tym AEPD uznała, że został naruszony art. 13 RODO i nałożyła karę pieniężną w wysokości 1 mln euro.

Źródło: https://edpb.europa.eu/news/national-news/2021/spanish-dpa-imposes-fine-1500000-euros-epd-comercializadora-sau-two_pl

## Holandia: 525 tys. euro kary dla firmy, która m.in. publikowała dane klientów, nie pytając ich, czy tego chcą

**Holenderski organ ochrony danych osobowych nałożył karę pieniężną w wysokości 525 tys. euro na stronę internetową Locatefamily.com, która publikuje adresy i numery telefonów osób, często bez ich wiedzy.**

Organ nadzorczy otrzymał skargi na Locatefamily.com. Strona wyświetla pełne adresy, a czasami również numery telefonów osób, które nie wiedzą, w jaki sposób ich dane się tam znalazły. Osoby te w żadnym przypadku nie udostępniły temu administratorowi swoich danych.

To wszystko ma znaczący wpływ na osoby, których dane znajdują się na Locatefamily.com. Osoby, które nie są świadome, że ich dane kontaktowe zostały upublicznione. Locatefamily.com to międzynarodowa platforma, na której ludzie mogą wyszukiwać dane kontaktowe członków rodziny, z którymi utracili kontakt lub innych osób, z którymi chcieliby się skontaktować.

Platforma udostępnia dane osobowe osób z całego świata, w tym z Unii Europejskiej. Na stronie znajduje się około 700 tys. Holendrów.

Każdy, kto chce usunąć swoje dane z tej strony, nie może tego łatwo zrobić, ponieważ Locatefamily.com nie ma przedstawiciela w UE. Tymczasem brak przedstawiciela w Unii stanowi naruszenie ogólnego

rozporządzenia o ochronie danych (RODO) i jest powodem nałożenia kary pieniężnej.

Aby zmusić Locatefamily.com do ustanowienia przedstawiciela w UE, holenderski organ nadzorczy nałożył również na Locatefamily.com nakaz jego wyznaczenia podlegający karze. Przedsiębiorstwo miało na to czas do 18 marca 2021 roku. W przeciwnym razie Locatefamily.com musi zapłacić 20 tys. euro za każde dwa tygodnie zwłoki w jego wyznaczeniu maksymalnie 120 tys. euro. Locatefamily.com nie potwierdziło organowi do tego czasu, czy wyznaczyło już przedstawiciela w UE.

Źródło: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-imposes-fine-eu525000-locatefamilycom_pl

## Norwegia: 25 tys. euro za nielegalne przesyłanie poczty elektronicznej pracownika

**Norweski organ ochrony danych osobowych nałożył na przedsiębiorstwo karę pieniężną za nielegalne przesyłanie poczty elektronicznej pracownika. Nazwa przedsiębiorstwa nie została podana do publicznej wiadomości, aby chronić tożsamość jego pracowników.**

Tłem sprawy jest skarga złożona przez osobę, która stwierdziła, że jej pracodawca poprosił o ustawienie automatycznego przekierowania z jej konta poczty elektronicznej na wspólne konto firmowe. Miało to wynikać z przyczyn operacyjnych.

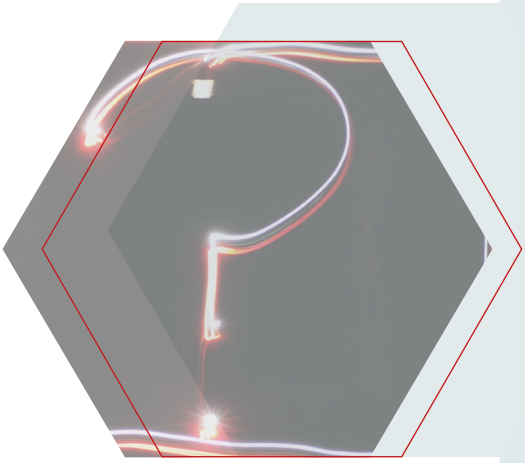
Po zbadaniu sprawy norweski organ ochrony danych osobowych stwierdził, że przedsiębiorstwu brakowało podstawy prawnej do przekazywania poczty elektronicznej. Odbyło się to z naruszeniem przepisów dotyczących dostępu pracodawcy do kont poczty elektronicznej i innych materiałów elektronicznych, a także wymogu podstawy prawnej wynikającego z RODO.

Przedsiębiorstwo nie opracowało również procedur dostępu do poczty elektronicznej. Norweski organ wskazał, że poprawa procedur mogłaby zapobiec przyszłym przypadkom niezgodnego z prawem dostępu.

Na tej podstawie norweski organ nadzorczy nakazał przedsiębiorstwu usprawnienie wewnętrznych procedur kontroli i wytycznych dotyczących dostępu do poczty elektronicznej pracowników. Ponadto przedsiębiorstwu nakazano uiszczenie kary pieniężnej w wysokości 250 tys. norweskich koron, czyli ok. 25 tys. euro za monitorowanie konta poczty elektronicznej skarżącego bez podstawy prawnej.

Źródło: https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-company-fined-illegal-forwarding-e-mail_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:

Czy z zewnętrznym IOD wykonującym zadania dla banku należy zawrzeć umowę powierzenia?

Czy obowiązek z art. 38 ust. 2 RODO dotyczy administratora korzystającego z usług zewnętrznego IOD?

Czy uczelnia może udostępnić dane osobowe studentów wyłącznie w oparciu o ustawę o Straży Granicznej?