Metoda oceny wagi naruszenia wg ENISA

Ocena naruszenia stwarza problemy. Dlatego przedstawiamy opracowaną przez ENISA (Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji) metodę oceny wagi naruszenia. Narzędzie pozwala na ocenę wagi naruszeń danych i ułatwia podjęcie decyzji zarówno o powiadomieniu organu, jak i osób, których dane zostały naruszone.

Mariola Więckowska

Wagę naruszenia danych osobowych określa stopień potencjalnego wpływu na prawa lub wolności osób, których dotyczy naruszenie. Rodo wiąże to z powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Metoda pozwala administratorowi dokonać ogólnej oceny wagi naruszenia poprzez określenie konkretnych kryteriów ilościowych.

Metoda wykorzystuje informacje, które administrator posiada w momencie naruszenia, zatem nie zawsze obejmie ona wszystkie możliwe oddziaływania na osoby.

OCENA WAGI NARUSZENIA (WN)

WN oblicza się za pomocą trzech czynników, które administrator powinien ocenić:

$$WN = KPD \times PI + ON$$

gdzie:

- KPD – Kontekst Przetwarzania Danych, jest to główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania
- PI – Prawdopodobieństwo Identyfikacji, to czynnik korygujący KPD, który może obniżyć wynik i oznacza łatwość identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały do nich dostęp
- ON – Okoliczności Naruszenia, to czynnik wzmacniający wagę naruszenia, który odnosi się do jego okoliczności i może wystąpić bądź nie

KONTEKST PRZETWARZANIA DANYCH (KPD)

Metoda oparta jest na czterech kategoriach danych, jednak zawsze powinny być uwzględnione czynniki kontekstowe związane z danymi. Podstawową ocenę należy traktować jako ogólne wskazanie krytyczności związanej z kategorią danych, a KPD będzie miał wartość od 1 do 4.

$$KPD = A+B$$

gdzie:

- A – określa rodzaj i poziom kategorii danych osobowych związanych z naruszeniem:
  - Dane podstawowe = 1
  - Dane dotyczące zachowań osoby (behawioralne) = 2
  - Dane finansowe lub poufne = 3
  - Dane szczególne = 4
- B – określa czynniki kontekstu przetwarzania danych, które mogą podwyższyć lub obniżyć ocenę:
  - Szeroki zakres danych dla tej samej osoby (+): zakres powinien być rozpatrywany zarówno pod względem czasu trwania naruszenia (np. te same dane przez pewien czas), jak i zakresu danych, np. czynnik będzie wyższy dla listy transakcji bankowych z całego roku niż dla pojedynczej transakcji
  - Duży wolumen danych (+): liczba osób, których dotyczy naruszenie, przekracza np. 100, co oznacza większą skalę incydentu
  - Specyfika administratora (+): może ujawniać dodatkowe informacje, np. czynnik będzie wyższy dla listy klientów apteki internetowej niż sklepu papierniczego
  - Specyfika podmiotu danych (+): osoby wymagające szczególnej opieki, w tym dzieci, osoby ubezwłasnowolnione, pozbawione praw publicznych lub osoby należące do grupy, która ze względu na swoją specyfikę obarczona jest wyższym ryzykiem, np. czynnik zostanie podwyższony dla danych osób zatrudnionych w tajnych służbach
  - Możliwe negatywne skutki dla podmiotu danych (+)
  - Nieważność danych (-): gdy dane utraciły znaczenie lub są nieaktualne, np. nieaktualna lista adresów pocztowych osób, do których nie można już wysłać listów
  - Dostępność publiczna (-): dane były publicznie dostępne przed naruszeniem
  - Charakter danych: wpływa na zwiększenie lub zmniejszenie oceny, np. zaświadczenie lekarskie, które poświadcza dobry stan zdrowia osoby i nie ujawnia żadnych innych informacji, mimo że jest kategorią szczególną = 4, to ostatecznie przyjmie wartość 1, gdyż nie, wpływa na ryzyko naruszenia praw lub wolności osoby. Czynnik ten należy rozważyć z wielką starannością i wyjaśnić, dlaczego obniżono podstawowy wynik KPD

Jeżeli zdecydujemy się na zmianę podstawy KPD, to nowy wynik powinien być poparty wyjaśnieniem opisującym czynniki kontekstowe naruszenia i ich wpływ na podmiot danych.

PRAWDOPODOBIEŃSTWO IDENTYFIKACJI (PI)

PI jest czynnikiem korygującym KPD, który ocenia, jak łatwo będzie stronie mającej dostęp do danych jednoznacznie zidentyfikować konkretną osobę.

Definiując PI, powinniśmy brać pod uwagę wszelkie racjonalne środki, które wpływają na identyfikację osób, w tym, m.in. dane publiczne oraz dostępne w internecie.

PI przyjmuje cztery poziomy:

- Znikome = 0,25 (trudno zidentyfikować osobę, ale nadal jest to możliwe w określonych warunkach, np. w kraju jest wiele osób, które noszą to samo nazwisko – Kowalski)

- Ograniczone = 0.5 (w kraju jest kilka osób o tym samym nazwisku)
- Wysokie = 0.75 (w mieście jest 1 lub kilka osób o tym samym nazwisku)
- Maksymalne = 1 (możliwość bezpośredniej identyfikacji osoby, bez dodatkowych działań, np. oprócz nazwiska, dostępna jest data urodzin i e-mail)

OKOLICZNOŚCI NARUSZENIA (ON)

W ON rozpatrujemy atrybuty bezpieczeństwa, czyli poufność, integralność, dostępność oraz intencjonalne działanie:

- Naruszenie poufności (NP): dane ujawnione:
  - znanym nieuprawnionym odbiorcom (+0.25)
  - nieznanej liczbie nieuprawnionych odbiorców (+0.5)
- Naruszenie integralności (NI): dane są zmienione, ale:
  - możliwe jest ich odzyskanie (+0.25)
  - brak jest możliwości ich odzyskania (+0.5)
- Naruszenie dostępności (ND): dane niedostępne:
  - tymczasowo (+0.25)
  - stałe, bez możliwości ich odzyskania (+0.5)
- Intencjonalne działanie sprawcy (IDS): czynnik zwiększający prawdopodobieństwo nieprawidłowego wykorzystania danych, np. włamanie lub kradzież danych w celu ich sprzedaży lub ujawnienia
  - IDS = (+0.5)

Wartość ON jest sumą czynników: ON = NP + NI + ND + IDS

CZYNNIK DODATKOWY (CD)

Na ostateczną wartość WN może wpłynąć CD, który, mimo że nie jest uwzględniony w WN, może być ważny dla końcowej decyzji. Chodzi tu o zastosowanie technik szyfrowania i pseudonimizacji danych jako czynnika zwiększającego ich bezpieczeństwo. Techniki te powodują, że dane są dostępne jedynie w nieczytelnej formie lub są całkowicie niedostępne, przez co znacznie zmniejsza się prawdopodobieństwo uzyskania dostępu do nich przez nieuprawnione osoby i negatywnego wpływu na podmioty danych. Uwzględnijmy to, zmniejszając odpowiednio prawdopodobieństwo identyfikacji, np. PI=0.25.

WN przy uwzględnieniu CD może być wyznacznikiem konieczności powiadamiania UODO o naruszeniu oraz decyzji o zawiadomieniu osób, których dane zostały naruszone.

PODSUMOWANIE

Przedstawiona metoda oceny wagi naruszenia danych jest na tyle obiektywna, powtarzalna i elastyczna, że może być zaadaptowana przez różne kategorie administratorów w celu wykazania się przed organem nadzorczym z przeprowadzenia oceny prawdopodobieństwa naruszenia praw lub wolności osób, których dane uległy naruszeniu zgodnie z zasadą rozliczalności.

PRZYKŁADY OCENY WN:

Zgubienie niezaszyfrowanego pendrive'a z listą 250 uczestników konferencji

1. Konferencja naukowa

Zakres danych: imię, nazwisko, e-mail

KPD = A + B = 1 (dane podstawowe) + 0 (brak) = 1

PI = 1

ON = NP+NI+ND+IDS = 0,5 (nieznana liczba odbiorców) + 0 + 0,25 (czasowa niedostępność) + 0 = 0.75 WN = KPD * PI + ON = 1 * 1 + 0.75 = 1.75 WN = Niska

2. Konferencja dla rodziców dzieci chorych na ...

Zakres danych: imię, nazwisko, e-mail

KPD = A + B = 1 (dane podstawowe) + 2 (specyfika administratora i możliwe negatywne skutki dla podmiotu danych) = 3

PI = 1

ON = NP+NI+ND+IDS = 0,5 (nieznana liczba odbiorców) + 0 + 0,25 (czasowa niedostępność) + 0 = 0.75 WN = KPD * PI + ON = 3 * 1 + 0.75 = 3.75

WN = Wysoka

Jeżeli pendrive byłby zaszyfrowany bezpiecznym algorytmem i hasłem, które nie zostało ujawnione, to WN może być zmniejszona nawet do poziomu niskiego. ■

Autorka pracuje w LexDigital jako Head of Privacy Innovative Technologies; pomaga wykorzystywać i wdrożyć nowe technologie w zgodzie z obowiązującymi zasadami ochrony i bezpieczeństwa danych osobowych.

Tabela 1. Przykłady oceny KPD

Dane podstawowe, np. dane kontaktowe, imię i nazwisko, e-mail, wykształcenie, doświadczenie zawodowe	Wynik
Domyślny wynik, kiedy nie są znane żadne dodatkowe czynniki	1
Zwiększenie o 1, np. kiedy ilość danych lub specyfika administratora umożliwiają profilowanie behawioralne danej osoby	2
Zwiększenie o 2, np. kiedy ilość danych lub cechy administratora pozwalają wywnioskować informacje finansowe, poufne	3
Zwiększenie o 3, np. kiedy specyfika administratora lub osoby może prowadzić do pozyskania danych szczególnych lub o przynależności osoby do grupy szczególnie zagrożonej, np. dzieci, i mogą mieć one kluczowe znaczenie dla ich bezpieczeństwa osobistego lub warunków fizycznych lub psychicznych	4

Dane dotyczące zachowań (behawioralne), np. dane geolokacyjne, dane dotyczące osobistych preferencji i nawyków	Wynik
Zmniejszenie o 1, np. kiedy charakter zbioru danych nie pozwala na profilowanie zachowań danej osoby lub dane są publicznie dostępne	1
Domyślny wynik, kiedy nie są znane żadne dodatkowe czynniki	2
Zwiększenie o 1, np. kiedy ilość danych lub specyfika administratora pozwalają stworzyć profil społeczny lub finansowy	3
Zwiększenie o 2, np. kiedy ilość danych lub specyfika administratora pozwalają stworzyć profil dotyczący danych szczególnych	4

Dane finansowe lub poufne, np. dochód, transakcje finansowe, wyciągi bankowe, inwestycje, karty kredytowe, faktury, pomoc społeczna	Wynik
Zmniejszenie o 2, np. kiedy dane nie zawierają istotnych danych finansowych lub dane są publicznie dostępne	1
Zmniejszenie o 1, np. kiedy dane zawierają dane finansowe, które jednak nie pozwalają na określenie sytuacji finansowej osób, np. tylko numery rachunków bankowych	2
Domyślny wynik, kiedy nie są znane żadne dodatkowe czynniki	3
Zwiększenie o 1, np. kiedy dane lub ich charakter pozwalają wywnioskować dane szczególne lub stworzyć profil społeczny lub finansowy umożliwiający oszustwo lub kradzież tożsamości	4

Dane szczególne, np. stan zdrowia, preferencje seksualne, przekonania polityczne lub religijne, przynależność do grup szczególnie zagrożonych, dzieci	Wynik
Zmniejszenie o 3, np. kiedy dane są publicznie dostępne	1
Zmniejszenie o 2, np. kiedy charakter danych może jedynie prowadzić do ogólnych założeń i odkrycia informacji behawioralnych	2
Zmniejszenie o 1, np. kiedy charakter danych może prowadzić tylko do informacji finansowych lub poufnych	3
Domyślny wynik, gdy nie są znane żadne dodatkowe czynniki	4

Tabela 2. Waga naruszenia

Wynik	Waga naruszenia	Opis	Działanie
WN<2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności	Odnotowanie incydentu w rejestrze incydentów (RI)
2<=WN<3	Średnia	Osoby mogą napotkać niedogodności, które są możliwe do pokonania	Odnotowanie incydentu w RI oraz zgłoszenie do UODO
3<=WN<4	Wysoka	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami	Odnotowanie incydentu w RI oraz zgłoszenie do UODO
4<=WN	Bardzo wysoka	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje	Odnotowanie incydentu w RI, zgłoszenie do UODO oraz powiadomienie osób, których dane zostały naruszone