MIEJSKA BIBLIOTEKA PUBLICZNA
ul. Piłata 42
05-230 KOBYŁKA
tel. 22 763-42-42

Kobyłka dn., 04.06.2020r.

Zarządzenie Nr 9/2020

Dyrektora Miejskiej Biblioteki Publicznej w Kobyłce
z dnia 04.06.2020 r.
w sprawie wprowadzenia
Procedury zarządzania naruszeniami danych osobowych
w Miejskiej Bibliotece Publicznej w Kobyłce

DYREKTOR
Miejskiej Biblioteki Publicznej
Sylwia Carzyńska
Sylwia Carzyńska

Na podstawie Art. 24 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 (Dziennik Urzędowy Unii Europejskiej | L 119/1) dalej RODO.

zarządzam co następuje:

§1

Wprowadzam Procedurę zarządzania naruszeniami danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce, której treść stanowi załącznik nr 1 do zarządzenia.

§2

Zobowiązuję pracowników Miejskiej Biblioteki Publicznej w Kobyłce do zapoznania się z treścią załącznika nr 1 do niniejszego zarządzenia

§3

Zobowiązuję wszystkich pracowników do przestrzegania Procedury zarządzania naruszeniami danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce pod groźbą sankcji przewidzianych przepisami prawa.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

04.06.2020 Sylwia Cerpińska

(data i podpis dyrektora)

Załącznik nr 1
do Zarządzenia nr 9/2020
Dyrektora MBP w Kobyłce
z dnia 04.06.2020 r.

Procedura zarządzania naruszeniami danych osobowych

Miejskiej Biblioteki Publicznej w Kobyłce

Zatwierdzona: 04 czerwca 2020 r.

SPIS TREŚCI

1. DEFINICJA I SKRÓTY

Naruszenie ochrony danych – naruszenie przepisów o ochronie danych osobowych wywołujące ryzyko naruszenia praw i wolności osób, których dane dotyczą.

Osoba, której dane dotyczą – osoba fizyczna/osoba fizyczna prowadząca działalność gospodarczą, której dane przetwarza Administrator.

Organ Nadzorczy, UODO – Urząd Ochrony Danych Osobowych (UODO), niezależny organ publiczny ustanowiony w celu kontroli realizacji przepisów o ochronie danych osobowych, na czele, którego stoi Prezes Urzędu Ochrony Danych Osobowych (PUODO).

Podmiot przetwarzający – podmiot (osoba fizyczna lub firma) któremu Administrator powierzył dane osobowe do przetwarzania, na podstawie pisemnej umowy powierzenia przetwarzania danych osobowych.

Administrator Danych Osobowych (ADO) –Administratorem danych osobowych jest Miejska Biblioteka Publiczna w Kobyłce przy ul. Fałata 4a, 05-230 Kobyłka, (dalej: Biblioteka lub MBP), ADO reprezentowany jest przez Dyrektora Biblioteki (dalej: Dyrektor).

Inspektor Ochrony Danych (IOD) - Osoba wyznaczona przez Administratora danych zgodnie Art. 37 RODO.

Administrator Systemu, Informatyk - dedykowana osoba, zespół osób lub podmiot zewnętrzny wyznaczone do obsługi informatycznej Administratora Danych Osobowych.

Pracownik – osoba wykonująca pracę pod nadzorem Administratora danych na podstawie formalnych ustaleń (osoba pracująca (na podstawie stosunku pracy) oraz współpracująca (na podstawie zlecenia, umowy o dzieło, lub innego rodzaju umowy cywilnoprawnej (UCP)). Osobą taką jest pracownik związany z Administratorem danych umową o pracę, jak również inne osoby np.: praktykanci, stażyści, osoby wykonujące prace na podstawie umów cywilnych lub B2B (prowadzące działalność gospodarczą) pod warunkiem, że są włączone w strukturę organizacyjną Administratora.

2. ODPOWIEDZIALNOŚĆ

Osoby wykonujące opisane w procedurze działania (pracownicy, podmiot przetwarzający) są odpowiedzialne za ich prawidłową i terminową realizację.

Inspektor Ochrony Danych odpowiedzialny jest za rekomendowanie zgłoszenia w zakresie:

- Obowiązku zgłaszania naruszeń do organu nadzorczego
- Obowiązku informowania o naruszeniach osób, których dane dotyczą

Pracownicy odpowiedzialni są, za zgłaszanie naruszeń ochrony danych zgodnie z niniejszą procedurą.

Administrator Systemu, Informatyk odpowiedzialny jest za monitorowanie systemów informatycznych pod kątem naruszeń ochrony danych.

3. WSTĘP

Procedura określa odpowiedzialności i zasady postępowania obowiązujące przy identyfikowaniu naruszeń, zgłaszaniu naruszeń do organu nadzorczego oraz informowaniu o naruszeniach osób, których naruszenie dotyczy.

Administrator danych zarządza naruszeniami ochrony danych osobowych zgodnie z wymaganiami Art. 37 RODO.

4. OPIS POSTĘPOWANIA

1. Zgłaszanie naruszeń ochrony danych przez pracowników

1.1. Każdy pracownik, ma obowiązek niezwłocznego zgłaszania naruszeń przetwarzania danych osobowych bezpośrednio do IOD lub do Administratora Danych lub na adres mailowy iod@biblioteka.kobylka.pl ustanowiony do zgłoszeń. Dotyczy to również sytuacji, gdy zgłoszenie naruszenia danych składa właściciel danych lub inny podmiot zainteresowany lub działający w imieniu właściciela danych.

1.2. W celu ustalenia czy doszło do naruszenia pracownik ma obowiązek skonsultowania potencjalnego naruszenia z Inspektorem Ochrony Danych.

1.3. W konsultacjach z IOD zgłaszający ma obowiązek przekazać następujące informacje:

- **Czas stwierdzenia** (tj. datę i godzinę zidentyfikowania zdarzenia).
- **Opis naruszenia** (ogólną informację o tym co się wydarzyło).
- **Kategorie osób** (kogo dotyczy naruszenie np. pracowników, klientów, kontrahentów itp.)
- **Skalę naruszenia** (tj. informację ilu osób i jakiego zakresu danych dotyczy naruszenie).
- **Możliwe skutki** (tj. informację o możliwych konsekwencjach zdarzenia).
- **Propozycję wdrożenia działań zaradczych** (tj. co można zrobić żeby zaradzić naruszeniu i zmniejszyć prawdopodobieństwo jego ponownego wystąpienia)
- **Inne przydatne informacje** (tj. informacje, które w ocenie zgłaszającego są istotne dla sprawy).

1.4. W przypadku uznania przez IOD, że doszło do naruszenia, osoba odpowiedzialna przygotowuje zgłoszenie i przekazuje je do IOD? (wzór zgłoszenia określono w **załączniku nr 4**).

1.5. W przypadku braku wątpliwości pracownika, że doszło do naruszenia można przesłać zgłoszenie pisemne bez uprzednich konsultacji z IOD do IOD.

1.6. Na podstawie przekazanych informacji IOD ustala dalszy sposób postępowania, który opisany został w pkt 3 niniejszej procedury.

2. Zgłaszanie naruszeń przez podmioty przetwarzające

2.1. Podmiot przetwarzający, ma obowiązek zgłaszania naruszeń przetwarzania danych osobowych bez zbędnej zwłoki, nie później niż w terminie ustalonym w umowie powierzenia przetwarzania danych osobowych zawartej z Administratorem Danych Osobowych, bezpośrednio do IOD lub do Administratora Danych lub na adres mailowy iod@biblioteka.kobylka.pl ustanowiony do zgłoszeń.

2.2. Zgłoszenie podmiotu przetwarzającego zawiera:

- **Czas stwierdzenia** (tj. datę i godzinę zidentyfikowania zdarzenia).
- **Opis naruszenia** (ogólną informację o tym co się wydarzyło).

- **Kategorie osób** (kogo dotyczy naruszenie np. pracowników, klientów, kontrahentów itp.)
- **Skalę naruszenia** (tj. informację ilu osób i jakiego zakresu danych dotyczy naruszenie).
- **Możliwe skutki** (tj. informację o możliwych konsekwencjach zdarzenia).
- **Propozycję wdrożenia działań zaradczych** (tj. co można zrobić żeby zaradzić naruszeniu i zmniejszyć prawdopodobieństwo jego ponownego wystąpienia)
- **Inne przydatne informacje** (tj. informacje, które w ocenie zgłaszającego są istotne dla sprawy).

2.3. W przypadku uznania przez IOD, że doszło do naruszenia należy przesłać zgłoszenie w formie udokumentowanej (wzór zgłoszenia określono w **załączniku nr 4**).

2.4. W przypadku braku wątpliwości, że doszło do naruszenia można przesłać zgłoszenie pisemne bez uprzednich konsultacji z IOD.

2.5. Na podstawie przekazanych informacji Inspektor Ochrony Danych ustala dalszy sposób postępowania, który opisany został w pkt 3 niniejszej procedury.

3. **Sposób oceny/ klasyfikacji naruszenia**

3.1. **Inspektor Ochrony Danych** po otrzymaniu zgłoszenia przeprowadza jego analizę i w zależności od ustalonej wagi i poziomu naruszenia wydaje rekomendację w zakresie dalszego postępowania tj.:

3.1.1. Zgłoszenia do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych).

3.1.2. Poinformowania Osób, których dane dotyczą.

3.1.3. Wewnętrznej rejestracji naruszenia.

3.2. Waga i poziom naruszenia są ustalane na podstawie Metody oceny wagi naruszenia wg. Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) z użyciem kwestionariusza oceny poziomu naruszenia (wzór kwestionariusza określono w **załączniku nr 1**).

3.3. Po otrzymaniu rekomendacji od IOD Administrator Danych Osobowych podejmuje ostateczną decyzję w sprawie dalszego postepowania (tj. zgłoszenia do UODO, poinformowania osób, których dane dotyczą, wewnętrznej rejestracji, rekomendacji działań zapobiegających wystąpienie naruszenia w przyszłości lub niwelujące jego negatywne skutki i zaplanowanie tych działań).

3.4. W przypadku, gdy zgłoszone naruszenie zostanie zakwalifikowane, jako naruszenie wymagające zgłoszenia do organu nadzorczego (PUODO) podejmowane są następujące czynności:

3.4.1. Sporządza się zgłoszenie naruszenia (wzór zgłoszenia określono w **załączniku nr 2**) lub dokonuje zgłoszenia elektronicznie przez formularz dostępny na stronie https://uodo.gov.pl/pl/134/233

3.4.2. Wypełnione zgłoszenie przesyła się do Urzędu Ochrony Danych Osobowych.

3.5. Zgłoszenie naruszenia ochrony danych do organu nadzorczego następuje nie później niż w ciągu 72 godzin od jego stwierdzenia z wyłączeniem szczególnych przypadków (np. ze względu na czasochłonność analizy naruszenia i jego skalę), kiedy to administrator zgłasza naruszenie w ciągu 72 godzin w niepełnej formie (bez przesłania niektórych informacji). Dodatkowe informacje o naruszeniu przesyła się do organu nadzorczego niezwłocznie (w trybie zgłoszenia uzupełniającego), gdy tylko uda się poczynić dodatkowe ustalenia.

3.6. Naruszenie wymagające zgłoszenia do organu nadzorczego rejestrowane jest także w wewnętrznym rejestrze naruszeń prowadzonym przez IOD (wzór rejestru określono **załącznik nr 3**).

3.7. Naruszenia, dla których zachodzi małe prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób, których dane dotyczą rejestrowane są wyłącznie u administratora w wewnętrznym rejestrze naruszeń prowadzonym przez IOD.

3.8. W przypadku gdy zaakceptowane i zaplanowane zostały działania zapobiegające wystąpieniu naruszenia w przyszłości lub niwelujące jego negatywne skutki, IOD weryfikuje skuteczność ich wdrożenia w uzgodnionym ze zgłaszającym terminie.

4. Informowanie o naruszeniach osoby, której dane dotyczą

4.1. W przypadku ustalenia, że naruszenie może spowodować wysokie ryzyko naruszenia praw lub wolności (zgodnie z analizą przeprowadzoną w kwestionariuszu oceny poziomu naruszenia) Administrator Danych Osobowych zawiadamia osoby, których dane dotyczą o takim naruszeniu.

4.2. Formę i sposób zawiadomienia dobiera się w ramach bieżących potrzeb np. poprzez wysłanie komunikatów o naruszeniu emailem, pocztą, sms, bezpośrednio do osoby/ osób, której/ych dane dotyczą.

4.3. Zawiadomienie nie jest konieczne, jeżeli Administrator Danych Osobowych 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;

4.4. W przypadku, gdy poinformowanie bezpośrednio zainteresowanych wymagałoby nadmiernie dużego wysiłku możliwe jest również poinformowanie poprzez:

4.4.1. Publikację ogłoszenia w prasie

4.4.2. Wyświetlanie komunikatów o naruszeniu na stronie www Administratora Danych Osobowych

4.5. Zawiadomienie zawiera:

4.5.1. Dane IOD (imię, nazwisko, dane kontaktowe), jeśli został wyznaczony,

4.5.2. Opis konsekwencji naruszenia ochrony danych,

4.5.3. Opis środków zastosowanych lub zaplanowanych do zastosowania w celu zaradzenia naruszeniu i zniwelowania ich negatywnych skutków.

4.6. Wyniki analizy naruszeń brane są pod uwagę przy m.in. ocenie ryzyka, decyzjach dotyczących wdrażania zabezpieczeń i przygotowywaniu programu dotyczącego podnoszenia świadomości pracowników.

5. ZAŁĄCZNIKI

Załącznik nr 1 - wzór kwestionariusza obliczania poziomu naruszenia.

Załącznik nr 2 - wzór zgłoszenia naruszenia.

Załącznik nr 3 - wzór rejestru naruszeń.

Załącznik nr 4 – karta zgłoszenia naruszenia

Załącznik nr 1

Kwestionariusz obliczania poziomu naruszenia przetwarzania danych osobowych (PN)

Informacje o naruszeniu (opis naruszenia):
Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Poziom naruszenia obliczamy według wzoru: PN=KP X SI + ON (P+I+D+C) gdzie
PN- poziom naruszenia
KP – kontekst przetwarzania
SI – stopień identyfikacji (łatwość identyfikacji)
ON –okoliczności naruszenia **(P (Poufność) + In (Integralności) + D (Dostępności) + IS (Celowość działania)**

Krok 1 – ustalenie wartości kontekstu przetwarzania

KONTEKST PRZETWARZANIA (KP) - jest to główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania). Ocenę przyznajemy w skali 1-4. Ocenę możemy podwyższyć (+) lub obniżyć (-) o 1 punkt, gdy wystąpią następujące okoliczności:

- **Naruszenie dotyczy szerokiego zakresu danych/wolumen danych (+)**
  - zwiększamy ocenę gdy np. usunięto/zmieniono/ujawniono bardzo dużą liczbę danych
- **Charakter danych (+/-)**
  - zwiększamy ocenę gdy np. usunięciu/zmianie/ujawnieniu uległy dane szczególnie istotne dla organizacji (np. numery PESEL pracowników/klientów (w tym dane wrażliwe w rozumieniu art. 9 RODO),
  - zmniejszamy ocenę, gdy usunięciu/zmianie/ujawnieniu uległy dane o marginalnym znaczeniu dla organizacji (np. same Imiona i Nazwiska bez żadnych powiązań).
- **Specyfika podmiotu danych lub administratora (+/-)**
  - zwiększamy ocenę, gdy administrator prowadzi działalność zaufania publicznego lub na dużą skalę (np. Urząd dużego miasta, Sklep internetowy prowadzący sprzedaż internetową na dużą skalę, fundacje).
  - zmniejszamy ocenę, gdy administrator nie prowadzi działalności istotnej z pkt. widzenia skali lub zaufania publicznego (np. niewielki sklep internetowy, niewielka jednostka organizacyjna gminy itp.)
- **Możliwe negatywne skutki dla podmiotu danych (+)**
  - zwiększamy ocenę, gdy możliwe są do zidentyfikowania negatywne skutki takie jak np. (prowadzące do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną).
- **Publiczna dostępność danych przed naruszeniem (-)**
  - zmniejszamy ocenę, gdy dane były zgodnie z prawem publicznie dostępne przed naruszeniem (zamieszczone na BIP/WWW/np. dane kontaktowe, pliki itp.)
- **Nieważność/Nieistotność danych (-)**
  - zmniejszamy ocenę, gdy dane są nieistotne (np. lista wpłat na wyjście do kina dzieci, które już się odbyło, nieaktualne numery telefonów, nieaktualne dane adresowe itp.)

Wartość oceny	Opis pomocniczy do ustalenia oceny wartości (dotyczy utraty poufności (P), dostępności (D), integralności(I).
1	gdy wśród danych znajdują się tylko **dane zwykłe** (np. imię i nazwisko, adres, nr tel., email) Przykłady: **D - *Utrata listy obecności ze szkolenia;*** **I – *Nieautoryzowane zmiany w liście obecności ze szkolenia (np. zalanie kawą, podarcie, „zamazanie";*** **P – *Wysyłka listy obecności na błędny adres firmy szkoleniowej, która miała wystawić zaświadczenia)***
2	gdy wśród danych znajdują się **dane behawioralne** (np. lokalizacja, zachowania, oceny) **D - *Utrata raportu z aktywności pracowników monitorowanych GPS;*** **I – *Nieautoryzowana zmiana treści raportu z aktywności pracowników monitorowanych GPS;*** **P – *Opublikowanie raportu w sieci firmowej***
3	gdy wśród danych znajdują się **dane finansowe** (np. nr rachunku bankowego, wysokość wynagrodzenia) **D- *Utrata listy płac;*** **I – *Nieautoryzowane zmiany w liście płac;*** **P – *Wysyłka listy płac do niewłaściwego odbiorcy;***
4	gdy wśród danych znajdują się dane szczególne (Art. 9) i dane dotyczące postepowań sądowych i naruszeń prawa (Art. 10 RODO) **D- *Utrata zaświadczenia lekarskiego o zdolności do pracy;*** **I – *Częściowe zniszczenie zaświadczenia lekarskiego uniemożliwiające np. odtworzenie informacji o dacie ważności;***

	P – *Pozostawienie zaświadczenia w miejscu ogólnodostępnym;*
Wynik:	**KP=**
Uzasadnienie oceny:	

Krok 2 – ocena łatwości identyfikacji osób, których dane dotyczą

STOPIEŃ IDENTYFIKACJI (SI) - jest to czynnik korygujący KP, który może obniżyć wynik w zależności od zaistniałych okoliczności tj. jak oceniamy prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich).

Wartość oceny	Opis pomocniczy do ustalenia oceny wartości
0,25	Ocenę dajemy gdy: • nie dotyczy poufności (naruszenie dotyczy dostępności i integralności); • identyfikacja za pomocą danych objętych naruszeniem jest bardzo trudna (tj. ustalenie tożsamości właściciela danych jest bardzo trudne lub niemożliwe).
0,5	Ocenę dajemy, gdy dane zostały ujawnione ale identyfikacja za pomocą danych objętych naruszeniem jest trudna
0,75	Ocenę dajemy, gdy dane zostały ujawnione ale identyfikacja za pomocą danych objętych naruszeniem jest łatwa
1	Ocenę dajemy, gdy dane zostały ujawnione ale identyfikacja za pomocą danych objętych naruszeniem jest bardzo łatwa lub natychmiastowa (jednoznaczna ze wskazaniem tożsamości właściciela/właścicieli danych)
• **Wynik:**	**SI=**
Uzasadnienie oceny	

Krok 3 – Ocena okoliczności naruszenia

OKOLICZNOŚCI NARUSZENIA (ON) - jest to czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku. ON wyliczany jest na podstawie sumy oceny wszystkich okoliczności naruszenia jakie wystąpiły (tj. Poufności + Integralności + Dostępności + Intencjonalności Działań Sprawcy)

ON=P+I+D+C

Wartość oceny	Poufność	Integralność	Dostępność	Celowość
0	nie nastąpiło naruszenie poufności	nie nastąpiło naruszenie integralności	nie nastąpiło naruszenie dostępności	gdy działanie sprawcy nie jest celowe
0,25	gdy udostępniono dane znanym odbiorcom lub mały zakres ujawnienia	gdy w wyniku naruszenia integralności możliwe jest odzyskanie zmienionych/uszkodzonych danych	gdy utrata dostępności jest czasowa	trudno powiedzieć
0,5	gdy dane udostępnione nieznanej liczbie odbiorców	gdy w wyniku naruszenia integralności brak jest możliwości odzyskania zmienionych/uszkodzonych danych	gdy naruszenie dostępności jest nieodwracalne i brak jest możliwości odzyskania danych	gdy działanie sprawcy jest celowe
Wynik	**ON=**			

Uzasadnienie	

Krok 4 Określenie poziomu ryzyka naruszenia praw i wolności podmiotów danych

Na podstawie wzoru **PN=KP X SI + ON (P+I+D+C)** ustalamy poziom naruszenia ochrony danych osobowych

KP		
SI		
ON (P+I+D+C)		
PN=		
PN<2	POZIOM BARDZO NISKI	Niskie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Osoby, których dane dotyczą nie zostaną dotknięte sutkami naruszenia lub wywoła ono drobne niedogodności
2 ≤ PN < 3	POZIOM NISKI	Skutki naruszenia będą odczuwalne na poziomie utrudnień. Osoby, których dane dotyczą mogą napotkać niedogodności, które są możliwe do wyeliminowania
3 ≤ PN < 4	POZIOM ŚREDNI	Skutki naruszenia będą znaczące i trudne do wyeliminowania. Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami.
4 ≤ PN	POZIOM WYSOKI	Skutki naruszenia będą poważne, bardzo trudne do wyeliminowania a nawet nieodwracalne.
Wynik:		

Krok 5 Postępowanie z naruszeniem (w zależności od wyniku poziomu naruszenia należy podjąć określone działania opisane poniżej)

PN<2	POZIOM BARDZO NISKI	1. Naruszenie nie wymaga zgłoszenia do organu nadzorczego. 2. Należy wpisać naruszenie do rejestru naruszeń prowadzonego przez IOD. 3. Należy dokonać analizy wdrożonych zabezpieczeń oraz jeżeli ma to zastosowanie podjąć działania ograniczające następstwa naruszenia oraz działania zapobiegawcze (środki zaradcze (pozwalających na zmniejszenie prawdopodobieństwa lub skutków wystąpienia naruszenia w przyszłości).
2 ≤ PN < 3	POZIOM NISKI	1. Należy wpisać naruszenie do rejestru naruszeń prowadzonego przez IOD. 2. Należy powiadomić organ nadzorczy o naruszeniu (zgłoszenie należy wysłać w ciągu 72 godzin od stwierdzenia naruszenia). 3. Należy podjąć działania ograniczające następstwa naruszenia oraz działania zapobiegawcze (środki zaradcze (pozwalających na zmniejszenie prawdopodobieństwa lub skutków wystąpienia naruszenia w przyszłości).
3 ≤ PN < 4	POZIOM ŚREDNI	1. Należy wpisać naruszenie do rejestru naruszeń prowadzonego przez IOD. 2. Należy powiadomić organ nadzorczy o naruszeniu (zgłoszenie należy wysłać w ciągu 72 godzin od stwierdzenia naruszenia). 3. Należy podjąć działania ograniczające następstwa naruszenia oraz działania zapobiegawcze (środki zaradcze (pozwalających na zmniejszenie prawdopodobieństwa lub skutków wystąpienia naruszenia w przyszłości).

		4. Należy rozważyć konieczność powiadomienia osób, których dane dotyczą i jeżeli to zasadne powiadomić je.
4 ≤ PN	POZIOM WYSOKI	1. Należy wpisać naruszenie do rejestru naruszeń prowadzonego przez IOD. 2. Należy powiadomić organ nadzorczy o naruszeniu (zgłoszenie należy wysłać w ciągu 72 godzin od stwierdzenia naruszenia). 3. Należy podjąć działania ograniczające następstwa naruszenia oraz działania zapobiegawcze (środki zaradcze (pozwalających na zmniejszenie prawdopodobieństwa lub skutków wystąpienia naruszenia w przyszłości). 4. Należy powiadomić osoby, których dane dotyczą o naruszeniu.
Szczegółowy opis działań podjętych w ramach postepowania z naruszeniem (w tym zaplanowanie działań naprawczych i zapobiegawczych):		

.....

Data i podpis Inspektora Ochrony Danych

.....

Data i podpis Administratora

Zgłoszenie naruszenia ochrony danych osobowych

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) Kliknij tutaj, aby wprowadzić tekst.

◉ Zgłoszenie kompletne/jednorazowe	○ Zgłoszenie wstępne	○ Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić tekst.

☐ Naruszenie zostało lub zostanie zgłoszone organowi ochrony danych osobowych w innym państwie Jeśli tak, podaj w jakim.

☐ Naruszenie zostało lub zostanie zgłoszone innym organom np. Policja, CSIRT NASK, CSIRT GOV, CSIRT MON (najedź myszką na nazwę organu by dowiedzieć się więcej)

Podaj nazwy tych organów
Kliknij tutaj, aby wprowadzić tekst.

Podaj numer/sygnaturę zgłoszenia do innego organu
Kliknij tutaj, aby wprowadzić tekst.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.

REGON (opcjonalnie) Podaj numer. NIP (opcjonalnie) Podaj numer. KRS (opcjonalnie) Podaj numer.

Sektor (opcjonalnie) Dla sektora publicznego: Wybierz element. Dla sektora prywatnego: Wybierz element.

2B. Adres siedziby administratora danych

Ulica	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer Numer lokalu Podaj numer
Miejscowość	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Powiat	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Państwo	Kliknij tutaj, aby wprowadzić tekst.

2C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
2.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
3.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
4.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
5.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

2D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** oraz dowód uiszczenia opłaty skarbowej

2E. Inspektor ochrony danych

Imię i nazwisko imię i nazwisko. Numer telefonu Numer telefonu. Adres e-mail E-mail.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
2.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
3.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
4.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
5.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

☐ a) Zgubienie lub kradzież nośnika/urządzenia

☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ d) Nieuprawnione uzyskanie dostępu do informacji

☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ j) Niezamierzona publikacja

☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy

☐ l) Ujawnienie danych niewłaściwej osoby

☐ m) Ustne ujawnienie danych osobowych

4C. Działanie złośliwego oprogramowania (odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczono pole f)

a) Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności?
(w sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu)

Kliknij tutaj, aby wprowadzić tekst.

b) Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (podaj nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin)

Kliknij tutaj, aby wprowadzić tekst.

c) Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak to w jakim czasie ją przywrócił?

Kliknij tutaj, aby wprowadzić tekst.

UWAGA: *Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem https://incydent.cert.pl/. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe.*
O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza) podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska).

4D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

4E. Charakter

☐ Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐ Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐ Naruszenie dostępności danych
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4F. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- ☐ Nazwiska i imiona
- ☐ Imiona rodziców
- ☐ Data urodzenia
- ☐ Numer rachunku bankowego
- ☐ Adres zamieszkania lub pobytu
- ☐ Numer ewidencyjny PESEL
- ☐ Adres e-mail
- ☐ Nazwa użytkownika i/lub hasło
- ☐ Dane dotyczące zarobków i/lub posiadanego majątku
- ☐ Nazwisko rodowe matki
- ☐ Seria i numer dowodu osobistego
- ☐ Numer telefonu
- ☐ Wizerunek
- ☐ Inne, wskaż jakie:

Kliknij tutaj, aby wprowadzić tekst.

6B. Dane szczególnej kategorii

- ☐ 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

6C. Dane, o których mowa w art. 10 RODO

- ☐ Dane dotyczące wyroków skazujących
- ☐ Dane dotyczące czynów zabronionych
- ☐ Inne

Kliknij tutaj, aby wprowadzić tekst.

7. Kategorie osób

- ☐ Pracownicy
- ☐ Użytkownicy
- ☐ Subskrybenci
- ☐ Studenci
- ☐ Uczniowie
- ☐ Służby mundurowe (np. wojsko, policja)
- ☐ Klienci (obecni i potencjalni)
- ☐ Klienci podmiotów publicznych
- ☐ Pacjenci
- ☐ Dzieci
- ☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie:
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie
W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące 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
- ☐ Nieuprawnione odwrócenie pseudonimizacji
- ☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

- ◉ Tak
- ○ Nie

Uzasadnienie

Kliknij tutaj, aby wprowadzić tekst.

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

10. Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

◉ Tak	○ Nie, ale zostaną zawiadomione Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO.	○ Nie, nie zostaną zawiadomione, ponieważ:	○ Nie oceniłem jeszcze

Czy indywidualnie?

◉ Tak

○ Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został bądź zostanie wydany publiczny komunikat lub zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą, zostały bądź zostaną poinformowane w równie skuteczny sposób.

Wskaż datę zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

Wskaż datę planowanego zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

Liczba zawiadomionych osób
Kliknij tutaj, aby wprowadzić tekst.

☐ Nie znam jeszcze daty kiedy zamierzam zawiadomić osoby, których dane dotyczą

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą
Kliknij tutaj, aby wprowadzić tekst.

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.

Pamiętaj, że zawiadomienie powinno:

- opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Kliknij tutaj, aby wprowadzić tekst.

○ przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

○ po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

○ stwierdzono brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (uzasadnienie w pkt. 8B formularza).

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

11. Przetwarzanie transgraniczne

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Islandia	☐ Liechtenstein
☐ Litwa	☐ Luksemburg	☐ Łotwa	☐ Malta
☐ Niemcy	☐ Norwegia	☐ Portugalia	☐ Rumunia
☐ Słowacja	☐ Słowenia	☐ Szwecja	☐ Węgry
☐ Wielka Brytania	☐ Włochy		

Data, miejscowość
(dla zgłoszenia w formie papierowej)

Podpis osoby lub osób upoważnionych do reprezentowania administratora[1]
(dla zgłoszenia w formie papierowej)

[1] Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa

Informacja:

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO[1] bądź art. 44 ust. 1 – 5 DODO[2], podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

Okres przechowywania danych.
Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 RODO i art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

---

[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 (RODO) oraz podjętych działań.

[2] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Rejestr zgłoszeń/naruszeń przetwarzania danych osobowych

Lp.	Data	Opis naruszenia	Ocena (naruszenie/zgłoszenie nie będące naruszeniem)*	Skutki naruszenia	Ryzyko dla osób których dane dotyczą (wysokie/niskie)	Opis działań podjętych w celu zapobieżenia skutkom naruszenia w przyszłości	Zgłoszenie do PUODO? (Tak/Nie)	Data zgłoszenia do UODO

*** W przypadku oceny zgłoszenia jako nie będącego naruszeniem nie są wypełniane kolumny dotyczące naruszenia (tj. skutki naruszenia, ryzyko, opis działań zapobiegawczych, informacja o zgłoszeniu do PUODO, Data zgłoszenia).**

Załącznik nr 4 – Zgłoszenie naruszenia Ochrony Danych Osobowych

Kliknij tutaj, aby wprowadzić datę. (data, Imię, Nazwisko zgłaszającego, funkcja) **ZGŁOSZENIE** **W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH**		
Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu Kliknij tutaj, aby wprowadzić datę.r.		
1.	***Czas stwierdzenia naruszenia*** *(tj. data i godzina zidentyfikowania zdarzenia).*	
2.	**Opis zdarzenia** *(co się stało?)*	
3.	**Kategoria osób** *(czyje dane uległy naruszeniu np. pracowników, klientów, dłużników, kontrahentów itp.)*	
4.	**Skala naruszenia** *(informacja ilu osób i jakiego zakresu danych dotyczy naruszenie)*	
5.	**Propozycja wdrożenia działań zaradczych** (tj. co można zrobić żeby zaradzić naruszeniu i zmniejszyć prawdopodobieństwo jego ponownego wystąpienia)	
6.	**Inne przydatne informacje** (tj. informacje, które w ocenie zgłaszającego są istotne dla sprawy)	

* Zgłoszenie należy wysłać na adres mailowy Inspektora Ochrony Danych lub na inny uzgodniony z IOD