# **Procedura oceny poziomu naruszenia bezpieczeństwa danych**

Celem procedury jest ocena poziomu naruszenia bezpieczeństwa danych osobowych w celu określenia trybu i zasad postępowania osób upoważnionych do przetwarzania danych osobowych, w przypadku gdy stwierdzono naruszenie ochrony danych osobowych.

1. Za przeprowadzenie oceny poziomu naruszenia bezpieczeństwa danych odpowiada Inspektor Ochrony Danych.
2. Niezależnie od wyniku oceny incydent odnotowany zostaje w prowadzonym przez Administratora Danych Osobowych w ewidencji naruszeń bezpieczeństwa danych osobowych.
3. Opis metody oceny wagi naruszenia bezpieczeństwa danych osobowych.
	1. Metoda oceny wagi naruszenia opracowana wg. Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)
	2. Waga naruszenia

**WN = KPD \* PI + ON**

* Waga Naruszenia - **WN**
* Kontekst Przetwarzania Danych - **KPD**
	+ główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania
* Prawdopodobieństwo Identyfikacji - **PI**
	+ czynnik korygujący KPD, który może obniżyć wynik. Prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich
* Okoliczności Naruszenia - **ON**
	+ czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku.
	1. Kontekst Przetwarzania Danych

**KPD = A + B**

|  |
| --- |
| A |
| Rodzaj wrażliwości danych | **Poziom wrażliwości danych** |
| Dane podstawowe  | 1 |
| Dane behawioralne | 2 |
| Dane finansowe | 3 |
| Dane szczególne | 4 |

|  |
| --- |
| B |
| Kontekst przetwarzania | **Podwyższenie lub obniżenie wyceny** |
| Szeroki zakres danych/wolumen danych  | (+) |
| Charakter danych  | (+/-) |
| Specyfika podmiotu danych lub administratora  | (+/-) |
| Możliwe negatywne skutki dla podmiotu danych  | (+) |
| Publiczna dostępność danych przed naruszeniem  | (-) |
| Nieważność danych | (-) |

* 1. Prawdopodobieństwo identyfikacji **(PI)**

Znikome - 0,25

Ograniczone - 0,5

Wysokie - 0,75

Maksymalne – 1

* 1. Okoliczności Naruszenia

**ON = NP + NI + ND + ID**

|  |  |
| --- | --- |
| ON |  |
| Naruszenie Poufności  | Dane ujawnione znanym odbiorcom danych (+0,25)Dane ujawnione nieznanej liczbie odbiorców danych (+0,5) |
| Naruszenie Integralności  | Dane zmienione i możliwe jest ich odzyskanie (+0,25)Brak jest możliwości ich odzyskania (+0,5) |
| Naruszenie Dostępności  | Niedostępność danych czasowa (+0,25)Pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5) |
| Intencjonalne Działanie  | Intencjonalne Działanie Sprawcy (+0,5) |

* 1. Ocena wagi naruszenia

|  |  |  |
| --- | --- | --- |
| **Wynik**  | **Waga naruszenia** | **Opis** |
| WN<2  | Niska  | Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności |
| 2<=WN<3 | Średnia | Osoby mogą napotkać niedogodności, które są możliwe do pokonania |
| 3<=WN<4 | Wysoka | Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami |
| 4<=WN | Bardzo wysoka | Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje |