Warszawa, 08.09.2020 r.

Wytyczne organów - przypadkowe ujawnienie danych

Komunikacja elektroniczna jest dziś podstawowym sposobem przesyłania informacji. Wiążą się z nią jednak pewne ryzyka, zwłaszcza jeśli przekazywane komunikaty i dokumenty załączane do wiadomości elektronicznych zawierają dane osobowe. Dane osobowe mogą być również przesyłane pocztą tradycyjną i również ta forma komunikacji nie jest pozbawiona zagrożeń.

Główne ryzyko polega na przypadkowym przesłaniu danych osobowych przez administratora danych osobowych (w praktyce przez jego pracowników/współpracowników) do podmiotu trzeciego. Będziemy mieli wówczas do czynienia z naruszeniem ochrony danych osobowych, które wymaga zarówno działań po stronie administratora, jak i odpowiedniej reakcji przypadkowego odbiorcy danych.

Jakie działania mogą prowadzić do przypadkowego ujawnienia danych osobowych osobie trzeciej? Oto przykłady:

- Bank lub inna instytucja finansowa przypadkowo przesyła korespondencję do niewłaściwego klienta lub osoby niebędącej klientem;
- Urząd przesyła wydaną decyzję lub wezwanie na niewłaściwy adres;
- Firma pozbywa się starego laptopa bez usunięcia danych z dysku, zawierającego informacje działu HR;
- Pomyłka we wpisanym adresie mailowym adresata wiadomości elektronicznej;
- Załączenie do wiadomości email dokumentów dotyczących innej osoby niż adresat wiadomości;
- Nośnik USB zawierający dane klientów zgubiony w pociągu.

Powyższe błędy mogą prowadzić do ujawnienia danych osobowych osobom trzecim, które nie spodziewają się ani nie mają intencji otrzymania takich informacji. Nierzadko informacje do nich trafiające mogą mieć charakter danych wrażliwych. Osoby, które nawet przypadkowo weszły w posiadanie danych osobowych powinny pamiętać, że osoby, których te dane dotyczą, mają określone prawa przysługujące im nie tylko na podstawie przepisów o ochronie danych osobowych, a w szczególności RODO, lecz także na podstawie Europejskiej Konwencji Praw Człowieka czy Karty Praw Podstawowych Unii Europejskiej. **Przypadkowi odbiorcy danych osobowych również mają obowiązek przestrzegać powyższych praw.**

Jak więc mają postępować odbiorcy danych osobowych, a także administratorzy w razie przypadkowego ujawnienia danych osobowych? Wskazówki znajdziecie w poniższej infografice.

Opracowano na podstawie wytycznych irlandzkiego organu nadzorczego.

iSecure

iSecure

PRZYPADKOWE UJAWNIENIE DANYCH OSOBOWYCH

JAK POSTĘPOWAĆ?

WSKAZÓWKI DLA ADMINISTRATORÓW I PRZYPADKOWYCH ODBIORCÓW DANYCH

Administrator

Podejmij działania jak najszybciej po wykryciu błędu i tak, aby prawa osób, których dane dotyczą, nie zostały naruszone. Skontaktuj się z Inspektorem Ochrony Danych, jeśli go wyznaczyłeś, w celu oceny, czy konieczne jest powiadomienie PUODO i ewentualnie osoby, kórej dane dotyczą.

Odbiorca danych

Podejmij działania jak najszybciej i tak, aby prawa osób, których dane dotyczą, nie zostały naruszone. Zidentyfikuj administratora danych (np. na podstawie adresu e-mail lub papieru firmowego nadawcy) i poinformuj go o błędnym ujawnieniu. Nie czekaj, aż skontaktuje się z Tobą.

Zidentyfikuj błędnego odbiorcę danych i poinformuj go o przypadkowym ujawnieniu. Poinformuj go niezwłocznie o dalszym, sposobie postępowania. Może wystarczyć trwałe usunięcie wiadomości e-mail z folderów "skrzynka odbiorcza" i "usunięte pliki". Możesz też zorganizować odebranie od odbiorcy źle zaadresowanego listu lub paczki, lub poprosić o ich bezpieczne zniszczenie i przesłanie pisemnego potwierdzenia, że zostało to zrobione.
Potwierdzenie powinieneś zarchiwizować dla celów dowodowych.

Unikaj otwierania załączników do wiadomości e-mail, plików lub dokumentów, które nie należą do Ciebie.
Ustal z administratorem, jak dalej postąpić. Może wystarczyć trwałe usunięcie wiadomości e-mail z folderów "skrzynka odbiorcza" i "usunięte pliki". Administrator danych może zorganizować odebranie od Ciebie źle zaadresowanego listu lub paczki, lub możesz zgodzić się na ich zniszczenie, na przykład poprzez bezpieczne zniszczenie informacji i pisemne potwierdzenie administratorowi danych, że to zrobiłeś.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa

www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54

fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729

Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686

Kapitał zakładowy opłacony w całości: 50 000,00 zł

Jeśli przypadkowe ujawnienie danych może wiązać się z wysokim ryzykiem dla praw i wolności osoby, której dane dotyczą, powiadom tę osobę o naruszeniu i o tym, jakie działania można podjąć, aby skutki naruszenia zostały zminimalizowane.

Nie próbuj identyfikować i kontaktować się z osobą, do której dane te należą, ponieważ jest to dalsze przetwarzanie informacji i możesz zostać uznany za odrębnego administratora danych. Kontakt z tą osobą pozostaw administratorowi.

Porozmawiaj z pracownikami, którzy przesłali dane osobowe do błędnego adresata. Przypomnij im o zasadach przetwarzania danych osobowych i o konieczności weryfikacji adresatów i przesyłanych do nich dokumentów.

Nie udostępniaj otrzymanych danych innym osobom trzecim, w tym nie udostępniaj ich publicznie na platformach mediów społecznościowych. Zostaniesz wówczas potraktowany jako administrator danych.

Przeprowadź wśród personelu dodatkowe szkolenia z zakresu ochrony danych osobowych.

Jeśli nie możesz zidentyfikować lub skontaktować się z administratorem danych, skontaktuj się z Urzędem Ochrony Danych Osobowych, który powinien pomóc w rozwiązaniu problemu.

Pamiętaj - naruszenie ochrony danych osobowych, jeśli powoduje przynajmniej średnie ryzyko dla praw i wolności osób, których dane dotyczą, wymaga zgłoszenia do Prezesa UODO w ciągu 72 h od wykrycia naruszenia.

Brak zgłoszenia może wiązać się z nałożeniem kary pieniężnej przez organ nadzorczy w wysokości do 10 mln euro.

Pamiętaj - jeśli będziesz przetwarzać dalej otrzymane nawet przypadkowo dane osobowe, możesz zostać uznany za administratora i narazić się na odpowiedzialność cywilną, a nawet karną.

Kto nie jest uprawniony do przetwarzania danych może podlegać karze grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2, a w przypadku danych wrażliwych - do lat 3.

Agnieszka Rapcewicz, Specjalista ds. ochrony danych osobowych iSecure Sp. z o.o.