FUNDACJA „AKADEMIA ANTYKORUPCYJNA”

mgr Krzysztof Śnieżko

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie

e-mail: krzysztof.sniezko/at/protonmail.com

ORCID: 0000-0003-2692-4351

ZAKRES PRZEDMIOTOWY NARUSZEŃ RODO

Przepisy w zakresie ochrony danych osobowych wprowadziły obowiązek informowania przez poszczególnych administratorów danych osobowych Prezesa UODO o stwierdzonych w danym podmiocie naruszeniach przepisów, zarówno w sektorze publicznym jak i w prywatnym. Część naruszeń miała charakter błędów ludzkich, a niektóre dotyczyły braku należytej staranności w ochronie danych osobowych. Zdarzało się również zupełne lekceważenie ochrony w tym zakresie, co skutkowało utratą znacznej ilości danych osobowych. Dochodziło do tego z braku należytego zabezpieczenia informatycznego posiadanych baz danych oraz z zagubienia nośników danych, na których znajdowały się duże zbiory danych osobowych przetwarzanych w podmiocie.

Słowa kluczowe: dane osobowe, RODO, naruszenia, utrata

Od 25 maja do 31 grudnia 2018 r. do UODO wpłynęło 2446 zgłoszeń naruszeń pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w tym 1882 naruszeń zostało zgłoszonych przez podmioty sektora prywatnego, zaś 564 przez podmioty sektora publicznego. W sektorze prywatnym najwięcej zgłoszeń napłynęło od firm:

1. telekomunikacyjnych,
2. ubezpieczeniowych,
3. finansowych (w tym od banków),
4. służby zdrowia.

W sektorze publicznym zgłoszenia incydentów z danymi osobowymi najczęściej przesyłały:

1. jednostki samorządu terytorialnego,
2. szkoły, przedszkola, żłobki,
3. placówki służby zdrowia.

Wśród zgłoszeń w zakresie naruszeń ochrony danych osobowych najczęściej popełniane błędy obejmowały zagadnienia takie jak:

1) brak w przesyłanych zgłoszeniach, niektórych wymaganych informacji np.:
   a) opisu charakteru naruszenia ochrony danych osobowych,
   b) wskazywania kategorii i przybliżonej liczby osób której dotyczyły,
   c) wpisu danych osobowych, których dotyczyły naruszenie,
   d) imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych,
   e) opisu możliwych konsekwencji zgłaszanego naruszenia,
   f) opisu środków zaradczych zastosowanych lub proponowanych przez administratora w celu zminimalizowania negatywnych skutków incydentu;
2) niedokładne, lakoniczne i nierzetelne wypełnianie zgłoszeń, utrudniające właściwą ocenę naruszenia i odpowiednią reakcję na nie np. żądania od administratora powiadomienia właściwych osób;
3) wypełnianie zgłoszeń w sposób rutynowy niedbały i szablonowy a nawet błędny, wynikający z automatycznego przenoszenia informacji dotyczących innych zdarzeń;
4) zgłaszanie naruszeń przez podmiot przetwarzający bądź inny podmiot nie będący administratorem zobowiązanym do zgłoszenia takich incydentów organowi nadzorczemu.

Zakres przedmiotowy naruszeń zgłaszanych przez administratorów z sektora publicznego obejmował najczęściej nieprawidłowości w przetwarzaniu danych osobowych polegające na:

1) udostępnieniu danych osobie innej, niż adresat korespondencji, powstałych wskutek błędu pracowników przy adresowaniu korespondencja niezależnie czy to w formie tradycyjnej czy też emailowej,
2) udostępnieniu bez właściwej anonimizacji danych w trybie dostępu do informacji publicznej,
3) zniszczeniu, zagubieniu czy też kradzież dokumentacji bądź innych nośników np. laptopa czy też telefonu komórkowego, zawierających dane osobowe, a nawet zagubieniu korespondencji przez operatora pocztowego,
4) udostepnieniu danych osobowych osobom nieuprawnionym poprzez błędne wydawania im dokumentów czy też zaświadczeń,
5) złamaniu zabezpieczeń systemów informatycznych, zainstalowaniu złośliwego oprogramowania a nawet zaszyfrowaniu danych uniemożliwiając do nich dostęp osobom uprawnionym,

Najczęściej zgłaszane naruszenia w sektorze prywatnym polegały na:

1) omyłkowym wysłaniu danych osobowych do niewłaściwego odbiorcy (np.: faktura, umowa wysyłana pocztą elektroniczną trafiła do niewłaściwego adresata),
2) uzyskaniu nieuprawnionego dostępu do danych osobowych na skutek luk bezpieczeństwa w systemach informatycznych,
3) wysyłaniu e-maila do wielu adresatów zawierającego wcześniejsze e-maile od innych osób,
4) niezamierzonej publikacji danych osobowych na stronie internetowej firmy,
5) przesłaniu newslettera wraz z adresami e-mail do wszystkich odbiorców newslettera,
6) uzyskaniu dostępu do danych osobowych innego użytkownika przy logowaniu się do konta,
7) utraceniu umowy z klientem,
8) omyłkowym udostępnieniu przez pracownika *call center* w trakcie rozmowy telefonicznej danych innego klienta,
9) zagubieniu czy też kradzieży niezabezpieczonych smartfonów, komputerów przenośnych, dysków zewnętrznych,

10) zagubieniu dokumentacji papierowej zawierającej dane osobowe w trakcie wyjazdów do klientów,
11) uzyskaniu nieuprawnionego dostępu do bazy danych klientów, poprzez ataki hackerskie, w celu wysyłki phishingowych wiadomości SMS służących wyłudzenia danych dostępowych do kont bankowych.

Odpowiednie zabezpieczenie danych osobowych przez podmioty do tego zobowiązane odgrywa istotną rolę w zakresie ich bezpieczeństwa. Chociaż zdarzają się sytuacje przypadkowej utraty danych osobowych, to jednak bardzo duże znaczenie ma właściwe informatyczne zabezpieczenie baz danych, uniemożliwiające dostęp do informacji podmiotom nieuprawnionym.