NEWSLETTER
Ochrona danych osobowych

W pierwszym newsletterze w 2021 roku zapraszamy do lektury na temat obowiązków notyfikacyjnych w przypadku naruszenia ochrony danych oraz transferu danych do Wielkiej Brytanii po Brexicie.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH
Obowiązki notyfikacyjne

Co to jest naruszenie ochrony danych osobowych?

Zgodnie z art. 4 pkt 12 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: „**RODO**") **naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych**.

Przykładowe naruszenia bezpieczeństwa danych osobowych:

- zgubienie lub kradzież nośnika danych;
- przesłanie umowy z danymi klienta na niewłaściwy adres;
- nieuprawniony dostęp osoby trzeciej do bazy danych.

Kiedy należy zgłosić naruszenie ochrony danych osobowych?

Administratorzy powinni zgłaszać naruszenia ochrony danych do właściwych organów nadzoru (w Polsce jest to Prezes Urzędu Ochrony Danych Osobowych; „**PUODO**"), **chyba że jest mało prawdopodobne**, aby naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych.

Kiedy takie ryzyko może zaistnieć? Zgodnie z motywem 75 RODO, **ryzyko naruszenia praw lub wolności, o różnym prawdopodobieństwie i wadze, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych.** Dotyczy to m.in. sytuacji, gdy przetwarzanie może skutkować dyskryminacją, kradzieżą tożsamości, stratą finansową czy naruszeniem poufności danych osobowych chronionych tajemnicą zawodową.

WAŻNE! Administrator powinien zgłosić naruszenie ochrony danych (jeżeli jest związane z ryzykiem naruszenia praw i wolności osób fizycznych) do PUODO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin.

Ponadto, jeżeli naruszenie może skutkować **wysokim ryzykiem naruszenia praw lub wolności** osób fizycznych, dodatkowo należy zawiadomić osoby, których dane dotyczą.

Praktyka PUODO – zgłoszenie nieprawidłowej wysyłki maila

W dniu 28 grudnia 2020 r. na stronie internetowej UODO opublikowano komunikat informujący o nałożeniu kary pieniężnej w wysokości 85 588 zł na Towarzystwo Ubezpieczeniowe

i Reasekuracyjne Warta („**TUiR Warta**") za niezgłoszenie naruszenia ochrony danych osobowych w przewidzianym przepisami terminie.

Naruszenie ochrony danych polegało na wysłaniu pocztą elektroniczną przez agenta ubezpieczeniowego pod niewłaściwy adres mailowy (błędnie podany przez klienta) wiadomości potwierdzającej zawarcie umowy ubezpieczenia samochodu – do wiadomości została załączona polisa zawierająca dane dwóch osób (numery PESEL, imiona, nazwiska, adres zamieszkania i informacje o przedmiocie ubezpieczenia). O niewłaściwej wysyłce poinformowała UODO osoba, która otrzymała maila w wyniku pomyłki w adresie.

UODO zwrócił się do administratora o wyjaśnienie – TUiR Warta potwierdziło, że doszło do incydentu oraz że została przeprowadzona ocena ryzyka naruszenia praw i wolności osób fizycznych w związku z naruszeniem. Ocena wykazała brak konieczności dokonania zgłoszenia – w ocenie administratora mało prawdopodobne było ryzyko naruszenia praw i wolności osób, których dane znajdowały się w mailu.

PUODO doszedł do wniosku, że TUiR Warta naruszyło przepisy związane z obowiązkiem zawiadomienia organu o naruszeniu i w rezultacie nałożyło na spółkę karę pieniężną.

W ocenie PUODO naruszenie wiąże się z wysokim ryzykiem naruszenia ochrony praw lub wolności osób fizycznych – niestety organ nie uzasadnił swojej oceny. W konsekwencji decyzja (pierwsza wydana przez PUODO w zakresie obowiązku notyfikacyjnego) nie daje przedsiębiorcom jasnych wskazówek, jakimi kryteriami kierował się organ przy zakwalifikowaniu incydentu jako nie tylko skutkującego ryzykiem dla praw i wolności, ale jako wywołującym **wysokie ryzyko** dla praw osób.

Decyzja nie jest ostateczna – może zostać zaskarżona do wojewódzkiego sądu administracyjnego.

Z analizy decyzji można już teraz wyciągnąć **wnioski, które mogą być wskazówką co do praktyki organu w przyszłości**:

- **administrator dopuszczając możliwość komunikowania się poprzez pocztę elektroniczną powinien mieć świadomość ryzyk z tym związanych** i wprowadzić np. odpowiednią weryfikację adresu mailowego dla sprawdzenia, czy adres podany przez klienta jest prawidłowy;
- **administrator powinien rozważyć przesyłanie dokumentów zawierających dane osobowe w zaszyfrowanym załączniku**, szczególnie, gdy dotyczy to danych wrażliwych lub zawierających numer PESEL;
- **zwrócenie się z prośbą do niewłaściwego adresata maila o trwałe usunięcie otrzymanej korespondencji nie może być argumentem wskazującym na to, że ryzyko naruszenia praw i wolności osób nie jest wysokie**, gdyż nie ma pewności, czy nieuprawniony adresat nie wykonał, np. kserokopii dokumentów, czy też ich nie utrwalił (organ nie podaje jednak, w jakim celu mogłyby zostać wykorzystane tak utrwalone dane).

Z treścią decyzji można zapoznać się na stronie organu: **link.**

TRANSFER DANYCH OSOBOWYCH DO WIELKIEJ BRYTANII Co dalej?

Transfer danych poza UE

W przypadku, gdy przedsiębiorca planuje przekazanie danych osobowych do państw trzecich (tj. poza obszar Europejskiego Obszaru Gospodarczego) **konieczne jest wdrożenie dodatkowych wymogów w celu zapewnienia odpowiedniego bezpieczeństwa danych**. Przepisy, które należy zastosować dla legalnego przesyłania danych poza EOG, zostały uregulowane w **RODO, które przewiduje kilka mechanizmów dla legalnego transferu danych**. Takim mechanizmem jest m.in. decyzja Komisji Europejskiej o uznaniu państwa trzeciego za zapewniającego adekwatny poziom ochrony danych. W przypadku niewydania takiej decyzji, transfer jest możliwy, jeżeli zapewnione są „odpowiednie zabezpieczenia i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej" (np. za pomocą standardowych klauzul umownych, wiążących reguł korporacyjnych lub zatwierdzonego kodeksu postępowania).

Umowa UE-UK

Unia Europejska i Wielka Brytania zawarły umowę o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej. Zgodnie z nią, **Wielka Brytania nie będzie uważana za państwo trzecie w kontekście transferu danych osobowych z państw członkowskich UE**. Ten okres przejściowy potrwa pół roku – do 1 lipca 2021 r.

Umowa zakłada, że do tego czasu Komisja Europejska wyda odpowiednią decyzję na mocy art. 45 ust. 3 RODO uznającą Wielką Brytanię za państwo zapewniające odpowiedni poziom ochrony danych osobowych.

Transfer danych do UK – co dalej?

Jeżeli – zgodnie z założeniem umowy o handlu i współpracy – Komisja wyda decyzję, administratorzy będą mogli swobodnie kontynuować współpracę z podmiotami mającymi siedzibę w Wielkiej Brytanii.

W naszej ocenie, **warto jak najszybciej zweryfikować współpracę z podmiotami mającymi siedzibę w UK i ustalić, czy dane osobowe są przesyłane z terenu UE do Wielkiej Brytanii**. Dzięki temu przedsiębiorcy będą przygotowani na wciąż możliwy scenariusz, że decyzja Komisji nie zostanie wydana w zakładanym terminie – co oznacza, że dla zalegalizowania transferu po 1 lipca 2021 r. konieczne będzie wdrożenie innych mechanizmów prawnych przewidzianych przez RODO.

W przypadku pytań zachęcamy do kontaktu:

Agnieszka Wiercińska-Krużewska
partner, adwokat
agnieszka.wiercinska@wkb.pl

Karolina Miksa
adwokat
karolina.miksa@wkb.pl