Ocena naruszenia przy błędnie wysłanym PIT – case study

Czas wysyłania PIT-11 do pracowników to szczególnie gorący okres dla inspektorów ochrony danych. Przesyłek jest mnóstwo, nic zatem dziwnego, że niektóre z nich trafiają do niewłaściwych osób. A to potencjalnie oznacza naruszenie ochrony danych osobowych, które należy przeanalizować pod kątem naruszenia praw i wolności osoby, która została takim incydentem objęta. Z pomocą przychodzi nam na szczęście ENISA, czyli Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, która przygotowała świetny poradnik i jednocześnie metodologię oceny naruszeń, który można zupełnie za darmo pobrać tutaj: Recommendations for a methodology of the assessment of severity of personal data breaches — ENISA (europa.eu).

W poniższym wpisie chciałbym przedstawić jak ta metodologia może być użyta w praktyce na bazie konkretnego case study.

Stan faktyczny:

- W dniu 10 sierpnia 2021 r. pracownik Jest Pięknie Sp. z o.o. („Spółka") zgłosił mailowo do Departamentu HR fakt zmiany adresu zamieszkania. Z uwagi na błąd ludzki zmiana ta nie została odnotowana w systemie teleinformatycznym. Ww. pracownik zakończył współpracę ze Spółką w listopadzie 2021 r.
- W związku z obowiązkiem wystawienia dokumentu PIT-11 oraz ZUS IMIR (Informacja Miesięczna i Roczna) Spółka przygotowała powyższe dokumenty i w dniu 12.02.2022 r. wysłała je do byłego pracownika.
- Z uwagi na fakt, że Spółka nie dokonała aktualizacji adresu zamieszkania zainteresowanego, przesyłka ww. dokumentów została wysłana na poprzedni adres zamieszkania (nie powiązany już w żaden sposób z ex-pracownikiem).
- Następnie Spółka otrzymała w dniu w dniu 17.02.2022 r. informację, że przesyłka została odebrana.
- W dniu 01.03.2022 r. ex-pracownik zgłosił do Spółki, że nie otrzymał do tej pory swojego PIT. Jednocześnie przypomniał, że zgłaszał w stosownym czasie zmianę adresu zamieszkania, co może mieć istotne znaczenie dla sprawy.
- Na podstawie informacji od ex-pracownika Spółka przeprowadziła dochodzenie i ustaliła, że dokumenty PIT i ZUS IMIR zostały wysłane na niewłaściwy adres byłego pracownika.
- W dniu 02.03.2022 r. Departament HR wysłał e-mail do IOD o treści: „Inspektorze, ratuj!" ☺

Podstawowe informacje

- Kategorie podmiotów danych: naruszenie ochrony danych dotyczyło byłego pracownika Spółki
- Zakres danych: imiona i nazwiska, data urodzenia, adres zamieszkania lub pobytu, PESEL, dane dotyczące zarobków, zestawienie należnych składek ZUS (ubezpieczenie społeczne, zdrowotne), zestawienie wypłaconych świadczeń i wynagrodzeń za czas absencji

chorobowej oraz rodzaje i okresy przerw w opłacaniu składek, miejsce pracy (obecnie już nieaktualne).

Biorąc pod uwagę powyższy zakres danych można stwierdzić, że naruszeniem objęte zostały dane proste oraz dane finansowe. Wśród danych objętych naruszeniem nie ma danych wrażliwych.

- Liczba osób i wpisów:
  - liczba osób: 1
  - liczba wpisów: 2
- Źródło naruszenia:
  - wewnętrzne działanie niezamierzone (błąd ludzki)

Kontekst przetwarzania danych (KPD):

KPD ustalamy na podstawie rodzaju danych, którego dotyczyło naruszenie. Jak zostało wskazane powyżej naruszenie dotyczyło danych prostych (współczynnik na potrzeby obliczeń: 2) oraz finansowych (współczynnik na potrzeby obliczeń: 2). Przypisane współczynniki mogą być modyfikowane w zależności od okoliczności, jednak w omawianym przypadku nie będzie miało to zastosowania (brak złej woli). Zgodnie z metodologią bierzemy pod uwagę najwyższy współczynnik – w tym przypadku wynosi on 2 zarówno dla danych zwykłych jak i finansowych. A zatem:
KPD = 2

Łatwość identyfikacji (ŁI):

Poszczególnym poziomom ŁI przypisujemy współczynniki:

- znikoma (identyfikacja za pomocą danych objętych naruszeniem jest bardzo trudna) – 0,25
- ograniczona (identyfikacja za pomocą danych objętych naruszeniem jest trudna) – 0,5
- znacząca (identyfikacja za pomocą danych objętych naruszeniem jest łatwa) – 0,75
- maksymalna (identyfikacja jest bardzo łatwa lub natychmiastowa) – 1

Biorąc pod uwagę zakres danych, którego dotyczy naruszenie, mamy tu maksymalną łatwość identyfikacji, czyli:

ŁI = 1

Okoliczności naruszenia (ON):

Elementy, które rozpatrywane są w kontekście ON to utrata bezpieczeństwa (w odniesieniu do poufności, integralności, dostępności) oraz ew. złe intencje. Naruszenie, do którego doszło w Spółce spowodowało utratę poufności danych (dostęp do danych mogła uzyskać osoba nieuprawniona). Naruszenie nie jest skutkiem złych intencji. Przypisujemy zatem współczynnik na potrzeby obliczeń:

- utrata poufności danych – współczynnik 0,25 (dane zostały wysłane – w formie przesyłki pocztowej – do nieuprawnionego odbiorcy; nie ma pewności, że odbiorca

zapoznał się z danymi, brak też informacji ilu mogło być potencjalnych odbiorców np. współdomowników błędnego odbiorcy)

Podsumowując:
ON = 0,25

Powaga naruszenia (PN):

PN = KPD x ŁI + ON
PN = 2 x 1 + 0,25
PN = 2,25

Zgodnie z metodologią ENISA, jeśli wartość PN mieści się w przedziale 2 ≤ PN < 3 mamy do czynienia ze średnią powagą naruszenia. Osoba, która została objęta naruszeniem, może napotykać znaczne niedogodności, z którymi będzie w stanie sobie poradzić pomimo kilku trudności (dodatkowe koszty, odmowa dostępu do usług biznesowych, strach, niezrozumienie, stres, drobne dolegliwości fizyczne, itp.).

Średnia powaga naruszenia oznacza dla Spółki konieczność:

- dokonania wpisu do rejestru naruszeń
- wdrożenie środków zaradczych
- powiadomienie organu nadzorczego (PUODO)
- powiadomienie podmiotów danych (rekomendowane wyłącznie z uwagi na to, że w ramach dokumentów znajdował się numer ewidencyjny PESEL)

Michał Sztąberek – ekspert ds. ochrony danych osobowych / prezes zarządu iSecure Sp. z o.o.