Zarządzenie Nr 25/2023
Starosty Aleksandrowskiego
z dnia 24 października 2023 roku

w sprawie wprowadzenia Instrukcji postępowania w przypadku naruszenia bezpieczeństwa danych osobowych oraz zmiany zarządzenia nr 8/2018 Starosty Aleksandrowskiego z dnia 16 marca 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych oraz Instrukcji Zarządzenia Systemami Informatycznymi w Starostwie Powiatowym w Aleksandrowie Kujawskim

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. 2022 poz. 1526 z późn. zm.) oraz art. 24 ust.1 rozporządzenia 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) (Dz.U.UE.L.2016.119.1) zarządza się, co następuje:

§ 1. W Starostwie Powiatowym w Aleksandrowie Kujawskim wprowadza się dla zapewnienia ochrony przetwarzania danych osobowych *Instrukcję postępowania w przypadku naruszenia bezpieczeństwa danych osobowych*, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Z treścią dokumentów, o których mowa w §1 zobowiązani są zapoznać się wszyscy pracownicy Starostwa Powiatowego w Aleksandrowie Kujawskim.

§ 3. Zobowiązuje się wszystkich pracowników Starostwa Powiatowego w Aleksandrowie Kujawskim do przestrzegania zasad wynikających z dokumentów, o których mowa w §1.

§ 4. W zarządzeniu nr 8/2018 Starosty Aleksandrowskiego z dnia 16 marca 2018 roku w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych oraz Instrukcji Zarządzenia Systemami Informatycznymi w Starostwie Powiatowym w Aleksandrowie Kujawskim w § 1 ust. 1 uchyla się pkt 3 oraz załącznik nr 3.

§ 5. Wdrożenie zarządzenia powierza się Sekretarzowi Powiatu.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA ALEKSANDROWSKI

STAROSTA
ALEKSANDROWSKI
Lidia Tokarska

Sprawdz. pod. wzgl. formalno-prawnym:
RADCA PRAWNY Anna J. Szpadt
Toruń 2023-10-24

Załącznik do zarządzenia nr 25/2023
Starosty Aleksandrowskiego z dnia 24 października 2023 roku

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Cel instrukcji i postanowienia ogólne

§1

Celem instrukcji jest określenie sposobu postępowania gdy:

1. Stwierdzono naruszenie zabezpieczeń danych osobowych.
2. W przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
3. W przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

§2

Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych, zgodne z „Tabelą form naruszeń bezpieczeństwa danych osobowych", stanowiącą załącznik nr 1 do niniejszej instrukcji.

§3

Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

a) nieautoryzowany dostęp do danych,
b) nieautoryzowane modyfikacje lub zniszczenie danych,
c) udostępnienie danych nieautoryzowanym podmiotom,
d) nielegalne ujawnienie danych,
e) pozyskiwanie danych z nielegalnych źródeł.

§4

1. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w Starostwie Powiatowym w Aleksandrowie Kujawskim jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, Inspektorowi Ochrony Danych lub Administratorowi Danych Osobowych, a następnie postępować stosownie do podjętej przez niego decyzji.
2. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:
   a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,
   b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§5

Inspektor Ochrony Danych lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:

a) minimalizację negatywnych skutków zdarzenia,
b) wyjaśnienie okoliczności zdarzenia,
c) zabezpieczenie dowodów zdarzenia,
d) umożliwienie dalszego bezpiecznego przetwarzania danych.

§6

W celu realizacji zadań wynikających z niniejszej instrukcji Inspektor Ochrony Danych lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

a) żądania wyjaśnień od pracowników,
b) korzystania z pomocy konsultantów,
c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§7

Polecenia Inspektora Ochrony Danych lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

§8

Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Ochrony Danych lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych.

§9

Inspektor Ochrony Danych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu stanowi załącznik nr 2 do niniejszej instrukcji.

§10

Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§11

Jeżeli skutkiem działania określonego w §10 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

§12

Jeżeli skutkiem działania określonego w §10 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.

Ograniczanie skutków naruszeń

§ 13

1. Dokumentacja naruszenia podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów, które mają zastosowanie przy postępowaniu z naruszeniem, w tym: rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe, bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.
2. IOD przeprowadza bieżące działania zmierzające do ograniczenia skutków naruszenia i zidentyfikowania jego źródła. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.
3. W przypadku, gdy działania opisane w ust. 2 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych Starostwa Powiatowego, IOD przedstawia decyzję do akceptacji ADO.

Odtwarzanie systemu

§ 14

1. Osoba upoważniona przez ADO przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła naruszenia.
2. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego ASI ma uzasadnioną pewność, że nie zawiera źródła naruszenia.
3. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
4. ADO, po zasięgnięciu opinii IOD, może podjąć decyzję o podjęciu przetwarzania danych mimo braku pewności usunięcia źródła naruszenia, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

Zgłaszanie naruszenia ochrony danych do UODO

§ 15

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w ust. 1, musi zawierać co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) zawierać imię i nazwisko oraz zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisywać środki zastosowane lub proponowane przez ADO w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. ADO 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 niniejszego artykułu.
5. Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie www.uodo.gov.pl na 4

sposoby:

1) elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie www.biznes.gov.pl;

2) elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP

3) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie www.biznes.gov.pl;

4) tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Zawiadamianie osób o naruszeniu ochrony ich danych osobowych

§ 16

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.

3. Nie dokonuje się zawiadomienia osób w następujących przypadkach, gdy:

1) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

2) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

STAROSTA
ALEKSANDROWSKI
Lidia Tokarska

Załącznik nr 1
do „Instrukcji postępowania w sytuacji
naruszenia bezpieczeństwa danych osobowych"

Tabela form naruszeń bezpieczeństwa danych osobowych

Kod naruszenia	Formy naruszeń	Sposób postępowania
A	Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych	
A.1	W zakresie wiedzy:	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IOD.
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IOD.
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IOD.
A.2	W zakresie sprzętu i oprogramowania	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić IOD. Sporządzić raport.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić IOD. Sporządzić raport.

	danych osobowych przez osoby nie będące pracownikami	
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymieniona czynność, aby jej zaniechała. Wezwać ASI w celu odinstalowania programów. Sporządzić raport.
A.2.6	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
A.2.7	Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać ASI w celu wykonania kontroli antywirusowej. Sporządzić raport.

A.3	W zakresie dokumentów i obrazów zawierających dane osobowe	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. Sporządzić raport.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń sporządzić raport.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane. Sporządzić raport.
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IOD. Sporządzić raport.
A.3.7	Utrata kontroli nad kopią danych osobowych	Podjąć próbę odzyskania kopii. Powiadomić IOD. Sporządzić raport.
A.4	W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych	

A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych . Sporządzić raport.
A.4.2	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i IOD. Sporządzić raport.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić ASI i IOD. Sporządzić raport.
A.5	**W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci.**	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.)	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić ASI i IOD. Sporządzić raport.
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić ASI i IOD. Sporządzić raport.

B	Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach	Powiadomić niezwłocznie IOD oraz ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	Powiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie IOD. Sporządzić raport.
C	Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej	Powiadomić IOD. Sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić IOD. Sporządzić raport.
D	Utrata poufności danych	
D.1	Udostępnienie danych osobowych osobie nieuprawnionej.	Powiadomić IOD. Postępować zgodnie z właściwymi przepisami. Sporządzić raport.
D.2	Brak anonimizacji lub pseudonimizacji danych osobowych w procesie ujawniania informacji przewidzianej prawem.	Powiadomić IOD. Postępować zgodnie z właściwymi przepisami. Sporządzić raport.

D.3	Kradzież urządzenia służącego do przetwarzania danych osobowych. (pamięć przenośna, komputer, telefon itp.)	Powiadomić ASI i IOD. Postępować zgodnie z właściwymi przepisami. Sporządzić raport.
D.4	Zgubienie urządzenia służącego do przetwarzania danych osobowych. (pamięć przenośna, komputer, telefon itp.)	Powiadomić ASI i IOD. Postępować zgodnie z właściwymi przepisami. Sporządzić raport.

Załącznik nr 2
do „Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych"

Wzór raportu końcowego sporządzanego przez Inspektora Ochrony Danych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych

Raport o sytuacji naruszenia bezpieczeństwa danych osobowych

Sporządzający raport:

Imię i nazwisko: .....

stanowisko (funkcja) .....

Dział, pokój, nr telefonu .....

Kod formy naruszenia ochrony danych ..... (wg tabeli)

1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):

.....

.....

2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

.....

.....

3) Osoby , które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

.....

.....

4) Informacje o danych, które zostały lub mogły zostać ujawnione:

.....

.....

- przybliżona liczba osób, których mogło dotyczyć naruszenie.....

- przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie.....

5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....

6) Przyczyna naruszenia:

□ Wewnętrzne działanie niezamierzone

□ Wewnętrzne działanie zamierzone

□ Zewnętrzne działanie niezamierzone

□ Zewnętrzne działanie zamierzone

7) Opisać możliwe konsekwencje naruszenia ochrony danych osobowych:

Naruszenie ma wpływ na:

□ poufność (nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych)

□ integralność (wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub

przechowywania)

□ dostępność (brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez do tego uprawnioną)

8) Kategorie danych osobowych, których dotyczy naruszenie:

□ nazwiska i imiona

□ nazwa użytkownika i/lub hasło

□ imiona rodziców

□ dane dot. zarobków

□ data urodzenia

□ nazwisko rodowe matki

□ nr rachunku bankowego

□ seria i numer dowodu osobistego

□ adres zamieszkaniu lub pobytu

□ numer telefonu

□ numer ewidencyjny PESEL

□ wizerunek

□ adres e-mail

□ inne.....

9) Dane szczególnej kategorii przetwarzania:

□ dane o pochodzeniu rasowym lub etnicznym

□ dane o poglądach politycznych

□ dane o przekonaniach religijnych lub światopoglądowych

□ dane o przynależności do związków zawodowych

□ dane dotyczące seksualności lub orientacji seksualnej

□ dane dotyczące zdrowia

□ dane genetyczne

□ dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

10) Opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):

.....

.....

11) Opisać możliwe konsekwencje naruszenia ochrony danych osobowych:.....

12) Naruszenie ma wpływ na:

□ poufność (nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych)

□ integralność (wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania)

□ dostępność (brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez do tego uprawnioną

13) Możliwe konsekwencje (opisać konsekwencje dla osoby, której dane dotyczą):

□ utrata kontroli nad własnymi danymi osobowymi

□ ograniczenie możliwości realizowania praw z art. 15-22 RODO

□ ograniczenie możliwości realizowania praw

□ dyskryminacja

□ kradzież lub sfałszowanie tożsamości

□ strata finansowa

□ naruszenie dobrego imienia

□ utrata poufności danych osobowych chronionych tajemnicą zawodową

□ inne:

.....

14) Czy naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:

□ NIE

□ TAK (art. 33 ust.1 RODO)

niskie/ średnie/ wysokie

.....

15) Wnioski:

.....

.....

....

(miejsce, data i godzina sporządzenia raportu) (podpis sporządzającego raport)