.

PROCEDURA WYKRYWANIA I KLASYFIKOWANIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH W OSOBOWYCH W FIRMIE: BIURO RACHUNKOWE VECTIGAL CONSULTING EWA DĄBROWSKA

…

1. Zgłoszenie i wykrywanie naruszeń
   1.1. Każda z osób, która poweźmie wiarygodną informację dotyczącą możliwości wystąpienia naruszenia ochrony danych osobowych zobowiązana jest do niezwłocznego poinformowania o tym fakcie Inspektora ochrony danych osobowych, w przypadku gdyby nie został on powołany, Administratora danych osobowych,
   1.2. Podmiot przyjmujący zgłoszenie, przy udziale osoby informującej o naruszeniu, sporządza Raport z incydentu naruszenia bezpieczeństwa danych osobowych, którego wzór stanowi załącznik nr 1 do niniejszej procedury.
   1.3. Osoba sporządzająca raport zobowiązana jest zweryfikować informacje przekazane przez zgłaszającego oraz:
      1.3.1. gdy nie zostaną one potwierdzone, odnotować go w raporcie i zakończyć procedurę,
      1.3.2. gdy zostaną potwierdzone, przejść do przeprowadzenia klasyfikacji naruszenia ochrony danych osobowych zgodnie z punktem 2,
      1.3.3. wpisać zgłoszone naruszenie do Rejestru naruszeń ochrony danych osobowych.
   1.4. Inspektor ochrony danych osobowych, Administrator systemów informatycznych lub inny podmiot wyznaczony przez Administratora danych osobowych zobowiązany jest do okresowego wykonywania audytów mających na celu weryfikację przestrzegania zasad bezpieczeństwa ochrony danych osobowych. Zakres audytu oraz jego termin jego przeprowadzenia każdorazowo określa Administrator danych osobowych. Przy czym audyt obejmujący wszystkie komórki organizacyjne należy przeprowadzić nie rzadziej niż raz na 12 miesięcy.
   1.5. W przypadku wykrycia naruszeń ochrony danych osobowych w czasie audytu, osoba przeprowadzająca audyt postępuje zgodnie z punktami 1.2 oraz 1.3.
   1.6. Jeżeli wykryte naruszenie ochrony danych osobowych lub jego skutki mogą mieć wpływ na treść prowadzonych rejestrów należy zastosować Procedurę aktualizacji rejestrów.

Komórki odpowiedzialne: inspektor ochrony danych osobowych, administrator systemów informatycznych, obsługa prawna

2. Klasyfikacja naruszenia
   2.1. Klasyfikacji rodzaju naruszenia dokonuje inspektor ochrony danych osobowych, w razie konieczności we współpracy z administratorem systemów informatycznych lub obsługą prawną,
   2.2. Proces szacowania ryzyka naruszenia ochrony danych osobowych składa się z następujących etapów:

Krok 1. **<u>Określenie potencjalnych następstw realizacji ryzyka naruszenia ochrony</u>** danych osobowych przetwarzanych [DO], opisanych współczynnikiem N. **Im poważniejsze są konsekwencja incydentu naruszenia ochrony DO dla naruszenia praw lub wolności osób fizycznych, których dane osobowe są przetwarzane w określonym zbiorze, tym wyższy jest współczynnik N danego zbioru**. Przez ryzyko naruszenia praw lub wolności osób fizycznych rozumie się wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą (powstanie uszczerbku fizycznego lub szkody majątkowej/niemajątkowej tej osoby). **Współczynnik N może przyjmować wartość: 3 – niskie konsekwencje, 6 – średnie konsekwencje, 9 – wysokie konsekwencje. Współczynnik N określany jest przez osobę dokonującą klasyfikacji naruszenia na podstawie zweryfikowanego Raportu z incydentu naruszenia bezpieczeństwa danych osobowych.**

Krok 2. **<u>Określenie zasobów, w których doszło do naruszenia</u>**. Zasoby te mogą stanowić zarówno miejsca fizyczne (np. konkretne pomieszczenie), ich części (np. szafa w pomieszczeniu), a także określać lokalizacje logiczne (np. serwery).W razie potrzeby lista zasobów jest aktualizowana. **Zasoby te określane są przez osobę dokonującą klasyfikacji naruszenia na podstawie zweryfikowanego Raportu z incydentu naruszenia bezpieczeństwa danych osobowych.**

Krok 3. **<u>Określenie poziomu bezpieczeństwa (B) jaki gwarantują poszczególne zasoby</u>** w których doszło do naruszenia, poprzez prawdopodobieństwo realizacji określonego zagrożenia (np. wycieku danych osobowych). Dla każdego z zagrożeń osoba dokonująca analizy ryzyka przyporządkowuje **prawdopodobieństwo jego realizacji określone w skali niskie (3), średnie (6), wysokie (9)**. Wartości współczynnika B zawierają się w przedziale <3,9>.

Krok 4. **<u>Obliczenie poziomu ryzyka</u>**. Dla każdej z komórki macierzy (Zbioru danych osobowych) x (Zasoby wykorzystywane do przetwarzania informacji) określone zostaje ryzyko **obliczone według wzoru R = N*B**. Wartości współczynnika R zawierają się w przedziale <9,81>. Im wyższa wartość współczynnika R, tym większe ryzyko naruszenia ochrony danych osobowych przetwarzanych z wykorzystaniem określonego zasobu.

Dla potrzeb oceny przyjęto następującą metodę klasyfikacji ryzyka:

Ryzyko naruszenia ochrony danych osobowych	Przedział współczynnika R
niskie	<9-25)
średnie	<25-50)
wysokie	<50-81>

Graficzne przedstawienie możliwych do uzyskania wyników przedstawia **Rysunek 1.**

	3	4	5	6	7	8	9
3	9,0	12,0	15,0	18,0	21,0	24,0	27,0
4	12,0	16,0	20,0	24,0	28,0	32,0	36,0
5	15,0	20,0	25,0	30,0	35,0	40,0	45,0
6	18,0	24,0	30,0	36,0	42,0	48,0	54,0
7	21,0	28,0	35,0	42,0	49,0	56,0	63,0
8	24,0	32,0	40,0	48,0	56,0	64,0	72,0
9	27,0	36,0	45,0	54,0	63,0	72,0	81,0

Kryteria klasyfikacji ryzyka:

- Ryzyka w przedziale niskie – tj. wrt. współczynnika <9,25> - naruszenie nieistotne,
- Ryzyka w przedziale średnim – tj. wrt. <25,50> - naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych,
- Ryzyka w przedziale wysokie – tj. wrt. współczynnika <50,81> - naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

Komórki odpowiedzialne: inspektor ochrony danych osobowych, administrator systemów informatycznych, obsługa prawna

3. Działania następcze
   3.1. Po określeniu poziomu ryzyka związanego z danym naruszeniem ochrony danych osobowych należy przejść do Procedury zawiadamiania o naruszeniu ochrony danych osobowych,
   3.2. Jeżeli wykryto naruszenie ochrony danych osobowych Inspektor ochrony danych osobowych, Administrator systemów informatycznych albo inna osoba wskazana przez Administratora danych osobowych zobowiązana jest do przedłożenia rekomendacji w zakresie zmian mających na celu wyeliminowanie zidentyfikowanego ryzyka w przyszłości.
   3.3. Podmiot odbierający zgłoszenie dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania prawa przez organizację,
   3.4. Jeżeli stwierdzone zostanie, że do naruszenia ochrony danych osobowych doszło z winy konkretnego podmiotu należy:
      3.4.1. W przypadku pracowników – zawiadomić pracodawcę w celu rozważenia konieczności wyciągnięcia konsekwencji służbowych,
      3.4.2. W przypadku osób związanych umową cywilnoprawną – zawiadomić organ zarządzający celem rozważenia konieczności wyciągnięcia konsekwencji umownych,
      3.4.3. Rozważyć czy mogło dojść do popełnienia przestępstwa, o którym mowa w przepisach art. 107-108 ustawy z … 2018 r. o ochronie danych osobowych. W

przypadku uznania, że mogło dojść do popełnienia przestępstwa, należy zawiadomić właściwą miejscowo jednostkę prokuratury.

Komórki odpowiedzialne: inspektor ochrony danych osobowych, administrator systemów informatycznych

4. Przegląd procedury
   4.1. Dokument będzie poddawany przeglądowi minimalnie raz na 12 miesięcy.

Komórki odpowiedzialne: inspektor ochrony danych osobowych

5. Postanowienia końcowe
   5.1. Procedura może zostać zmieniona przez organ zarządzający po uzyskaniu uprzedniego stanowiska komórki obsługi prawnej oraz inspektora ochrony danych osobowych.
   5.2. Zmiana procedury wchodzi w życie z dniem jej ogłoszenia w sposób zwyczajowo przyjęty.
   5.3. Procedura wchodzi w życie z dniem 25 maja 2018 roku.

6. Załączniki:
   6.1. Wzór raportu z incydentu naruszenia bezpieczeństwa danych osobowych