ZARZĄDZENIE NR 65
Wójta Gminy Odrzywół
z dnia 18 października 2019 roku

w sprawie trybu postępowania w przypadku incydentów
w zakresie bezpieczeństwa informacji i danych osobowych w Urzędzie Gminy w Odrzywole

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2019r. poz. 506), w związku z art. 33 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 (tzw. Ogólne Rozporządzenie o Ochronie Danych Osobowych/ dalej: RODO),mając na uwadze prawidłowość realizacji obowiązków wynikających z art. 33 tj. stosowania unormowań RODO w zakresie notyfikacji naruszeń ochrony danych osobowych oraz w celu maksymalizacji poziomu bezpieczeństwa danych administrowanych przez Urząd Gminy w Odrzywole jako Administratora Danych Osobowych wprowadza się Procedura postępowania w sytuacji naruszenia ochrony danych stanowiącą doprecyzowanie unormowań Polityki bezpieczeństwa danych osobowych.

§ 1.

Mając na uwadze prawidłowość realizacji obowiązków wynikających z art. 33 tj. stosowania unormowań RODO w zakresie notyfikacji naruszeń ochrony danych osobowych oraz w celu maksymalizacji poziomu bezpieczeństwa danych administrowanych przez Urząd Gminy w Odrzywole jako Administratora Danych Osobowych wprowadza się procedurę postępowania w przypadku incydentów w zakresie bezpieczeństwa informacji i danych osobowych stanowiącą doprecyzowanie unormowań Polityki bezpieczeństwa danych osobowych.

§ 2.

Procedura postępowania w sytuacji naruszenia ochrony danych stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania

WÓJT
mgr Marian Kmieciak

Ilona Głogowska-Kowalczyk
PRAWNIK
Inspektor Ochrony Danych

Opr. Ilona Głogowska-Kowalczyk - Inspektor Ochrony Danych (DPO)
18.10.2019 r.

Akceptacje:

1. Sekretarz Gminy:

Sprawdzono pod względem zgodności z procedurą .....

Z up. WÓJTA
mgr Genowefa Pogorzała
SEKRETARZ GMINY

Aktualizacja załącznika nr 1 do Zarządzenia nr 65 Wójta Gminy Odrzywół z dnia 18 października 2019r.

PROCEDURA POSTĘPOWANIA SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Nazwa/ dane kontaktowe Administratora danych	
Nazwa	Urząd Gminy w Odrzywole
Adres	ul. Warszawska 53, 36-425 Odrzywół
Email	sekretariat@odrzywol.eu
Telefon	48 6716057

Inspektor Ochrony Danych	
Nazwa	Ilona Głogowska-Kowalczyk
Adres	26-600 Radom, ul. Żwirki i Wigury 40 lok. 23
Email	kancelaria.odo@gmail.com
Telefon	608292823

Wersja:	Druga wersja dokumentu
Data wersji:	22.07.2020r.
Utworzony przez:	Ilona Głogowska-Kowalczyk
Historia zmian	
Data:	18.10.2019r. 22.07.2020r.
Wersja:	0.2
Utworzona przez:	Ilona Głogowska-Kowalczyk
Zatwierdzona przez:	Pan Marian Kmieciak-Wójt Gminy Odrzywół
Dokumenty referencyjne:	Polityka ochrony danych osobowych
Opis zmian:	Aktualizacja dokumentu w związku z pracą zdalną podczas pandemii

Procedura reagowania w sytuacji incydentu i zgłaszania naruszeń

Procedura definiuje katalog zagrożeń i incydentów mogących prowadzić do naruszenia bezpieczeństwa danych osobowych przetwarzanych przez administratora (również tych danych, które zostały powierzone na rzecz administratora przez inny podmiot) oraz sposób reagowania na zagrożenia i incydenty.
Celem opracowania procedury jest ograniczenie skutków wystąpienia incydentów godzących w bezpieczeństwo przetwarzania danych osobowych oraz zmniejszenie ryzyka ich powstania w przyszłości.
Procedura dzieli się na:

1. Postępowanie wewnętrzne;
2. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu;
3. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;
4. Oceny wagi naruszenia, szacowanie wg ENISA

Postępowanie wewnętrzne

1. Każdy pracownik administratora, w przypadku stwierdzenia zagrożenia lub podejrzenia naruszenia zasad ochrony danych osobowych, zobowiązany jest do niezwłocznego poinformowania o ww. okolicznościach bezpośredniego przełożonego lub ASI jeżeli został wyznaczony. Bezpośredni przełożony lub ASI w przypadku powzięcia powyższej informacji zobowiązany jest do jej niezwłocznego przekazania IOD. Zgłoszenie incydentu IOD dokonywane
2. Rodzaje najczęściej występujących zagrożeń bezpieczeństwa danych osobowych:
    a. niewłaściwe zabezpieczenie stacji roboczych, komputerów przenośnych, tabletów, smartphonów, nośników przenośnych oraz oprogramowania IT przed kradzieżą, zniszczeniem lub utratą danych osobowych;
    b. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń oraz dokumentów;
    c. nieprzestrzeganie przyjętych zasad ochrony danych osobowych przez upoważnione osoby.
3. Przykładowe incydenty naruszające zasadę bezpieczeństwa danych osobowych:
    a. incydenty losowe zewnętrzne np. pożar obiektu lub pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;

b. incydenty losowe wewnętrzne np. awarie stacji roboczych, awarie serwera, awarie oprogramowania, utrata lub zgubienie danych zawartych na nośnikach przenośnych;
c. incydenty umyślne np. ataki hakerskie, włamania do pomieszczeń, celowe i świadome zniszczenie dokumentów, szkodliwe oprogramowanie.

Katalog naruszeń ochrony danych osobowych zawiera załącznik nr 1.

4. W przypadku podejrzenia wystąpienia zagrożenia lub incydentu IOD w porozumieniu z ASI prowadzi postępowanie wstępne, w toku którego:
   a. ustala zakres i przyczyny zagrożenia lub incydentu oraz jego ewentualne skutki;
   b. inicjuje ewentualne postępowanie dyscyplinarne;
   c. rekomenduje działania prewencyjne zmierzające do eliminacji podobnych zagrożeń lub incydentów w przyszłości;
   d. dokumentuje prowadzone postępowanie;
   e. przedstawia raport z przeprowadzonego postępowania administratorowi.
5. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych, IOD informuje administratora o konieczności zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
6. Oceny, czy występuje ryzyko naruszenia praw lub wolności człowieka, administrator dokonuje we współpracy z IOD. Ocena powinna być oparta na obiektywnych kryteriach, jak dotychczasowe doświadczenie związane z podobnymi naruszeniami lub wiedza z zakresu bezpieczeństwa informacji, oraz na uwzględnieniu okoliczności samego naruszenia ochrony danych osobowych.
7. W toku dokonywania oceny, o której mowa w pkt. 6 administrator bierze pod uwagę wszelkie możliwe szkody, jak i krzywdy, które mogą wyniknąć dla osób fizycznych z danego naruszenia. Mogą one w szczególności polegać na:
   - utracie kontroli nad własnymi danymi osobowymi,
   - negatywnych konsekwencjach wizerunkowych,
   - możliwości zawierania przez inną osobę umów z wykorzystaniem danych osobowych innej osoby fizycznej,
   - stratach finansowych,
   - negatywnym odbiorze społecznym, który może być konsekwencją upublicznienia niektórych danych osobowych.

8. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych IOD, niezależenie od pkt. 5, niezwłocznie rozpoczyna audyt doraźny. W ramach czynności audytowych IOD:
    a. określa sposób dokumentowania audytu, a w jego ramach:
        - sporządza notatki z czynności audytowych, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
        - odbiera pisemne wyjaśnienia osoby, której czynności objęto audytem;
        - sporządza kopie okazanych dokumentów;
        - sporządza kopię obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
        - sporządza kopie zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.
    b. zabezpiecza ewentualne dowody związane z incydentem;
    c. ustala osoby odpowiedzialne za powstanie incydentu;
    d. wskazuje możliwe sposoby przywrócenia stanu zgodnego z prawem;
    e. wnioskuje o wszczęcie postępowań dyscyplinarnych;
    f. przygotowuje raport dla administratora.
9. IOD zawiadamia administratora o rozpoczęciu audytu doraźnego przed podjęciem pierwszej czynności w toku audytu.
10. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta powinna pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania niniejszej Procedury.
11. IOD prowadzi rejestr naruszeń, **zgodnie ze wzorem zawartym w procedurze załącznik nr 2**.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, 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. **Zgłoszenie incydentu załącznik nr 3.**

2. W sytuacji, gdy naruszenie dotyczy danych osobowych osób fizycznych, których jednostka nie jest administratorem, a podmiotem przetwarzającym, któremu na podstawie art. 28 RODO zostały dane powierzone, to po stwierdzeniu naruszenia ochrony danych osobowych dyrektor/kierownik jednostki, bez zbędnej zwłoki, zgłasza naruszenie podmiotowi, który dane powierzył.
3. Zgłoszenie, o którym mowa w pkt. 1, zawiera co najmniej:
   a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
   d) opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

Zawiadamianie osoby, której dane dotyczą o naruszeniu danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych na podstawie art. 34 w związku z art. 33 ust. 3 lit. b, c i d rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, dalej: RODO), **formularz powiadomienia osoby stanowi załącznik nr 4.**
2. Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej następujące informacje i środki:

a) imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
c) opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

Wzór zawiadomienia podmiotu danych stanowi załącznik nr 5.

3. Zawiadomienie nie jest wymagane, w następujących przypadkach:
   a) administrator 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;
   b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku administrator wyda publiczny komunikat lub zastosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

Skrócona instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych stanowi załącznik nr 6.

Ocena wagi naruszenia, szacowanie według ENISA

1. Wagę naruszenia danych osobowych określa stopień potencjalnego wpływu incydentu na prawa i/lub wolności osób, których dotyczy naruszenie.

Naruszenie może wiązać się z powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

2. Administrator dokonuje ogólnej oceny wagi naruszenia poprzez określenie możliwych oddziaływań na osobę.

3. Identyfikacja konsekwencji (skutków naruszenia ochrony danych) dla osób fizycznych - Motyw 85 RODO:

- utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw,
- dyskryminacja,
- kradzież lub sfałszowanie tożsamości,
- strata finansowa,
- nieuprawnione odwrócenie pseudonimizacji,
- naruszenie dobrego imienia,
- naruszenie poufności danych osobowych chronionych tajemnicą zawodową
- wszelkie inne znaczne szkody gospodarcze lub społeczne

Metodę oceny wagi naruszenia zawiera załącznik nr 7 do niniejszej procedury

Wykaz załączników:

Załącznik nr 1: Katalog naruszeń ochrony danych osobowych
Załącznik nr 2: Rejestr naruszeń ochrony danych
Załącznik nr 3: Zgłoszenie incydentu naruszenia ochrony danych osobowych
Załącznik nr 4: Formularz powiadomienia podmiotu danych o naruszeniu ochrony danych osobowych
Załącznik nr 5: Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych
Załącznik nr 6: Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

Załącznik nr 7: Metoda oceny wagi naruszenia wg. Agencja unii europejskiej ds. Bezpieczeństwa sieci i informacji (enisa)[1]

WÓJT
mgr Marian Kmieciak

22.07.2020 r. .....

data, podpis Administratora danych

[1] https://www.enisa.europa.eu/publications/dbn-severity/

Załącznik nr 1

Katalog naruszeń ochrony danych osobowych

1. Można wyróżnić **trzy typy naruszenia ochrony danych osobowych**:

a) **naruszenie poufności** – polega na ujawnieniu danych osobowych nieuprawnionej osobie, np. „Przypadkowe wysłanie danych osobowych klienta do niewłaściwego działu firmy lub osoby postronnej."

b) **naruszenie dostępności** – polega na trwałej utracie lub zniszczeniu danych osobowych, np. „Zgubienie lub kradzież nośnika zawierającego kopię bazy danych klientów administratora." lub „Pracownik przypadkowo lub osoba nieupoważniona celowo usuwa dane ze zbioru. Administrator próbuje odzyskać dane z kopii zapasowej, jednak jego działania nie przynoszą rezultatu.", lub „W wyniku przerwy w dostawie prądu lub ataku typu blokada usług, administrator tymczasowo lub trwale traci dostęp do danych osobowych."

c) **naruszenie integralności** – polega na zmianie treści danych osobowych w sposób nieautoryzowany, np. „Pracownik zmienia nazwiska klientów poprzez dopisanie litery „s" na końcu każdego z nich."

2. Naruszenie może polegać na:
   - Dokumentacja papierowa (zawierająca dane osobowe) została zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji;
   - Nieuprawione uzyskanie dostępu do informacji;
   - Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
   - Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych;
   - Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing);
   - Nieprawidłowa anonimizacja danych osobowych w dokumencie;
   - Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora;
   - Niezamierzona publikacja;
   - Ujawnienie danych niewłaściwej osoby;
   - Ustne ujawnienie danych osobowych;
   - Zmiana danych bez zgody osoby, której dane dotyczą;
   - Wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwie zaadresowanie poczty elektronicznej);

- Zgubienie lub kradzież nośników danych (telefon, laptop, USB, teczki zawierające dane w wersji papierowej);
- Nieuprawnione udostępnienie danych (np. elektronicznie – przekazywanie danych przez zdalny dostęp np. VPN, często przydzielane bezterminowo - ale też np. telefonicznie (rozmówca podaje się za pracownika policji czy urzędu, próbując wyciągnąć informacje).

3. Naruszenia w zakresie wiedzy:
   - Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym;
   - Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej;
   - Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.
4. Naruszenia w zakresie sprzętu i oprogramowania
   - Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych;
   - Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony;
   - Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci;
   - Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym;
   - Samodzielne instalowanie jakiegokolwiek oprogramowania;
   - Modyfikowanie parametrów systemu i aplikacji.
5. Naruszenia w zakresie dokumentów i obrazów zawierających dane osobowe:
   - Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru;
   - Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych;
   - Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie;
   - Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią;
   - Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe;
   - Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą;
   - Utrata kontroli nad kopią danych osobowych.
6. Naruszenia w zakresie pomieszczeń infrastruktury:
   - 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;
   - Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym;
   - Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci

komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji;
- 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.);
- Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.

7. Naruszenia w związku z wykonywaniem pracy zdalnie dotyczące dokumentów i obrazów zawierających dane osobowe:
   - Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru;
   - Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych;
   - Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie;
   - Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią;
   - Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe;
   - Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą;
   - Utrata kontroli nad kopią danych osobowych.

Załącznik nr 2

Rejestr naruszeń ochrony danych

Nazwa i dane kontaktowe Administratora Danych

Nazwa:
Adres:
Email:
Inspektor Ochrony Danych

Nazwa: Ilona Głogowska-Kowalczyk
Adres:26-600 Radom
Email: kancelaria.odo@gmail.com
Telefon: 608292823

Art. 4 pkt12 RODO - „naruszenie ochrony danych osobowych" 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;

Zgodnie z art. 33 ust. 5 RODO, administrator danych dokumentuje wszelkie naruszenie ochrony danych osobowych w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania art. 33 RODO.

Dokumentowanie naruszeń ochrony danych osobowych(naruszenie, okoliczności, skutki, środki zaradcze)		
1.	Naruszenie (opis naruszenia) Data, godzina zgłoszenia podejrzenia naruszenia, stwierdzenia naruszenia oraz miejsca i okresu, którego naruszenie dotyczy,	
2.	Kategorie i liczba osób oraz kategorie danych, których naruszenie dotyczy Źródło informacji o zdarzeniu(osoba, instytucja)	
3.	Okoliczności naruszenia – przebieg i analiza zdarzenia, przyczyny wystąpienia	
4.	Opis możliwych skutków / konsekwencji naruszenia	

	Ryzyko naruszenia praw i wolności i opis możliwego naruszenia (podanie przyczyn uznania ryzyka naruszenia za mało prawdopodobne)[2]	
5.	Osoby/ jednostki odpowiedzialne za zdarzenie	
6.	Podjęta działania zaradcze – opis środków zaradczych(zastosowanych lub zaproponowanych) dla zminimalizowania skutków naruszenia	
7.	Rezultat postępowania naprawczego, osoba odpowiedzialna za postępowanie naprawcze	
8.	Obowiązek poinformowania do instytucji nadzorczej, innych instytucji (zachodzi, nie zachodzi z uzasadnieniem)[3]	
9.	Obowiązek zawiadomienia osoby, której dane dotyczą z określeniem sposobu przekazania informacji i opisem zaleceń (zawiadomienie wymagane, niewymagane w związku z określonymi uwarunkowaniami i działaniami administratora)	
10.	Monitoring ochrony danych osobowych	

W przypadku danych, dla których jednostka jest podmiotem przetwarzającym, o każdym naruszeniu należy powiadomić wyłącznie administratora danych osobowych

[2] Naruszenia klasyfikowane są do jednej z następujących kategorii:
-naruszenie nieistotne nie skutkuje ryzykiem naruszenia praw i wolności osób fizycznych
-naruszenie powoduje ryzyko dla praw i wolności osób fizycznych
-naruszenie skutkuje wysokim ryzykiem dla praw i wolności osób fizycznych
[3] W zależności od zakwalifikowania danego naruszenia należy zgłosić je:
-Prezesowi UODO- w odniesieniu do wszystkich naruszeń poza nieistotnymi
-osobie , której dane dotyczą, gdy naruszenie skutkuje wysokim ryzykiem dla praw lub wolności osób fizycznych oraz nie zachodzą przesłanki uchylające ten obowiązek z art. 34 ust. 3 RODO

Załącznik nr 3

....., dn.
..... r.
[data sporządzenia]

Prezes Urzędu Ochrony Danych Osobowych
.....

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Radu (UE) 2016/679 z 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), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl

na platformie biznes.gov.pl lub tradycyjną pocztą

Załącznik nr 4

FORMULARZ POWIADOMIENIA PODMIOTU DANYCH O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

.....

miejscowość, data sporządzenia powiadomienia

I FIRMA LUB NAZWA ADMINISTRATORA DANYCH OSOBOWYCH

KRS

NIP

REGON

ULICA I NUMER BUDYNKU ORAZ NUMER LOKALU

KOD POCZTOWY I MIEJSCOWOŚĆ

II DANE OSOBY REPREZENTUJĄCEJ ADMINISTRATORA

NAZWISKO I IMIĘ

STANOWISKO

TELEFON SŁUŻBOWY

E-MAIL SŁUŻBOWY

III OZNACZENIE PODMIOTU DANYCH

NAZWISKO I IMIĘ

ULICA I NUMER BUDYNKU ORAZ NUMER LOKALU

KOD POCZTOWY I MIEJSCOWOŚĆ

POWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Działając w imieniu i na rzecz administratora danych osobowych wskazanego powyżej, na podstawie art. 34 w związku z art. 33 ust. 3 lit. b, c i d rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, dalej: RODO), niniejszym zawiadamiam o naruszeniu ochrony danych osobowych.

1. Opis okoliczności naruszenia ochrony danych osobowych.

2. Na czym polegało naruszenie danych osobowych.

3. Dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego w ramach administratora danych osobowych

4. Możliwe konsekwencje naruszenia ochrony danych osobowych.

5. Środki zastosowane lub proponowane przez administratora danych osobowych w celu zminimalizowania naruszenia ochrony danych osobowych

Załącznik: np. pełnomocnictwo dla osoby dokonującej powiadomienia w imieniu i na rzecz administratora danych osobowych

Załącznik nr 5

Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych
WZÓR

„Z przykrością informujemy, ze w dniu ..... r. o godzinie ..... pracownik naszej placówki wysłał wiadomość e-mail zawierającą załącznik w postaci listy dłużników (zawierającą imię i nazwisko, adres zamieszkania, PESEL, saldo zadłużenia, tytuł prawny zadłużenia) do osoby nieupoważnionej.
Następstwem naruszenia ochrony danych jest udostępnienie osobie nieupoważnionej Pani/a danych osobowych we wskazanym wyżej zakresie.
Zdarzenie może powodować dla Pani/Pana następujące konsekwencje:
• osoby trzecie mogą podjąć próbę uzyskania na Pani/Pana szkodę, pożyczek w instytucjach pozabankowych np. przez Internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości; • osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL; • Pani/Pana dane osobowe mogą zostać wykorzystane np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego tym samym skorzystać z Pani/Pana praw obywatelskich; • Pani/Pana dane osobowe mogą zostać wykorzystane przez osobę trzecią do próby wyłudzenia ubezpieczenia; • osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilno-prawnych, np. najmu nieruchomości; • Pani/Pana dane osobowe mogą zostać wykorzystane przez osoby trzecie do ukrycia swojej tożsamości, np. przy otrzymywaniu mandatu.

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy aby Pan/Pani: • skorzystał/a z możliwość założenia konta w systemie informacji kredytowej celem monitorowania prób uzyskania kredytu, • zachował/a ostrożność przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem internetu czy telefonu, • skorzystał z możliwości zastrzeżenia dokumentu tożsamości w systemie dokumenty zastrzeżone (więcej informacji www.dokumentyzastrzezone.pl) i jego wymiany.

Administrator danych natychmiast skontaktował się z odbiorcą wiadomości, który zobowiązał się do niezwłocznego usunięcia otrzymanych danych ze wszelkich nośników danych wraz z ich kopiami zapasowymi. Wdrożono następujące działania zaradcze:

- zmieniono procedury korzystania z poczty elektronicznej;
- wprowadzono szyfrowanie wiadomości email zawierających dane osobowe;
- przeszkolono wszystkich pracowników placówki;
- naruszenie ochrony danych zgłosiliśmy Prezesowi UODO.

W celu uzyskania dodatkowych informacji może się Pani/Pan skontaktować z inspektorem ochrony danych w naszej spółce pod numerem telefonu ..... lub mailowo .....".

Załącznik nr 6

Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

Użytkownik jest zobowiązany powiadomić inspektora ochrony danych (lub inną osobę zajmującą się kwestiami ochrony danych, jeżeli inspektor ochrony danych nie został wyznaczony), jeśli stwierdzi, że doszło do naruszenia ochrony danych osobowych lub będzie miał podejrzenie, że mogło dojść do takiego zdarzenia.

Typowe sytuacje, o których użytkownik powinien powiadomić inspektora ochrony danych:

1) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
2) zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki,
3) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
4) otwarte drzwi do pomieszczeń, szaf, w których przechowywane są dane osobowe,
5) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
6) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia inspektora ochrony danych,
7) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
8) telefoniczne próby wyłudzenia danych osobowych,
9) kradzież komputerów lub CD, twardych dysków, pendrive'a z danymi osobowymi,
10) e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
11) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
12) przechowywanie haseł do systemów w pobliżu komputera.

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
- zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora lub osoby upoważnionej.

Załącznik nr 7

METODA OCENY WAGI NARUSZENIA WG. AGENCJA UNII EUROPEJSKIEJ DS. BEZPIECZEŃSTWA SIECI I INFORMACJI (ENISA)[4]

Narzędzie pozwala na ocenę wagi naruszeń danych i ułatwia podjęcie decyzji zarówno o powiadomieniu organu jak i osób, których dane zostały naruszone.

GR29: Czynniki ryzyka:	Rodzaj naruszenia (poufność, integralność, dostępność)
	Charakter, wrażliwość i ilość danych osobowych
	Łatwość identyfikacji osób fizycznych
	Waga konsekwencji dla osób fizycznych
	Cechy szczególne danej osoby fizycznej
	Cechy szczególne administratora
	Liczba osób fizycznych, na które naruszenie wywiera wpływ

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.

Kontekst Przetwarzania Danych – KPD

KPD = A + B

Kontekst Przetwarzania Danych-= A + B	
A – rodzaj i poziom wrażliwości danych	Dane podstawowe = 1
	Dane dotyczące zachowań osoby (behawioralne)= 2
	Dane finansowe lub poufne = 3
	Dane szczególne = 4

[4] https://www.enisa.europa.eu/publications/dbn-severity/

B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę	Szeroki zakres danych dla tej osoby(+) Zakres powinie być rozpatrywany zarówno pod wzg. Czasu trwania naruszenia jak i zakresu danych
	Duży wolumen danych (+) Liczba osób, których dotyczy naruszenie
	Charakter danych (+/-)
	Specyfika administratora (+) Może ujawniać dodatkowe informacje np. czynnik wyższy dla klientów apteki niż dla sklepu internetowego
	Specyfika podmiotu danych (+) Osoby wymagające szczególnej opieki w tym dzieci
	Możliwe negatywne skutki dla podmiotu danych (+)
	Publiczna dostępność danych przed naruszeniem (-) Dane były publicznie dostępne przed naruszeniem
	Nieważność danych (-) Dane utraciły znaczenie lub są nieaktualne

Prawdopodobieństwo identyfikacji – PI

Prawdopodobieństwo identyfikacji	Znikome = 0,25 Trudno zidentyfikować osobę ale nadal jest to możliwe w określonych warunkach
	Ograniczone = 0,5
	Wysokie = 0,75
	Maksymalne = 1 Możliwość identyfikacji osoby bez dodatkowych działań.

Okoliczności Naruszenia - ON

ON = NP + NI + ND + IDS

Okoliczności Naruszenia = NP + NI + ND + IDS	
Naruszenie Poufności NP– Dane ujawnione:	znanym nieuprawnionym odbiorcom danych (+0,25)
	nieznanej liczbie nieuprawnionych odbiorców danych (+0,5)
Naruszenie Integralności NI- Dane zmienione ale:	możliwe jest ich odzyskanie (+0,25)
	brak jest możliwości ich odzyskania (+0,5)
Naruszenie Dostępności ND- Niedostępność danych:	czasowa (+0,25)
	pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)

Intencjonalne Działanie Sprawcy IDS (+0,5)
Czynnik zwiększający prawdopodobieństwo nieprawidłowego wykorzystania danych np. włamanie lub kradzież danych w celu ich sprzedaży lub ujawnienia

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