MIEJSKA BIBLIOTEKA PUBLICZNA W KOBYŁCE
im. Stanisława Ryszarda Szpotańskiego
ul. Leśna 8 lokal 0.3
05-230 KOBYŁKA
tel. 22 763-42-42
REGON 000939289, NIP 1250559111

Kobyłka, dnia: 17.05.2024 roku

Zarządzenie Dyrektora Miejskiej Biblioteki Publicznej w Kobyłce
im. Stanisława Ryszarda Szpotańskiego
nr 10/2024
z 17 maja 2024 roku

w sprawie wprowadzenia Procedury zarządzania naruszeniami danych osobowych w Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

Na podstawie art. 33 i art. 34 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) zarządzam co następuje:

§ 1

Wprowadzam Procedurę Zarządzania naruszeniami danych osobowych.

§ 2

Zobowiązuję pracowników Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego do zapoznania się z treścią i załącznikami Procedury.

§ 3

Zobowiązuje wszystkich pracowników do stosowania zasada zawartych w Procedurze zarządzania naruszeniami danych osobowych.

§ 4

Zarządzenie nr 9/2020 Dyrektora Miejskiej Biblioteki Publicznej w Kobyłce z dnia 04.06.2020 roku dotyczące wprowadzenia Procedury Zarządzania naruszeniami danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce traci moc.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Sylwia Carzyńska

DYREKTOR
Miejskiej Biblioteki Publicznej w Kobyłce
im. Stanisława Ryszarda Szpotańskiego

Sylwia Carzyńska

MIEJSKA BIBLIOTEKA PUBLICZNA W KOBYŁCE
im. Stanisława Ryszarda Szpotańskiego
ul. Leśna 8 lokal 0.3
05-230 KOBYŁKA
tel. 22 763-42-42
REGON 000939289, NIP 1250559111

Procedura zarządzania naruszeniami danych osobowych

Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

Zatwierdzona: 17 maj 2024 r.

Stwierdzam zgodność z oryginałem
Kobyłka, dnia 11.06.2024
Z up. Burmistrza
Sylwia Carzyńska
Dyrektor M.B.P. w Kobyłce
im. S. R. Szpotańskiego

DYREKTOR
Miejskiej Biblioteki Publicznej w Kobyłce
im. Stanisława Ryszarda Szpotańskiego
Sylwia Carzyńska

Procedura zarządzania naruszeniami danych osobowych

Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

Zatwierdzona: 17 maj 2024 r.

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 im. Stanisława Ryszarda Szpotańskiego przy ul. Leśnej 8/lokal 0.3 , 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 pracę 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.

- **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://www.biznes.gov.pl/pl/opisy-procedur/-/proc/889

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.

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;***

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).

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.

(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk ✚, który pojawi się po prawej stronie)

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)

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
☐ Klienci (obecni i potencjalni)
☐ Klienci podmiotów publicznych
☐ Pacjenci
☐ Dzieci

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)

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:

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