ZARZĄDZENIE Nr 9/2020
STAROSTY KONECKIEGO
z dnia 27 lutego 2020 r.

w sprawie przyjęcia procedury postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa

Na podstawie §23 ust. 5 Regulaminu Organizacyjnego Starostwa Powiatowego w Końskich przyjętego Uchwałą Nr 28/2017 Zarządu Powiatu w Końskich z dnia 22 marca 2017 r. ze zm. w związku z art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 ze zm.) oraz §20 ust.2 pkt.13 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247) zarządzam, co następuje:

§1.

Przyjmuje się do stosowania w Starostwie Powiatowym w Końskich „Procedurę postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa" w brzmieniu stanowiącym załącznik do niniejszego Zarządzenia.

§2.

Wykonanie zarządzenia powierza się pracownikom Starostwa Powiatowego w Końskich.

§3.

Nadzór nad wykonaniem Zarządzenia powierzam Sekretarzowi Powiatu.

§4.

Zarządzenie wchodzi w życie od dnia 2 marca 2020 r.

STAROSTA
Grzegorz Piec

RADCA PRAWNY
mgr Iwona Bogacka-Urbaś

Załącznik
Do Zarządzenia Nr 9/2020
Starosty Koneckiego
z dn. 27 lutego 2020 r.

Procedura postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa

Spis treści

1. Cel

Celem wprowadzenia do stosowania niniejszej procedury jest zapewnienie właściwego postępowania w zakresie zgłaszania i obsługi incydentów bezpieczeństwa i cyberbezpieczeństwa.

2. Zakres

Zobowiązani do stosowania niniejszej procedury są pracownicy i współpracownicy Jednostki.

3. Definicje

Jednostka – Starostwo Powiatowe w Końskich.

RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Ustawa o ochronie danych osobowych – ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781).

Dane osobowe (Zgodnie z art. 4 ust. 1 pkt 1 RODO) - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane szczególne (Szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 2 RODO) – ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne oraz dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Incydent bezpieczeństwa – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne prawdopodobieństwo wystąpienia naruszenia ochrony danych osobowych.

Incydent cyberbezpieczeństwa – to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Starostwo Powiatowe w Końskich.

Naruszenie ochrony danych osobowych (dalej: Naruszenie) (Zgodnie z art. 4 ust. 1 pkt 12 RODO) – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Organ nadzorczy (Zgodnie z art. 4 ust. 1 pkt 21 RODO) – Prezes Urzędu Ochrony Danych Osobowych.

Osoba nieuprawniona – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe z naruszeniem przepisów o ochronie danych osobowych, lub poza wyraźnym uprawnionym poleceniem Administratora Danych Osobowych.

Administrator Systemów Informatycznych – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwanego dalej „ASI"

Osoba wyznaczona do kontaktów w sprawach cyberbezpieczeństwa – osoba wyznaczona zgodnie z art. 21 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa

Osoba upoważniona – osoba wykonująca zadania polegające na przetwarzaniu, w formie tradycyjnej lub elektronicznej, danych osobowych na wyraźne polecenie Administratora Danych Osobowych i jest upoważniona do wykonywania tych czynności.

4. Administrator danych osobowych

Administratorem danych osobowych jest Starostwo Powiatowe w Końskich reprezentowane przez Starostę, który ustala cele i sposoby przetwarzania danych osobowych.

Administrator danych osobowych mając na uwadze jak ważne jest bezpieczeństwo przetwarzanych danych osobowych ze względu na ochronę podstawowych praw i wolności osób fizycznych, a w szczególności ich prawo do ochrony danych osobowych oraz w celu zapewnienia zgodności z wymaganiami prawa, a w tym ochronę dobrego imienia jednostki, ustanawia system ochrony danych osobowych tj. zasady oraz zabezpieczenia stosowane podczas przetwarzania danych osobowych.

5. Przyczyny i kategorie incydentów

5.1 Przyczyną incydentu bezpieczeństwa lub cyberbezpieczeństwa może być:

1) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
2) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych;
3) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

5.2 Incydentami bezpieczeństwa informacji w szczególności są:

1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.

5.3 Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:

1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
2) działania szkodliwego oprogramowania;
3) próby omijania systemów zabezpieczeń;
4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
6) zniszczenia lub kradzieży nośników danych;

7) próby wyłudzeń informacji;
8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
10) naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

6. Zgłaszanie i obsługa Incydentów bezpieczeństwa

6.1. Każdy pracownik oraz współpracownik ma obowiązek zgłosić podejrzenie wystąpienia Incydentu bezpieczeństwa lub cyberbezpieczeństwa.
6.2. Zgłoszenie Incydentu bezpieczeństwa należy złożyć w jeden w poniższych sposobów:
- drogą elektroniczną na adres: **incydent@konecki.powiat.pl**;
- pisemnie przekazując zgłoszenie **Kancelarii Ogólnej Urzędu**;
- w formie notatki **bezpośredniemu przełożonemu** lub **osobie wyznaczonej do kontaktów w sprawie cyberbezpieczeństwa**

6.3. Zgłoszenie o podejrzeniu wystąpienia Incydentu bezpieczeństwa powinno zawierać: opis sytuacji wskazującej na potencjalne naruszenie / naruszenie zasad ochrony danych osobowych, datę zdarzenia, konsekwencje zdarzenia (o ile zaistniały), uczestników zdarzenia oraz dotychczasowo podjęte działania w zakresie minimalizacji skutków zdarzenia (o ile zostały podjęte).
6.4. Za obsługę Incydentów bezpieczeństwa odpowiada **osoba wyznaczona do kontaktów w sprawie cyberbezpieczeństwa**.
6.5. W przypadku nieobecności **osoby wyznaczonej do kontaktów w sprawie cyberbezpieczeństwa** obsługę incydentu zapewnia wyznaczony **Administrator Systemu Informatycznego.**
6.6. Osoba odpowiedzialna za obsługę Incydentu bezpieczeństwa dokonuje analizy otrzymanego zgłoszenia tj. przedstawionych informacji i identyfikuje przyczynę wystąpienia zdarzenia oraz wskazuje działania do podjęcia w celu minimalizacji skutków zdarzenia.
6.7. W przypadku gdy Incydent bezpieczeństwa ma charakter Naruszenia ochrony danych osobowych, to osoba obsługująca Incydent zobowiązana jest do niezwłocznego przekazania informacji Inspektorowi Ochrony Danych (IOD).
6.8. W przypadku stwierdzenia incydentu cyberbezpieczeństwa **osoba wyznaczona do kontaktów w sprawie cyberbezpieczeństwa** w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK zgodnie z procedurą opisaną pod adresem internetowym **https://incydent.cert.pl**
6.9. Naruszenie ochrony danych obsługiwane jest zgodnie z zapisami Polityki ochrony danych osobowych obowiązującej w Jednostce.

7. Raportowanie Incydentów bezpieczeństwa

7.1. Każdy zgłoszony Incydent bezpieczeństwa musi zostać zarejestrowany w rejestrze, którego wzór stanowi załącznik nr 1 do niniejszej procedury.
7.2. Osoba obsługująca Incydent bezpieczeństwa zobowiązana jest do monitorowania wdrożenia działań naprawczych, tj. takich które mają zapobiegać ponownemu zdarzeniu, które naruszy zasady ochrony danych osobowych.

7.3. Raz na pół roku zarejestrowane Incydenty bezpieczeństwa są analizowane przez **Wydział Organizacji i Informatyzacji Powiatu we współpracy z Inspektorem Ochrony Danych** a wnioski z analizy są przedstawiane **Zespołowi ds. Zarządzania Ryzykiem.**

7.4. **Osoba do obsługi Incydentów bezpieczeństwa**, raz na pół roku, na dwa tygodnie przed planowaną datą przekazania raportu **Zespołowi ds. Zarządzania Ryzykiem** przygotowuje dane do analizy z zarejestrowanych Incydentów bezpieczeństwa. Raport może mieć dowolną formę, uzgodnioną z **Naczelnikiem Wydziału Organizacji i Informatyzacji Powiatu,** niemniej jednak musi zawierać takie informacje jak:

a) ilość zdarzeń,
b) ilość zdarzeń o charakterze naruszenia ochrony danych,
c) przyczyny zdarzenia,
d) podjęte działania.

8. Odpowiedzialność za naruszenie ochrony danych osobowych

8.1. Postępowanie wbrew obowiązującym zasadom ochrony danych osobowych, określonych przez Administratora może być uznane za naruszenie ustalonej organizacji i porządku pracy. W takiej sytuacji może zostać, zgodnie z przepisami art. 108 Kodeksu pracy, nałożona kara porządkowa.

8.2. Nieprzestrzeganie zasad ochrony danych osobowych (naruszenie ochrony danych osobowych) skutkuje sankcjami karnymi przewidzianymi w Kodeksie Karnym art. 266 – 269,287.

8.3. Ponadto, zgodnie z art. 82 RODO, każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia ogólnego rozporządzenia o ochronie danych, ma prawo uzyskać od Administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

9. Załączniki

Załącznik nr 1 – wzór rejestru Incydentów bezpieczeństwa.

10. Dokumenty powiązane

Polityka ochrony danych osobowych

Załącznik nr 1 – Wzór rejestru Incydentów bezpieczeństwa i cyberbezpieczeństwa

Lp.	Data zgłoszenia	Kategoria zgłoszenia (*Incydent bezpieczeństwa/ cyberbezpieczeństwa lub Naruszenie ochrony danych osobowych)	Opis incydentu (zdarzenia)	Osoba zgłaszająca	Kategoria incydentu	Przyczyna lub potencjalna przyczyna wystąpienia incydentu	Opis działań podjętych w związku z incydentem	Data zamknięcia incydentu