Zarządzenie Nr 54/2022
Starosty Powiatu Ropczycko – Sędziszowskiego
w Ropczycach z dnia 1 września 2022 r.

w sprawie:

wprowadzenia zmiany do Zarządzenia nr 104/2019 Starosty Powiatu Ropczycko – Sędziszowskiego z dnia 1 października 2019 r. dotyczącego *„ Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w Starostwie Powiatowym w Ropczycach”*

Na podstawie art. 35 ust.2 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (tj. Dz. U. z 2022 r., poz. 1526), w związku z art. 24 i art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119, s. 1)

zarządzam co następuje:

§ 1. W „Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w Starostwie Powiatowym w Ropczycach” stanowiącej załącznik nr 1 do Zarządzenia nr 104/2019 Starosty Powiatu Ropczycko – Sędziszowskiego z dnia 1 października 2019 r. wprowadza się następujące zmiany:

1). W **§ 5** dodaje się ustęp **8** w brzmieniu:

„ 8. Procedura oceny powagi naruszenia ochrony danych osobowych u Administratora stanowi ***załącznik nr 5*** do niniejszej instrukcji.”

§ 2. Załącznik nr 5 do „Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w Starostwie Powiatowym w Ropczycach” *Procedura oceny powagi naruszenia ochrony danych osobowych u Administratora* otrzymuje brzmienie określone w *załączniku nr 1* do niniejszego zarządzenia.

§ 3. Pozostała treść „Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w Starostwie Powiatowym w Ropczycach” nie ulega zmianie.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Witold Darłak

Bernadeta Safin-Wielis
adwokat

Załącznik nr 1 do Zarządzenia nr 54/2022
Starosty Powiatu Ropczycko – Sędziszowskiego
w Ropczycach z dnia 1 września 2022 r.

Załącznik nr 5 do „Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w Starostwie Powiatowym w Ropczycach"

PROCEDURA OCENY POWAGI NARUSZENIA OCHRONY DANYCH OSOBOWYCH U ADMINISTRATORA

1. Celem procedury jest ocena poziomu naruszenia bezpieczeństwa danych osobowych (ich dostępności, poufności, integralności oraz rozliczalności) w celu zakwalifikowania zdarzenia wymagającego lub nie, zgłoszenia do Urzędu Ochrony Danych Osobowych i/lub poinformowania osób fizycznych, których dane dotyczą na temat zdarzenia, zgodnie z ciążącymi na administratorze obowiązkami określonymi w art. 33 i w art. 34 RODO.
2. Procedura została opracowana na podstawie rekomendacji Urzędu Ochrony Danych Osobowych i odnosi się do metodologii opublikowanej w dniu 30 maja 2019 w wytycznych pt. Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, oraz metodologii oceny wagi naruszenia ochrony danych osobowych przygotowanej przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).
3. Za przeprowadzenie oceny odpowiada Administrator.
4. Niezależnie od wyniku oceny (od niskiego, do bardzo wysokiego) incydent ten zostaje odnotowany w prowadzonym przez administratora rejestrze incydentów.
5. **Opis narzędzia oceny (miernika)**. Jeżeli dane naruszenie powoduje:

1). **Małe** prawdopodobieństwo ryzyka wystąpienia naruszenia praw lub wolności osób, których dane dotyczą, administrator powinien:
   a) dokonać wpisu do prowadzonego rejestru naruszeń;
   b) wdrożyć środki zaradcze, tak by w przyszłości nie dochodziło do tego typu naruszeń.

2) **Prawdopodobne ryzyko** naruszenia praw lub wolności osób, których dane dotyczą, administrator powinien:
   a) dokonać wpisu do prowadzonego rejestru naruszeń;
   b) wdrożyć środki zaradcze, tak by w przyszłości nie dochodziło do tego typu naruszeń;
   c) powiadomić organ nadzorczy o naruszeniu (PUODO);
   d) uzupełnić informację, gdyby pierwotne zawiadomienie (do 72h od zdarzenia) nie zawierało wszystkich informacji lub wystąpiły nowe istotne okoliczności.

3).Występuje **wysokie ryzyko naruszenia praw lub wolności osób**, których dane dotyczą, administrator powinien:
   a) dokonać wpisu do prowadzonego rejestru naruszeń;
   b) wdrożyć środki zaradcze, tak by w przyszłości nie dochodziło do tego typu naruszeń;
   c) powiadomić organ nadzorczy o naruszeniu (PUODO);

d) powiadomić osoby, których dane dotyczą o naruszeniu, jego potencjalnych skutkach oraz metodach zaradzenia im;
e) uzupełnić informację, gdyby pierwotne zawiadomienie (do 72h od zdarzenia) nie zawierało wszystkich informacji lub wystąpiły nowe istotne okoliczności.

6.Kryteria oceny wagi naruszenia:

1) (DPC) Kontekst przetwarzania danych,
2) (EI) Łatwość identyfikacji osoby, które dane dotyczą,
3) (CB) Okoliczności naruszenia, mające dodatkowy wpływ na powagę (dotkliwość) naruszenia.

7.Końcowy wynik oceny dotkliwości naruszenia (SE), po uwzględnieniu przyjętych wartości punktowych dla poszczególnych kryteriów można uzyskać korzystając z następującego wzoru:

SE = DPC x EI x CB

8.Przykład zastosowania algorytmu przyjętej procedury:

1) (DPC) Kontekst przetwarzania danych

a) Określenie rodzajów i klasyfikacja danych, których dotyczy naruszenie (przyjęto podział na:
   - Dane zwykłe,
   - Dane behawioralne,
   - Dane finansowe,
   - Dane szczególnych kategorii (wrażliwe)

b) Ocena wystąpienia czynników dodatkowych, które mogły zwiększyć lub zmniejszyć wartość wskaźnika dla danego naruszenia. Ocenę kontekstu może podwyższyć lub obniżyć każdy z poniższych elementów:

- szeroki zakres danych tej samej osoby (+1) – szeroki zarówno w znaczeniu liczby kategorii danych, jak i czasu przez jaki podlegały naruszeniu;
- możliwe negatywne skutki dla podmiotu danych (+1);
- charakter danych (+1/-1) – przykładowo zaświadczenie lekarskie o idealnym stanie zdrowia będzie obniżało wycenę, pomimo że to dane szczególnej kategorii, a zaświadczenie o wstydliwej chorobie dodatkowo podwyższało;
- specyfika podmiotu danych (+1/-1) – inaczej wycenimy dane osób publicznych, inaczej dzieci, a inaczej pracowników służb, inspekcji, straży czy bezpieczeństwa;
- specyfika administratora (+1/-1) – inaczej wycenimy lokalny klub sportowy, a inaczej Stowarzyszenie np. Amazonek;
- publiczna dostępność danych przed naruszeniem (-1);
- nieaktualność danych (-1) – przykładowo numer karty kredytowej, której data ważności już upłynęła.

Określając czynniki obniżające należy wnikliwie przeanalizować poprawność tej decyzji oraz przygotować rozsądną argumentację.

2). Łatwość identyfikacji osoby fizycznej (EI)

Należy oszacować jak łatwo będzie podmiotowi, który ma nieuprawniony dostęp do danych, zidentyfikować osobę fizyczną, której dane dotyczą. W opisywanej metodologii określone zostały 4 poziomy tej kategorii:

- **Poziom niski (0,25)**
- **Poziom ograniczony (0,5)**
- **Poziom znaczny (0,75)**
- **Poziom wysoki (1)**

Przykład:
Naruszenie dotyczy Imienia i nazwiska petentów urzędu:

- *Poziom niski (0,25) – w całej populacji danego kraju bardzo wiele osób ma takie samo imię i nazwisko (Jan Kowalski)*
- *Poziom ograniczony (0,5) – w populacji kraju, niewiele osób ma takie same imię i nazwisko*
- *Poziom znaczny (0,75) – w danym regionie kilka osób ma takie samo imię i nazwisko*
- *Poziom wysoki (1) – w danym mieście jest tylko jedna osoba o takim imieniu i nazwisku*

3) Okoliczności naruszenia (CB)

Dane naruszenie może dotyczyć:

a) **Utraty poufności** danych:
   - 0 – gdy, dane mogły zostać narażone na utratę poufności, ale nie ma dowodów, że nastąpiło nielegalne przetwarzanie (np. laptop został zgubiony podczas transportu)
   - 0,25 – gdy dane mogły zostać ujawnione wielu znanym odbiorcom (np. wiadomość e-mail została błędnie przesłana do wielu znanych adresatów)
   - 0,5 – gdy dane zostały ujawnione wielu, nieznanym odbiorcom (np. opublikowanie danych na stronie Internetowej)

b) **Utraty integralności** danych:
   - 0 – gdy dane zostały zmienione, ale nie zidentyfikowano nieprawidłowości (np. bazy z danymi osobowymi zostały błędnie zaktualizowane, ale administrator posiada wersje oryginalne – niezmienione
   - 0,25 – gdy dane zostały zmienione i wykorzystane niepoprawnie, ale administrator może przywrócić poprawną wersję (np. zmieniono rekord niezbędny do świadczenia usługi online, a użytkownik musi poprosić o usługę offline)
   - 0,5 – gdy dane zostały zmienione i wykorzystane w niewłaściwy sposób, a administrator nie ma możliwości przywrócenia poprzedniej wersji

c) **Utraty dostępności** danych:
   - 0 – gdy dane mogą zostać odzyskane bez trudności (np. utracono kopię pliku ale administrator dysponuje kopią zapasową)
   - 0,25 – gdy dane osobowe nie są dostępne przez jakiś czas (np. dane zostały utracone i konieczne jest ich ponowne zebranie)

- 0,5 – gdy utracono dane osobowe i nie ma możliwości jej odtworzenia (np. nie istnieją kopie zapasowe ani nie można odtworzyć tych danych)

d) Istotne jest także czy naruszenie było **celowym czy przypadkowym** działaniem:
0,5 – gdy dane zostały utracone na skutek celowego działania (np. pracownik celowo przekazał dane klientów firmy jej konkurencji.

9. Ocena dotkliwości naruszenia bezpieczeństwa danych osobowych. Po analizie danego naruszenia, otrzymane wartości podstawiamy do wzoru:

SE = DPC x EI x CB

Otrzymany wynik oznacza:

SE < 2	**Poziom niski**	Osoby fizyczne nie będą dotknięte tym naruszeniem lub mogą napotkać niewielkie niedogodności, które będą mogły bez problemu pokonać (np. ponownie należy poświęcić czas na wprowadzenie danych);
2 ≤ SE < 3	**Poziom średni**	Osoby fizyczne mogą napotkać znaczne trudności, które jednak będą w stanie pokonać (np. dodatkowe koszty, odmowa dostępu do usługi, stres);
3 ≤ SE< 4	**Poziom wysoki**	Osoby fizyczne będą dotknięte znacznymi konsekwencjami, które z pewnym trudem będą mogły pokonać (np. umieszczenie na liście dłużników banku, uszkodzenie mienia, wezwanie do sadu, pogorszenie stanu zdrowia);
4 ≤ SE	**Poziom bardzo wysoki**	Osoby indywidualne mogą dotknąć znaczące a nawet nieodwracalne konsekwencje (np. kłopoty finansowe, niezdolność do pracy, dolegliwości psychiczne lub fizyczne, śmierć).

10. W przypadku, gdy procedurę przeprowadza IOD, Administrator ją akceptuje po zapoznaniu się z wynikiem i decyduje o czynnościach o których mowa w art. 33 i 34 RODO.

STAROSTA
Witold Darłak

Bernadeta Safin-Wielis
adwokat