FUNDACJA bezpieczna cyberprzestrzeń

Jak mierzyć poziom/wagę naruszenia bezpieczeństwa danych osobowych?

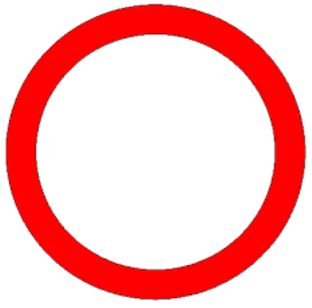
Mirosław Maj, Cyprian Gutkowski

Katalog kar za naruszenia

W razie stwierdzenia naruszeń RODO organ nadzorczy jest uprawniony w szczególności do:

- wydawania ostrzeżeń przedsiębiorcom przetwarzającym dane osobowe dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;
- udzielania upomnień przedsiębiorcom przetwarzającym dane osobowe w przypadku naruszenia przepisów RODO przez operacje przetwarzania;
- nakazania przedsiębiorcom przetwarzającym dane osobowe spełnienia żądań osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO;
- nakazania przedsiębiorcom przetwarzającym dane osobowe dostosowania operacji przetwarzania do przepisów RODO, a w szczególności, w stosownych przypadkach wskazania sposobu i terminu dostosowania;
- nakazania przedsiębiorcom przetwarzającym dane osobowe zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzenia czasowego lub całkowitego ograniczenia przetwarzania danych, w tym zakazu przetwarzania;
- nakazania sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazania powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu cofnięcia certyfikacji lub nakazania podmiotowi certyfikującemu nieudzielenia certyfikacji;
- nakazania zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Gradacja środków



Komisja Europejska wskazała kolejność stosowania środków prawnych, które przysługują organom nadzorczym:

- ostrzeżenie,
- nagana,
- zawieszenie przetwarzania danych,
- grzywna.

Kolejność jaką wskazała Komisja Europejska NIE JEST PRZYPADKOWA. Kary finansowe według niej są środkiem OSTATNIM.

Proces ustalania wysokości kar

Czynniki wpływające na wysokość i rodzaj kary:

- charakter, czas i waga naruszenia
- umyślność lub nieumyślność podmiotu
- wdrożone środki organizacyjne oraz techniczne
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu
- wcześniejsze naruszenia ze strony administratora
- kategorie danych osobowych, których dotyczyło naruszenie.

Jak ustalić wagę naruszenia?

Recommendations for a methodology of the assessment of severity of personal data breaches.

enisa
European Network and Information Security Agency

Algorytm wagi naruszenia

Narzędzie to pozwala wyliczyć wagę naruszenia, dzięki zastosowaniu następującego wzoru:

$$SE = DPC \times EI + CB$$

SE	waga naruszenia
DPC	kontekst przetwarzania danych, rodzaj naruszonych danych dostosowany do kontekstu przetwarzania
EI	łatwość identyfikacji osoby w oparciu o naruszone dane
CB	okoliczności naruszenia, mające dodatkowy wpływ na dotkliwość naruszenia (poufność, integralność, dostępność)

Do czego ma służyć algorytm?

Algorytm ma służyć pomocą:

- organowi nadzorczemu,
- administratorom i podmiotom przetwarzającym dane osobowe,
- inspektorom ochrony danych,
- wszystkim zajmującym się obsługą incydentów związanych z naruszeniami ochrony danych osobowych.

Szacowanie kontekstu przetwarzania (DPC)

Co w przypadku, jeśli nie wiemy dokładnie co wyciekło?

Jeśli są to **dane podstawowe** „simple data”, uzyskują **wartość 1**.

Jeśli są to **dane behawioralne**, pozwalające ustalić preferencje, lokalizację, status społeczny, powinny otrzymać we wzorze **wartość 2**.

Jeśli są to **dane finansowe**, mające związek z saldem, transakcjami, numerami kart, powinny otrzymać **wartość 3**.

Jeśli są to **dane wrażliwe**, powinny otrzymać **wartość 4**.

Szacowanie kontekstu przetwarzania (DPC)

SE = DPC x EI + CB

Lista klientów z numerem telefonu	Wynik	Przyczyna oceny
Kino	1	Brak możliwości powiązań kontekstowych
Luksusowy salon samochodowy	2	Pozwala na identyfikację statusu
Apteka sprzedająca leki dla diabetyków	3	Dane o stanie zdrowia
Lista informatorów CBŚP	4	Dane krytyczne dla bezpieczeństwa
Z sieci społecznościowych	Wynik	Przyczyna oceny
Ogólnie dostępnych (publicznych)	1	Dane ogólnie odstepne
Tylko dla znajomych (bez zdradzania preferencji)	2	Pozwala na identyfikację statusu
Tylko dla znajomytch zdradzających preferencje	3	Może nastąpić profilowanie
Prywatne wiadomości	4	Ujawnione dane wrażliwe
Informacje finansowe, dane kart kredytowych	Wynik	Przyczyna oceny
Dane kart ale mają więcej niż 10 lat	1	przedawnione
Sklep ale brak danych do wykonania transakcji	2	Informacje mogą określić status finansowy
Dane bankowe o niektórych zakupach bez możliwości zidentyfikownia osoby fizycznej	3	Ważne dane ale nie da się powiązać kontekstowo
Pełne dane	4	Możliwy fraud
Dane związane z polityką	Wynik	Przyczyna oceny
Dane liderów partyjnych	1	Publicznie znane
Zdjęcia z eventów partyjnych	2	Tylko generalne przypisanie
Dane mówców na konferencjach partyjnych	3	Pozwala na przypisanie poglądów politycznych
Dane członków partii	4	Przypisane poglądy

Szacowanie łatwości identyfikacji (EI)

SE = DPC x EI + CB

Co naruszone	Wynik EI	Przyczyna oceny
Imię i nazwisko	0,25	W populacji bardzo dużo osób o takich samych danych
Imię i nazwisko	0,5	W populacji wiele osób o takich samych danych
Imię i nazwisko	0,75	Mała grupa osób o tych danych w populacji
Imię i nazwisko	1	Dane bardzo łatwe do zidentyfikowania

Co naruszone	Wynik EI	Przyczyna oceny
Zdjęcie	0,25	Zdjęcie niewyraźne, z daleka, kamery przemysłowe
Zdjęcie	0,5	Zdjęcie niewyraźne ale zawiera informacje o lokalizacji osoby
Zdjęcie	0,75	Wyraźne zdjęcie ale bez wszelkich innych danych
Zdjęcie	1	Zdjęcie wyraźne i osoba łatwa do zidentyfikowania, poprzez inne informacje na nim zawarte

Co naruszone	Wynik EI	Przyczyna oceny
Numer telefonu	0,25	Gdy numer publicznie nie jest dostępny w książkach telefonicznych
Numer telefonu	0,75	Gdy numer telefonu wskazuje na małą miejscowość a nie jest publicznie dostępny
Numer telefonu	1	Gdy numer i dane osoby można odnaleźć w publicznej książce telefonicznej

Co naruszone	Wynik EI	Przyczyna oceny
ID	0,25	Gdy ustalenie danych po samym rekordzie jest niemożliwe
ID	0,75	Gdy rekord zawiera dane adresowe np. telefon lub e-mail
ID	1	Gdy rekord zawiera dane dodatkowe takie jak imię i nazwisko, zdjęcie, dane adresowe

Co naruszone	Wynik EI	Przyczyna oceny
Alias/Nick	0,25	Całkowicie nierozpoznawalny rekord, typu „Obywatel”
Alias/Nick	0,75	Rekord zawiera część prawdziwych danych, np. imię albo nazwisko
Alias/Nick	1	Rekord zawiera dane z imieniem i nazwiskiem osoby

Szacowanie okoliczności naruszenia (CB)

SE = DPC x EI + CB

Wynik CB (utrata poufności)	Przyczyna oceny
0	Nastąpiło naruszenie, ale bez dowodów świadczących o nielegalnym przetwarzaniu.
0,25	Dane zostały ujawnione znanym odbiorcom.
0,5	Dane zostały ujawnione nieznanym odbiorcom.

Wynik CB (utrata dostępności)	Przyczyna oceny
0	Dane mogą być odzyskane bez żadnego problemu.
0,25	Dane czasowo niedostępne, konieczne skorzystanie z backup'ów.
0,5	Dane stracone bez możliwości odzyskania.

Wynik CB (utrata integralności)	Przyczyna oceny
0	Dane zmienione, ale bez dowodów świadczących o nieautoryzowanym użyciu.
0,25	Dane zmienione i ewentualnie wykorzystane w nieprawidłowy lub nielegalny sposób, ale z możliwością odzyskania.
0,5	Dane zmienione i ewentualnie wykorzystane w nieprawidłowy lub nielegalny sposób bez możliwości odzyskania.

Jeśli naruszenie wynikało z celowego działania, np. w celu spowodowania problemu administratorowi danych (np. wykazania utraty bezpieczeństwa) i / lub w celu wyrządzenia szkody osobom fizycznym, należy doliczyć 0,5 do wartości CB.

Zgodnie z różnymi wymaganiami, punktacja może być dostosowana do konkretnej sytuacji w celu uzyskania właściwych wyników.

Waga naruszenia

Wynik SE	Waga	Wyjaśnienie
SE < 2	Niska	Osoby fizyczne nie zostaną dotknięte naruszeniem, lub wywoła ono skutki minimalne.
2 = SE < 3	Średnia	Mogą wystąpić niedogodności, ale będą one łatwe do wyeliminowania.
3 = SE < 4	Wysoka	Mogą wystąpić poważne niedogodności, możliwe do przezwyciężenia, ale z poważnymi trudnościami.
4 ≤ SE	Bardzo wysoka	Mogą wystąpić poważne, a nawet nieodwracalne konsekwencje.

Case study 1

Mail o rezerwacji stolików w restauracji, przez przypadek został wysłany do wszystkich klientów, którzy tego dnia zamówili stolik w restauracji. Można odczytać z niego imię i adres mailowy zamawiającego.

SE = DPC x EI + CB

- DPC=1 (dane o podstawowym kontekście)
- EI=0,75 (ponieważ maile zawierają imię lub nazwisko)
- CB=0,25 (dane ujawniono znanym odbiorcom)

SE = 1 x 0,75 + 0,25

SE = 1

Case study 2

Nastąpiło włamanie hakerskie do systemu teatru. W wyniku włamania skasowano dane o sprzedanych biletach, wraz z danymi klientów płacących złotą kartą (imię, nazwisko, telefon, adres email), niestety administrator nie prowadził backupów. Zmieniono również hasła klientów korzystających z usług on-line.

SE = DPC x EI + CB

- DPC=2 (dane pozwalające rozpoznać status)
- EI=1 (ponieważ rekord zawiera imię i nazwisko)
- CB=1,5 (zsumowanie poufności, dostępności, integralności), dodatkowo „premia” 0,5 za umyślność.

SE = 2 x 1 + 0,5 + 0,5 + 0,5 + 0,5

SE = 4

Seminarium FBC

- 24 kwietnia 2018
- Warszawa
  - Centrum Konferencyjne NIMBUS
- Więcej
  - www.cybsecurity.org

Dziękujemy za uwagę

miroslaw.maj@cybsecurity.org
cyprian.gutkowski@cybsecurity.org