ZARZĄDZENIE NR 4/2024

Dyrektora Miejskiego Ośrodka Kultury w Sulejowie
z dnia 04 stycznia 2024 roku
w sprawie wprowadzenia dokumentacji ochrony danych osobowych w Miejskim Ośrodku Kultury w Sulejowie

Na podstawie art. 24 ust. 1 i 2 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 (Dz. Urz. UE.L 2016 Nr 119, s. 1) zarządzam, co następuje:

§ 1. Wprowadza się do użytku służbowego dokumentację ochrony danych osobowych.

§ 2. Dokumentacja o której mowa §1. składa się z:

1) Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji wraz z załącznikami, stanowiącej Załącznik nr 1 do niniejszego Zarządzenia,
2) Instrukcji Zarządzania Systemem Informatycznym, stanowiącej Załącznik nr 2 do niniejszego Zarządzenia.

§ 3. Zobowiązuje się wszystkich pracowników do zapoznania się z treścią Zarządzenia.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1

Do Zarządzenia nr 4/2024 Dyrektora Miejskiego Ośrodka Kultury w Sulejowie z dnia 04.01.2024 r. w sprawie wprowadzenia dokumentacji ochrony danych osobowych w Miejskim Ośrodku Kultury w Sulejowie

POLITYKA OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA INFORMACJI

Miejski Ośrodek Kultury w Sulejowie

ul. Rynek 1

97-330 Sulejów

Sulejów, dnia 04 stycznia 2024 r.

SPIS TREŚCI

ZAKRES I PODSTAWA STOSOWANIA

Niniejszy dokument zatytułowany „Polityka Ochrony Danych Osobowych i Bezpieczeństwa Informacji” (dalej: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych i bezpieczeństwa informacji w Miejskim Ośrodku Kultury w Sulejowie (dalej: MOK) będący administratorem danych osobowych (dalej: Administrator).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (EU) 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) (Dz. Urz. UE.L 2016 Nr 119, s.1).

Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie procesy i czynności przetwarzania danych zarówno w formie elektronicznej jak i papierowej w celu zapewnienia ich poufności, dostępności, integralności oraz rozliczalności, poprzez wdrożenie niezbędnych do tego celu środków technicznych i organizacyjnych.

Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników MOK oraz inne osoby mające dostęp do danych, wykonujące zadania na rzecz Administratora.

ZAWARTOŚĆ

Polityka zawiera:
1) opis zasad ochrony danych osobowych i bezpieczeństwa informacji;
2) załączniki uszczegóławiające.

ODPOWIEDZIALNOŚĆ

1. Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest dyrektor MOK.
2. Odpowiedzialnymi za nadzór i monitorowanie przestrzegania Polityki jest Inspektor Ochrony Danych oraz Administrator.
3. Odpowiedzialnymi za stosowanie niniejszej Polityki są wszyscy pracownicy i współpracownicy Administratora w zakresie powierzonych im obowiązków, uprawnień, odpowiedzialności, upoważnień i pełnomocnictw.
4. Administrator zapewnia zgodność postępowania kontrahentów Administratora z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Administratora. Zasady powierzenia procesu przetwarzania danych osobowych opisuje osobny rozdział niniejszej Polityki.

SKRÓTY I DEFINICJE

§ 1. Ilekroć w Polityce Ochrony Danych Osobowych i Bezpieczeństwa Informacji oraz w załącznikach do tej polityki jest mowa o:

1) **Polityce** oznacza niniejszą Politykę Ochrony Danych Osobowych i Bezpieczeństwa Informacji, o ile co innego nie wynika wyraźnie z kontekstu;
2) **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (EU) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem

danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1);

3) **UODO** oznacza ustawę o ochronie danych osobowych z 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781);
4) **danych** oznacza dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;
5) **danych szczególnej kategorii** oznacza dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
6) **danych karnych** oznacza dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;
7) **osobie** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
8) **Administratorze, Administratorze danych osobowych, MOK** oznacza Miejski Ośrodek Kultury w Sulejowie, które samodzielnie lub wspólnie z innymi administratorami ustala cele i sposoby przetwarzania danych osobowych;
9) **Inspektorze Ochrony Danych** lub **IOD** oznacza osobę, która została powołana przez Administratora do wykonywania zadań określonych w art. 39 RODO.
10) **podmiocie przetwarzającym** lub **procesorze** oznacza podmiot, organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych;
11) **profilowaniu** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
12) **eksporcie danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
13) **RDCP** lub **Rejestrze** oznacza Rejestr Czynności Przetwarzania Danych Osobowych;
14) **organie nadzorczym** oznacza Prezesa Urzędu Ochrony Danych Osobowych („PUODO”).
15) **Użytkowniku** oznacza osobę, która przetwarza dane osobowe i informacje z użyciem systemu teleinformatycznego.

OCHRONA DANYCH OSOBOWYCH – ZASADY OGÓLNE

§ 2. Ochrona danych osobowych oparta jest o:

1) legalność – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
2) bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;
3) prawa jednostki – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;

4) rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki wynikające z RODO, aby w każdej chwili móc wykazać zgodność z przepisami.

§ 3. Administrator stosuje zasady ochrony danych osobowych:

1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2) rzetelnie i uczciwie (rzetelność);
3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
4) w konkretnych celach i nie „na zapas” (minimalizacja);
5) nie więcej niż potrzeba (adekwatność);
6) z dbałością o prawidłowość danych (prawidłowość);
7) nie dłużej niż potrzeba (czasowość);
8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 4. System ochrony danych osobowych składa się z następujących elementów:

1) **inwentaryzacja danych** - Administrator dokonuje identyfikacji zasobów danych osobowych, w tym:
   a) przypadków przetwarzania danych zwykłych, danych szczególnej kategorii i danych karnych,
   b) przypadków przetwarzania danych osób, których Administrator nie identyfikuje (dane niezidentyfikowane),
   c) przypadków przetwarzania danych dzieci,
   d) profilowania,
   e) współadministrowania danymi;
2) **rejestr -** Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych oraz gdy ma to zastosowanie Rejestr Kategorii Czynności Przetwarzania. Rejestry są narzędziem rozliczania zgodności ochrony danych z przepisami RODO i UODO;
3) **podstawy prawne** - Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych, w tym:
   a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora lub osoby, której dane osobowe dotyczą;
4) **obsługa praw jednostki** - Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) ***obowiązki informacyjne*** - Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków w celu spełnienia zasady rozliczalności ze stosowania przepisów RODO,
   b) ***możliwość wykonania żądań*** - Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających,
   c) ***obsługa żądań*** - Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i udokumentowane,
   d) ***zawiadamianie o naruszeniach*** - Administrator stosuje procedury pozwalające
   na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym

naruszeniem ochrony danych oraz Prezesa Urzędu Ochrony Danych Osobowych;

5) **minimalizacja** - Administrator weryfikuje zakres przetwarzanych danych (privacy by default), a w tym:
   a) dba o adekwatność danych,
   b) zarządza dostępem do danych,
   c) zarządza okresem przechowywania danych i weryfikacji dalszej ich przydatności;
6) **bezpieczeństwo** - Administrator zapewnia odpowiedni poziom bezpieczeństwa danych,
   w tym:
   a) przeprowadza analizy ryzyka dla zasobów przetwarzanych przez Administratora,
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw
      i wolności osób jest wysokie,
   c) dostosowuje środki ochrony danych do ustalonego ryzyka (plan postępowania z ryzykiem),
   d) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych w ramach zarządzania incydentami;
7) **przetwarzający** - Administrator stosuje dobór przetwarzających dane (podmiotów przetwarzających) na rzecz Administratora, którzy gwarantują odpowiedni stopień ochrony danych poprzez wdrożenie właściwych środków technicznych i organizacyjnych;
8) **eksport danych** - Administrator weryfikuje czy dane osobowe nie są przekazywane
   do państw trzecich lub do organizacji międzynarodowych oraz zapewnia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce;
9) **privacy by design** - Administrator zarządza zmianami wpływającymi na prywatność.
   W tym celu procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmian na ochronę danych osobowych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji, czy na początku nowego projektu. Każde zmiany są uzgadniane z IOD już od momentu projektowania. Zmiany podlegają analizie ryzyka w celu określenia prawdopodobieństwa wystąpienia określonego ryzyka oraz ewentualnego skutku dla ochrony danych osobowych.

INWENTARYZACJA

§ 5. Administrator inwentaryzuje i przetwarza:

1) **dane zwykłe, dane szczególnej kategorii i dane karne -** Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane zwykłe, szczególnej kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W chwili zidentyfikowania przypadku przetwarzania danych szczególnych lub danych karnych Administrator postępuje zgodnie z przyjętymi przepisami prawa zasadami

w tym zakresie lub w szczególnych przypadkach w oparciu o wyraźną zgodę osoby na przetwarzanie takich danych. Całość procesu przetwarzania opiera się o przesłanki określone w art. 6 RODO (dane zwykłe), art. 9 ust. 2 RODO (dane szczególnej kategorii) i art. 10 RODO (dane karne);

2) **dane niezidentyfikowane -** Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane. Do przetwarzania danych niezidentyfikowanych dochodzi m.in. w przypadku stosowania systemu monitoringu wizyjnego. Zasady przetwarzania danych przez system monitoringu wizyjnego określa odrębna dokumentacja wprowadzona do stosowania w MOK;
3) **profilowanie -** Administrator nie dokonuje profilowania przetwarzanych danych;
4) **współadministrowanie -** Administrator identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami. Administrator przy wsparciu IOD w porozumieniu z współadministratorem ustala podział obowiązków ze szczególnym uwzględnieniem realizacji praw przysługujących osobie, której dane dotyczą, w tym obowiązku informacyjnego według założeń art. 13 RODO oraz wskazuje się punkt kontaktowy dla osób, których dane dotyczą. Ustalenia powyższe każdorazowo mają postać zindywidualizowanej umowy w formie porozumienia pisemnego lub ogólnych warunków umowy. Do współadministrowania zachodzi przede wszystkim przy organizacji konkursów i wydarzeń, gdzie występuje więcej niż jeden organizator oraz w zakresie przetwarzania danych osobowych przy użyciu profili społecznościowych;

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

§ 6. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

§ 7. Administrator prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane.

§ 8. Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.

§ 9. W Rejestrze dla każdej czynności przetwarzania danych, którą Administrator uzna za odrębną dla potrzeb Rejestru odnotowuje co najmniej:

1) imię i nazwisko lub nazwa oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
2) cele przetwarzania;
3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 RODO akapit drugi, dokumentacja odpowiednich zabezpieczeń;
6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
7) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. RODO.

§ 10. 1. Wzór Rejestru stanowi ***Załącznik nr 1 Rejestr Czynności Przetwarzania Danych.*** Rejestr ma formę pisemną, w tym formę elektroniczną.

2. Administrator rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

§ 11. 1. Utrzymanie Rejestru powierza się IOD, który dokonuje wpisów aktualizacyjnych. Zmiany takie mogą być wymuszone w szczególności nowymi aktami prawa pociągającymi za sobą konieczność realizacji nowych zadań.
2. **Administrator oraz jego pracownicy zobowiązani są do informowania IOD o nowych czynnościach przetwarzania w celu aktualizacji Rejestru**.

§ 12. 1. Jeżeli przetwarzanie odbywa się zgodnie z art. 28 RODO, na zlecenie innego Administratora, prowadzony jest rejestr wszystkich kategorii czynności przetwarzania.
2. Wpisy w rejestrze ewidencjonuje się na rzecz każdego z administratorów zgodnie z ***Załącznikiem nr 2 Rejestr Kategorii Czynności Przetwarzania***.
3. Prowadzenie rejestru kategorii czynności powierza się IOD, który dokonuje wpisów aktualizacyjnych.
4. **Administrator i jego pracownicy zobowiązani są do informowania IOD o zleceniu przetwarzania przez innego Administratora.**

PODSTAWY PRZETWARZANIA

§ 13. Administrator przetwarza dane osobowe zgodnie z art. 6, 9 i 10 RODO.

§ 14. Administrator wdraża metody zarządzania zgodami umożliwiając rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS, itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

§ 15. Zgody stanowią część akt spraw i jako takie podlegają nadzorowi. ***Załącznik nr 3 Zgoda na przetwarzanie danych osobowych*** określa treść zgody na przetwarzanie, co pozwala na uzyskanie zgody od osoby, której dane dotyczą z zachowaniem jej obowiązkowych wg RODO cech, tj. dobrowolności, konkretności, świadomego i jednoznacznego określenia woli osoby. Wdrożone środki organizacyjne pozwalają na odwołanie zgody w dowolnym momencie.

§ 16. Z uwagi na złożony charakter działalności Administratora dopuszcza się stosowanie innych formularzy i zapisów „zgody na przetwarzanie danych”. Należy jednak w każdym uzasadnionym wypadku uzgodnić jej treść z IOD.

§ 17. Każdy pracownik Administratora przetwarzając dane osobowe ma obowiązek znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Administratora, pracownik ma obowiązek znać konkretny realizowany przetwarzaniem interes Administratora. Co do zasady przetwarzanie danych przez Administratora oparte jest o przepis prawa zarówno podczas przetwarzania danych zwykłych jak i danych szczególnej kategorii.

SPOSÓB OBSŁUGI PRAW OSÓB I OBOWIĄZKÓW INFORMACYJNYCH

§ 18. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza. Przekazywane informacje o przetwarzaniu danych osobowych napisane są jasnym i zrozumiałym językiem.

§ 19. Administrator ułatwia osobom korzystanie z praw poprzez różne działania, w tym zamieszczenie na stronie internetowej Administratora oraz w siedzibie Administratora i dokumentach, informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich u Administratora, w tym wymaganiach dotyczących identyfikacji oraz metodach kontaktu z Administratorem w tym celu.

§ 20. Osoba w celu realizacji swoich praw składa pisemny wniosek wskazując osobę, której dane dotyczą oraz żądanie zgodnie z ***Załącznikiem nr 4 Wniosek o realizację praw osób***. Każda osoba może złożyć żądanie w sposób inny niż wskazany w załączniku. Termin realizacji żądania liczony jest od momentu jego dostarczenia jeśli zawiera wszystkie potrzebne informacje w zakresie identyfikacji i przedmiotu żądania.

§ 21. W przypadku uznania żądania za nieuzasadnione lub nadmierne należy uzasadnić odmowę realizacji żądania wskazując powody przemawiające za przyjęciem takiej kwalifikacji i w formie pisemnej przekazać uzasadnienie osobie wnoszącej żądanie informując, o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

§ 22. Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, których dane dotyczą. Żądanie powinno być zrealizowane bezzwłocznie, lecz w czasie nie dłuższym niż miesiąc kalendarzowy. W przypadku wystąpienia okoliczności, na podstawie których żądanie nie jest możliwe do wykonania w ustawowym terminie, Administrator przekazuje informację osobie o przedłużeniu okresu realizacji z zastrzeżeniem, że okres ten nie będzie dłuższy łącznie niż 3 miesiące kalendarzowe.

§ 23. 1. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelnienia osób dla potrzeb realizacji praw osoby i obowiązków informacyjnych.
2. Podstawowym narzędziem identyfikacji i uwierzytelnienia jest podpis elektroniczny, profil zaufany lub wgląd do dokumentu tożsamości osoby, której dane dotyczą, a na rzecz której to osoby ma nastąpić realizacja jej praw i obowiązków informacyjnych.

3. Administrator prowadzi rejestr żądań w formie pisemnej, w tym elektronicznej zgodnie
z ***Załącznikiem nr 5 Rejestr żądań****.*
4. **Administrator i jego pracownicy zobowiązani są do informowania IOD o wystąpieniu żądania realizacji praw osoby, której dane dotyczą.**
5. Utrzymanie Rejestru żądań powierza się IOD.

§ 24. W celu realizacji praw osoby Administrator zapewnia możliwość identyfikacji danych konkretnych osób przetwarzanych przez Administratora, zintegrowanie ich, wprowadzanie
do nich zmiany i usuwanie.

OBOWIĄZKI INFORMACYJNE

§ 25. Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

§ 26. Administrator spełnia obowiązki informacyjne na żądanie niezwłocznie, a gdy ma ku temu podstawy, informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

§ 27. Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych
od tej osoby. Udostępnia się osobie treść obowiązku informacyjnego m.in. bezpośrednio
w miejscu uzyskania danych od osoby lub drogą komunikacji na odległość (np. w wiadomości e-mail, na stronie internetowej, Biuletynie Informacji Publicznej i in.).

§ 28. 1. Wzór ogólnego obowiązku informacyjnego stanowi ***Załącznik nr 6 Obowiązek informacyjny.***
2. Wzór obowiązku informacyjnego, zawierającego informacje, o których mowa w art. 13 RODO stanowi ***Załącznik nr 6a Obowiązek informacyjny zgodny z art. 13 RODO.***
2. W każdym przypadku treść obowiązków informacyjnych należy konsultować z IOD.

§ 29. 1. Administrator informuje o przetwarzaniu danych osobowych osoby, których dane pozyskał w sposób inny niż bezpośrednio od osoby, której dane dotyczą w rozsądnym terminie lecz nie dłuższym niż 30 dni.
2. Zakres informacji określa art. 14 RODO. Wzór obowiązku informacyjnego, zawierającego informacje, o których mowa w art. 14 RODO stanowi ***Załącznik nr 6b Obowiązek informacyjny zgodny z art. 14 RODO.***
3. Administrator nie informuje osoby o przetwarzaniu jej danych osobowych, jeśli osoba ta dysponuje już tymi informacjami, pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą lub dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie, w tym ustawowym obowiązkiem zachowania tajemnicy.

§ 30. Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.

§ 31. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania danych.

§ 32. Administrator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

§ 33. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby zgodnie ze wzorem określonym w ***Załączniku nr 6c Zawiadomienie osoby o naruszeniu danych osobowych.***

PRAWA OSÓB

§ 34. **Prawa osób trzecich.** Realizując prawa osób, których dane dotyczą, Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnica handlowa, dobra osobiste), Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądania.

§ 35. **Nieprzetwarzanie.** Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

§ 36. **Odmowa.** Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia i o prawach osoby z tym związanych.

§ 37. 1. **Dostęp do danych.** Na żądanie osoby dotyczące dostępu do jej danych Administrator informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących.
2. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

§ 38. **Kopie danych.** Na żądanie Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych z potwierdzeniem odbioru.

§ 39. 1. **Sprostowanie danych.** Administrator dokonuje sprostowania danych na żądanie osoby.
2. Administrator ma prawo odmówić sprostowania, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.
3. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych.

§ 40. 1. **Uzupełnienie danych.** Administrator uzupełnia i aktualizuje dane na żądanie osoby.
2. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych.
3. Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur
(np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

§ 41. 1. **Usunięcie danych** Na żądanie osoby Administrator usuwa dane, gdy:
1) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;
2) zgoda na ich przetwarzanie została cofnięta a nie ma innej podstawy prawnej przetwarzania;
3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
4) dane były przetwarzane niezgodnie z prawem;
5) konieczność usunięcia wynika z obowiązku prawnego;
6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. udział w konkursie na stronie internetowej).

2. Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą poniższe wyjątki:
1) jeżeli przetwarzanie danych jest konieczne do korzystania z prawa do wolności wypowiedzi i informacji;
2) jeżeli przetwarzanie danych jest konieczne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa;
3) jeżeli przetwarzanie danych jest konieczne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
4) jeżeli przetwarzanie danych jest istotne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
5) jeżeli przetwarzanie danych jest konieczne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
6) jeżeli przetwarzanie danych jest konieczne do ustalenia, dochodzenia lub obrony roszczeń.

3. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane o potrzebie usunięcia danych i dostępu do nich.

4. W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

§ 42. 1. **Ograniczenie przetwarzania.** Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;
2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich stosowania;
3) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

2. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
3. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
4. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

§ 43. **Przenoszenie danych.** Na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia albo wykonania umowy z nią zawartej w systemach informatycznych Administratora.

§ 44. **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane są przetwarzane przez Administratora w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

§ 45. 1. **Sprzeciw przy celach statystycznych.** Jeżeli Administrator przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania.
2. Administrator uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

§ 46. **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni taki sprzeciw i zaprzestanie takiego przetwarzania.

§ 47. **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli Administrator przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę , Administrator zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Administratora, chyba że taka automatyczna decyzja:

1) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą, a Administratorem;
2) jest wprost dozwolona przepisami prawa;
3) opiera się na wyraźnej zgodzie osoby odwołującej się.

MINIMALIZACJA

§ 48. Administrator dba o minimalizację przetwarzania danych pod kątem:

1) adekwatności danych do celów (ilość danych i zakresu przetwarzana);
2) dostępu do danych;
3) czasu przechowywania danych.

§ 49. 1. **Minimalizacja zakresu.** Administrator weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach RODO.

2. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania, w szczególności w momencie zmian przepisów.

3. Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

§ 50. 1. **Minimalizacja dostępu.** Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresu upoważnień), fizyczne (zamykanie pomieszczeń) i logiczne ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe.

2. Administrator stosuje kontrolę dostępu fizycznego, m.in. poprzez ograniczenie dostępu
do konkretnych pomieszczeń czy archiwum zakładowego.

3. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających w oparciu o wydane upoważnienia do przetwarzania danych oraz ewidencję osób upoważnionych do przetwarzania danych. Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich.

4. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach zgodnie z ***Załącznikiem nr 7 Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji*** oraz powiązanych z nimi załącznikami.

5. Szczegółowe zasady przetwarzania informacji w systemie informatycznym zawarte są w ***Instrukcji Zarządzania Systemem Informatycznym.***

§ 51. 1. **Minimalizacja czasu.** Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

2. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane
z systemów informatycznych Administratora, jak też z akt podręcznych i głównych.

3. Dane takie mogą być archiwizowane oraz znajdować się w kopiach zapasowych systemów
i informacji przetwarzanych przez Administratora.
4. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystywania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

BEZPIECZEŃSTWO

§ 52. 1. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administratora.
2. Administrator zapewnia bezpieczeństwo przetwarzania danych osobowych w obszarach przetwarzania wdrażając ograniczenia dostępu do tych obszarów.

§ 53. 1. **Analiza ryzyka i adekwatność środków bezpieczeństwa.** Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu Administrator:
1) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie
   i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;
2) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
3) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.

2. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
3. Analiza ryzyka jest wykonywana przy udziale IOD przez dyrektora MOK.
4. Szacowanie ryzyka przeprowadzane jest z uwzględnieniem potencjalnych skutków naruszenia praw lub wolności osób, których dane osobowe są przetwarzane w ramach prowadzonej działalności.
5. Metodyka szacowania ryzyka oraz tabela ryzyka opisana jest w ***Załączniku nr 8 Analiza ryzyka.***
6. Administrator wykonuje analizę ryzyka raz w roku lub częściej w przypadku zmian środowiskowych oraz organizacyjnych, które mogą mieć wpływ na wynik prawdopodobieństwa wystąpienia ryzyka naruszenia praw i wolności osób lub incydentu bezpieczeństwa informacji.

§ 54. 1. **Ocena skutków dla ochrony danych.** Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie
z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
2. Administrator przeprowadza ocenę skutków planowanych operacji przetwarzania niezależnie od wyników analizy ryzyka jeśli:
1) proces przetwarzania danych opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej;

2) proces przetwarzania danych odnosi się do przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych karnych;
3) proces przetwarzania danych odbywa się z wykorzystaniem systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

3. Administrator stosuje metodykę oceny skutków dla ochrony danych przyjętą w ***Załączniku nr 9 Ocena skutków dla ochrony danych*** i z wykorzystaniem tego załącznika dokumentuje przeprowadzenie oceny skutków.

4. Ocena skutków przetwarzania danych jest wykonywana przy udziale Administratora i IOD. 5. Ocena uwzględnia kryteria bezpieczeństwa, których nieosiągnięcie może spowodować naruszenie praw i wolności osoby, której dane są przetwarzane. Do tych kryteriów należą: poufność (P), integralność (I) i rozliczalność (R) przetwarzania danych.

6. Wskazanie skutków przetwarzania danych w każdym z kryteriów konkretnych zagrożeń
w liczbie od 0 do 4 daje poziom szacowany na wartość 1, kolejno
w liczbie od 5 do 8 daje wartość 2 i w liczbie od 9 do 12 daje wartość 3.

Po oszacowaniu wartości (P), (I), (R) Administrator mnożąc je przez siebie otrzymuje skalę powagi ryzyka, gdzie:
1) wartość od 1 do 3 oznacza ***niską powagę***;
2) wartość od 4 do 8 oznacza ***średnią powagę***;
3) wartość od 9 do 18 oznacza ***wysoką powagę***.

7. Stwierdzenie ***niskiej powagi*** określa wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka.

8. Stwierdzenie ***średniej powagi*** określa wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka oraz działanie obniżające przynajmniej jedną z maksymalnych wartości (P), (I), (R).

9. Stwierdzenie ***wysokiej powagi*** określa wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka, ewentualnie jeśli to możliwe zaniechanie przetwarzania danych i/lub delegację skutków ryzyka na stronę trzecią (np. ubezpieczenie) oraz działania obniżające maksymalne wartości (P), (I), (R).

10. Administrator po ustaleniu planu reakcji na ryzyko wyznacza metodę monitorowania bieżącego poziomu ryzyka, np. poprzez przegląd zdarzeń o charakterze incydentów bezpieczeństwa.

11. Jeżeli ocena skutków wskaże, że przetwarzanie powodowałoby wysokie ryzyko (powaga ryzyka liczona w wartości 27), gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka (ryzyko szczątkowe), to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym na zasadach określonych w art. 36 RODO.

§ 55. 1. **Środki bezpieczeństwa.** Administrator stosuje środki bezpieczeństwa ustalone
w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz oceny skutków dla ochrony danych.

2. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa i są bliżej opisane w procedurach przyjętych przez Administratora dla tych obszarów.

§ 56. 1. **Audyt systemu ochrony danych osobowych i bezpieczeństwa informacji.** Zgodnie z art. 32 RODO Administrator ocenia skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania poprzez

wykonywanie planowych audytów zgodności przetwarzania danych osobowych i bezpieczeństwa informacji z przepisami.
2. Audyty są wykonywane przez IOD, podmiot zewnętrzny lub zespół powołany przez Administratora w obszarach, w których występują wątpliwości co do skuteczności ochrony danych lub bezpieczeństwa informacji.
3. Ogólny zakres obszarów podlegających sprawdzeniu w zakresie ochrony danych osobowych zawarty jest w ***Załączniku nr 10 Audyt systemu ochrony danych osobowych***.

§ 57. 1. **Zgłaszanie naruszeń.** Administrator stosuje zapisy art. 33 i 34 RODO w identyfikacji, ocenie i zgłoszeniu zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia oraz powiadomienia osób, których dotyczyło naruszenie ochrony danych.
2. Administrator w celu wypełnienia obowiązków spoczywających na administratorze wprowadza instrukcję postępowania w przypadku wystąpienia naruszenia danych osobowych jako ***Załącznik nr 11 Instrukcja postępowania przy naruszeniu ochrony danych osobowych i bezpieczeństwa informacji*** do niniejszej Polityki.
3. W celu udokumentowania nadzoru nad zgłaszaniem naruszeń ochrony danych osobowych Administrator stosuje ***Załącznik nr 11a Rejestr naruszeń bezpieczeństwa danych osobowych*** oraz ***Załącznik nr 11b Protokół stwierdzenia naruszenia ochrony danych osobowych***.
4. Zgłoszenie naruszenia do PUODO odbywa się poprzez interaktywny formularz dostępny
na oficjalnej stronie organu nadzorczego www.uodo.gov.pl.
5. Zgłoszenie incydentu bezpieczeństwa informacji realizowane jest z wykorzystaniem formularza na stronie www.incydent.cert.pl.

PRZETWARZAJĄCY

§ 58. 1. Administrator posiada zasady doboru i weryfikacji przetwarzających dane osobowe
na rzecz Administratora, opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze.
2. Administrator weryfikuje podmioty przetwarzające przy użyciu arkusza zgodnie z ***Załącznikiem nr 12 Weryfikacja podmiotu przetwarzającego.***

§ 59. 1. Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych określone w ***Załączniku nr 13 Wzór umowy powierzenia przetwarzania danych osobowych***.
2. Administrator może po weryfikacji przyjąć wzór umowy powierzenia zaproponowany przez podmiot przetwarzający, jeśli wzór spełnia wymagania określone w art. 28 RODO.

§ 60. 1. Proces do realizacji i nadzoru procesu powierzenia spoczywa na Administratorze.
2. Zawarcie umowy odbywa się po konsultacji z IOD.
3. Administrator wspólnie z Inspektorem przygotowują treść umowy powierzenia przetwarzania danych.

§ 61. 1.Administrator może zlecić IOD przeprowadzenie weryfikacji wykonywania umowy powierzenia przez podmiot przetwarzający.
2. Administrator rozlicza przetwarzających z wykorzystania powierzonych danych, jak też
z innych wymagań wynikających z zasad umowy powierzenia danych osobowych.

EKSPORT DANYCH

§ 62. 1. Administrator rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.
2. Jeśli jest to zasadne, Administrator pobiera od osób, których dane dotyczą zgodę na eksport danych poza Europejski Obszar Gospodarczy.
3. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku
z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Administrator okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodnie z prawem ochrony danych rozwiązania równoważne.

PROJEKTOWANIE PRYWATNOŚCI

§ 63. Administrator zarządza zmianą mającą wpływ na prywatność w taki sposób, ab umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez Administratora odwołują się do zasady bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

SPIS ZAŁĄCZNIKÓW

Załącznik nr 1	Rejestr Czynności Przetwarzania Danych
Załącznik nr 2	Rejestr Kategorii Czynności Przetwarzania
Załącznik nr 3	Zgoda na przetwarzanie danych osobowych
Załącznik nr 4	Wniosek o realizację praw osób
Załącznik nr 5	Rejestr żądań
Załącznik nr 6	Obowiązek informacyjny
Załącznik nr 6a	Obowiązek informacyjny zgodny z art. 13 RODO
Załącznik nr 6b	Obowiązek informacyjny zgodny z art. 14 RODO
Załącznik nr 6c	Zawiadomienie osoby o naruszeniu danych osobowych
Załącznik nr 7	Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji
Załącznik nr 7a	Upoważnienie do przetwarzania danych osobowych
Załącznik nr 7b	Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 7c	Klauzula poufności
Załącznik nr 7d	Opis technicznych i organizacyjnych środków bezpieczeństwa
Załącznik nr 8	Analiza ryzyka
Załącznik nr 9	Ocena skutków dla ochrony danych

Załącznik nr 10	Audyt systemu ochrony danych osobowych
Załącznik nr 11	Instrukcja postępowania przy incydentach i naruszeniach
Załącznik nr 11a	Rejestr naruszeń bezpieczeństwa danych osobowych
Załącznik nr 11b	Protokół stwierdzenia naruszenia ochrony danych osobowych
Załącznik nr 11c	Plan ciągłości działania
Załącznik nr 12	Weryfikacja podmiotu przetwarzającego
Załącznik nr 13	Wzór umowy powierzenia przetwarzania danych

Załącznik nr 2
do Polityki Ochrony Danych
Osobowych i Bezpieczeństwa
Informacji

Rejestr Kategorii Czynności Przetwarzania

Rejestr kategorii czynności przetwarzania

Nazwa i dane kontaktowe administratora
Nazwa Miejski Ośrodek Kultury w Sulejowie
Adres ul. Rynek 1, 97 - 330 Sulejów
Email mok@sulejow.pl
Telefon 513 006 574

Inspektor Ochrony Danych
Nazwa Aleksandra Stańczyk
Adres -
Email kontakt@wbsystem.pl
Telefon 730-220-784

***Kolorem niebieskim oznaczono informacje wymagane w rejestrze przez art. 30 ust. 2 RODO**

	1	2	3	4	5	6	7
LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator			Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)		
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a			Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c

Załącznik nr 3

do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Zgoda na przetwarzanie danych osobowych

Sulejów , dn. ……

……
Imię i nazwisko

……
Adres zamieszkania

Ja, niżej podpisana/-y zostałam/-em poinformowana/-y o przysługującym mi prawie cofnięcia niniejszej zgody
w dowolnym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Aby wycofanie zgody było tak łatwe jak jej wyrażenie Administrator zapewnia mi dostęp w swojej siedzibie do niniejszego formularza i umożliwia złożenie podpisu pod klauzulą „Cofam zgodę na przetwarzanie danych".
Wyrażam dobrowolnie i świadomie zgodę na przetwarzanie danych osobowych przez Administratora danych osobowych – Miejski Ośrodek Kultury w Sulejowie w celu:

……

……
poniżej wymienionych moich danych osobowych:

……

……
i poświadczam ten fakt własnoręcznym podpisem pod klauzulą „Wyrażam zgodę na przetwarzanie danych".

Oświadczam, że udostępniono mi informacje o przetwarzaniu moich danych osobowych przez Administratora zgodnie z wymogiem wskazanym w art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych
i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie
o ochronie danych) (Dz. Urząd. Unii Europ. z dnia 04.05.2016 r. L 119/1).

Wyrażam zgodę na przetwarzanie danych

……..
Data i własnoręczny podpis

Cofam zgodę na przetwarzanie danych

……
Data i własnoręczny podpis

Obowiązek informacyjny (zgoda)

Wypełniając obowiązek prawny uregulowany zapisami art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urząd. Unii Europ. z dnia 04.05.2016 r. L 119/1) (dalej jako „RODO"), informujemy, że:

1. Administratorem danych osobowych jest Miejski Ośrodek Kultury w Sulejowie (dalej jako „Administrator"). Dane kontaktowe Administratora:
   a) adres: ul. Rynek 1, 97-330 Sulejów
   b) telefon: 513-006-574
   c) e-mail: mok@sulejow.pl
2. Kontakt z Inspektorem Ochrony Danych, e-mail: kontakt@wbsystem.pl
3. Pani/Pana dane osobowe przetwarzane są w celu określonym w zgodzie.
4. Podstawą prawną przetwarzania Pani/Pana danych osobowych jest dobrowolnie wyrażona zgoda w myśl art. 6 ust. 1 lit. a RODO.
5. Podanie danych osobowych jest dobrowolne ale konieczne do realizacji celu.
6. Administrator udostępni Pani/Pana dane osobowe, jeśli będzie się to wiązało z realizacją uprawnienia bądź obowiązku wynikającego z przepisu prawa. Należy podkreślić, że Administrator może też powierzać przetwarzanie danych osobowych lub udostępniać dane osobowe określonej grupie podwykonawców, świadczących usługi wspomagające w zakresie *infrastruktury technicznej (systemy informatyczne lokalne i w chmurze obliczeniowej), usług pocztowych (kanał tradycyjny - papierowy i hosting poczty elektronicznej), bankowości elektronicznej i in.*
7. Pani/Pana dane osobowe będą przetwarzane przez okres realizacji celu lub do wycofania zgody na przetwarzanie danych osobowych.
8. Przysługuje Pani/Panu prawo:
   a. dostępu do treści swoich danych osobowych, żądania ich sprostowania lub usunięcia, na zasadach określonych w art. 15 – 17 RODO;
   b. ograniczenia przetwarzania, w przypadkach określonych w art. 18 RODO;
   c. wycofania zgody na przetwarzanie danych osobowych, przy czym wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem;
   d. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa).

   W celu skorzystania z praw, o których mowa w pkt 8 ppkt a) - c) należy skontaktować się z Administratorem lub Inspektorem Ochrony Danych, korzystając ze wskazanych wyżej danych kontaktowych.
9. W trakcie przetwarzania danych osobowych nie dochodzi do wyłącznie zautomatyzowanego podejmowania decyzji ani do profilowania, o których mowa w art. 22 ust. 1 i 4 RODO. Oznacza to, że żadne decyzje dotyczące osób, których dane dotyczą nie będą zapadać wyłącznie automatycznie oraz nie stosuje się ich profilowania. Administrator nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Załącznik nr 4
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Wniosek o realizację praw osób

Dane osoby wnioskującej:

Miejski Ośrodek Kultury
w Sulejowie
ul. Rynek 1,
97-330 Sulejów

.....
(imię i nazwisko)

.....
(adres zamieszkania)

Dane osoby, której dane dotyczą
(jeżeli inne niż wnioskodawcy):

.....
(imię i nazwisko)

.....
(adres zamieszkania)

Niniejszym wnioskiem, wyrażam chęć skorzystania z przewidzianego przepisami Rozporządzenia UE 2016/679 (RODO):

***zaznaczyć właściwe**

☐ Prawa dostępu do informacji o przetwarzaniu danych, wynikającego z art. 15 RODO.

☐ Prawa do uzyskania kopii danych, wynikającego z art. 15 ust. 3 RODO.
Proszę wybrać format danych*****: odt, ods, xls, doc, pdf, csv lub forma tradycyjna – papierowa.

☐ Prawa do sprostowania danych, wynikającego z art. 16 RODO.
Proszę podać dane do aktualizacji w uwagach: (np. dane kontaktowe, nazwisko, itp.).

☐ Prawa do usunięcia danych, wynikającego z art. 17 RODO.

☐ Prawa do ograniczenia przetwarzania, wynikającego z art. 18 RODO.
Proszę podać powód ograniczenia przetwarzania w uwagach.

☐ Prawa do przenoszenia danych, wynikającego z art. 20 RODO.

☐ Prawa sprzeciwu, wynikającego z art. 21 RODO.
Proszę podać powód sprzeciwu w uwagach.

☐ Prawa o niepodleganiu z art. 22 RODO zautomatyzowanemu przetwarzaniu danych, w tym profilowaniu.

UWAGI (uszczegółowienie, tj. zakres lub kategorie danych, odbiorcy danych, inne):

……

……

Tożsamość osoby potwierdzono na podstawie dokumentu:

dowód osobisty / prawo jazdy / paszport / inny (jaki?)
…….. *

……
Data i podpis osoby przyjmującej wniosek

……..
Data i podpis osoby wnioskującej

Załącznik nr 5
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Rejestr żądań

Rejestr żądań i wniosków o realizację praw osób, których dane dotyczą						
NAZWA ADMINISTRATORA			Miejski Ośrodek Kultury w Sulejowie			
INSPEKTOR OCHRONY DANYCH			Aleksandra Stańczyk			
Lp.	**Data przyjęcia wniosku/żądania**	**Imię i nazwisko osoby wnioskującej**	**Imię i nazwisko osoby, której dane dotyczą (jeśli inne niż osoby wnioskującej)**	**Podstawa prawna żądania (art.15-22 RODO)**	**UWAGI**	**Termin oraz sposób realizacji**
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Załącznik nr 6
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

OBOWIĄZEK INFORMACYJNY
O PRZETWARZANIU DANYCH OSOBOWYCH

Zgodnie z art. 13 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 przekazujemy Państwu ogólne informacje dotyczące procesów przetwarzania danych osobowych w **Miejskim Ośrodku Kultury w Sulejowie.**

Kto jest administratorem danych osobowych?
Administratorem danych osobowych jest Miejski Ośrodek Kultury w Sulejowie (dalej jako „Administrator", „MOK"). Dane kontaktowe Administratora: adres: ul. Rynek 1, 97-330 Sulejów, telefon: **513-006-574,** e-mail: biuromok@sulejow.pl, mok@sulejow.pl
Czy w Miejskim Ośrodku Kultury wyznaczono Inspektora Ochrony Danych?
z dnia
z dnia Tak. Zadania Inspektora Ochrony Danych w placówce realizuje Pani **Aleksandra Stańczyk**, z którą można się skontaktować za pomocą poczty elektronicznej: kontakt@wbsystem.pl
z dnia
Na jakich podstawach prawnych przetwarzamy dane osobowe klientów i uczestników wydarzeń organizowanych przez Miejski Ośrodek Kultury?
W ramach wykonywania ustawowych obowiązków Administrator przetwarza dane osobowe klientów
i uczestników wydarzeń organizowanych przez Miejski Ośrodek Kultury na podstawie art. 6 ust. 1 lit. c) i e) RODO w ściśle określonych celach oraz zakresie, na podstawie konkretnych przepisów prawa, w szczególności ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej. Ponadto w niektórych przypadkach podstawą przetwarzania danych osobowych małoletnich, ich rodziców lub opiekunów prawnych jest zgoda, tj. art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO. Zgoda taka może dotyczyć np. przetwarzania danych osobowych w zakresie wizerunku z uwzględnieniem praw określonych w ustawie z dnia 4 lutego 1994 r. o prawach autorskich i prawie pokrewnym.

Na jakich podstawach prawnych przetwarzamy dane pracowników Miejskiego Ośrodka Kultury?
W ramach wykonywania ustawowych obowiązków nasza placówka przetwarza dane osobowe nauczycieli oraz innych pracowników na podstawie art. 6 ust. 1 lit. b) i c) RODO oraz w przypadku danych szczególnej kategorii art. 9 ust. 2 lit. b) RODO. Przetwarzanie wiąże się zatem z nawiązaniem i wykonywaniem umowy o pracę, na podstawie przepisów szczególnych, regulujących zakres danych jakie w ramach stosunku pracy MOK – jako pracodawca – musi przetwarzać w celu wypełnienia obowiązków prawnych. Przepisy te znajdują się przede wszystkim w przepisach ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

Na jakich podstawach prawnych przetwarzamy dane kontrahentów?
Administrator przetwarza dane osobowe kontrahentów bądź ich reprezentantów, którzy współpracują
z placówką na podstawie najróżniejszych umów cywilnych. Podstawą pozyskania i przetwarzania przez placówkę danych osobowych kontrahentów – osób fizycznych jest art. 6 ust. 1 lit. b) RODO, w przypadku osób prawnych reprezentowanych przez pełnomocników i

reprezentantów podstawą przetwarzania danych reprezentantów będzie art. 6 ust. 1 lit. c) RODO. Dane te są przetwarzane przez MOK na potrzebę realizacji umowy, ale również po zakończeniu okresu współpracy, ponieważ szereg przepisów szczególnych takich jak ustawa o rachunkowości i ustawy podatkowe zobowiązują placówkę do przetwarzania tych danych również po wygaśnięciu stosunku prawnego wynikającego z umowy.

W jakim celu placówka przetwarza dane osobowe?
Celem przetwarzania przez MOK jest pozyskiwanie i przygotowanie społeczności do aktywnego uczestnictwa w kulturze oraz jej współtworzenie a także promowanie działań Administratora na portalach społecznościowych i stornie internetowej placówki. Ponadto celem przetwarzania przez placówkę danych osobowych pracowników jest prawidłowa realizacja umów o pracę. W przypadku danych osobowych kontrahentów placówka przetwarza je dla prawidłowej realizacji i rozliczenia umowy.

Kiedy istnieje obowiązek podania danych?
W przypadku wyrażenia zgody, podanie danych osobowych nie jest obowiązkowe. Należy zaznaczyć, że wycofanie zgody nie wpływa na prawo przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. W przypadku umów, podanie danych może okazać się konieczne dla zawarcia umowy. Jeśli jednak podanie danych wynika z przepisów prawa, to jest ono obligatoryjne, a niepodanie danych może wiązać się z konsekwencjami takimi jak np. brak możliwości świadczenia usług realizowanych przez MOK.

Komu będziemy udostępniać przedmiotowe dane?
Placówka udostępni dane osobowe, jeśli będzie się to wiązało z realizacją uprawnienia bądź obowiązku wynikającego z przepisu prawa. Należy podkreślić, że MOK może też powierzać przetwarzanie danych osobowych określonej grupie podwykonawców, świadczących usługi wspomagające w zakresie infrastruktury technicznej (systemy informatyczne lokalne i w chmurze obliczeniowej), usług pocztowych (kanał tradycyjny - papierowy i hosting poczty elektronicznej), bankowości elektronicznej i in. Placówka nie przekazuje danych osobowych do państw trzecich i organizacji międzynarodowych, chyba że pozyska na to odpowiednią zgodę. Dane osobowe nie będą podlegać profilowaniu ani zautomatyzowanemu podejmowaniu decyzji.

Jak długo placówka przetwarza dane osobowe?
W zależności od podstawy prawnej przetwarzania, dane osobowe mogą być przetwarzane do czasu wycofania zgody na przetwarzanie danych lub do czasu, aż ustanie okres zobowiązujący MOK do przechowywania danych w związku z odpowiednim przepisem prawa.

Jakie prawa przysługują osobom, których dane osobowe są przetwarzane?
Każdemu przysługuje prawo dostępu do swoich danych osobowych i otrzymania kopii danych osobowych podlegających przetwarzaniu; sprostowania nieprawidłowych danych; żądania usunięcia danych (prawo do bycia zapomnianym) w przypadku wystąpienia okoliczności przewidzianych w art. 17 RODO; żądania ograniczenia przetwarzania danych w przypadkach wskazanych w art. 18 RODO; wniesienia sprzeciwu wobec przetwarzania danych w przypadkach wskazanych w art. 21 RODO; przenoszenia dostarczonych danych, przetwarzanych w sposób zautomatyzowany na zasadach przewidzianych w art. 20 RODO. Aby skorzystać z przysługujących praw należy skontaktować się z Administratorem lub Inspektorem Ochrony Danych. Ponadto każdemu, kto uważa, że jego dane osobowe są przetwarzane niezgodnie z prawem, przysługuje prawo wniesienia skargi do organu nadzorczego (PUODO, ul. Stawki 2, 00-193 Warszawa).

Załącznik nr 6a
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

OBOWIĄZEK INFORMACYJNY ZGODNY Z ART. 13 RODO

d) Wypełniając obowiązek prawny uregulowany zapisami art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urząd. Unii Europ. z dnia 04.05.2016 r. L 119/1) (dalej jako RODO), informujemy, że:

2. Administratorem danych osobowych jest Miejski Ośrodek Kultury w Sulejowie (dalej jako „Administrator", „MOK"). Dane kontaktowe Administratora: adres: ul. Rynek 1, 97-330 Sulejów, telefon: 513-006-574**,** e-mail: biuromok@sulejow.pl, mok@sulejow.pl.
3. Kontakt z Inspektorem Ochrony Danych, e-mail: kontakt@wbsystem.pl
4. Dane osobowe przetwarzane są w celu …….
5. Podstawą prawną przetwarzania jest……
6. Dane kontaktowe przetwarzane są na podstawie dobrowolnie wyrażonej zgody w myśl art. 6 ust. 1 lit a RODO.
7. Podanie danych osobowych jest obowiązkowe, a ich niepodanie lub podanie niepełnych danych osobowych może utrudnić lub uniemożliwić realizację celu. Podanie danych kontaktowych jest dobrowolne jednak może przyspieszyć załatwienie sprawy.

8. Administrator udostępni Państwa dane osobowe innym odbiorcom, którzy w ramach umowy lub powierzenia przetwarzania danych wspierają Administratora od strony informatycznej, dostarczania korespondencji (operatorzy poczty tradycyjnej oraz elektronicznej), prawnej, oraz bankowości elektronicznej, ……inne…….. Poza wskazanymi Administrator udostępni Państwa dane osobowe innym odbiorcom wyłącznie na podstawie przepisów prawa, w ramach przysługującego mu uprawnienia bądź w związku z koniecznością spełnienia ciążącego na nim obowiązku prawnego.

9. Administrator przetwarza Państwa dane osobowe przez okres ……..

10. Osobie, której dane są przetwarzane przysługuje prawo:

    a. dostępu do treści swoich danych osobowych, żądania ich sprostowania lub usunięcia, na zasadach określonych w art. 15 – 17 RODO;
    b. ograniczenia przetwarzania, w przypadkach określonych w art. 18 RODO;
    c. przenoszenia danych, w przypadkach określonych w art. 20 RODO; wniesienia sprzeciwu, w przypadkach określonych w art. 21 RODO;
    d. cofnięcia zgody na przetwarzanie danych osobowych, o ile przetwarzanie odbywa się na podstawie uprzednio udzielonej zgody, wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
    e. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa)

e) W celu skorzystania z praw o których mowa w pkt 7 ppkt a) - e) należy skontaktować się z Administratorem lub Inspektorem Ochrony Danych, korzystając ze wskazanych wyżej danych kontaktowych.

11. W trakcie przetwarzania danych osobowych nie dochodzi do wyłącznie zautomatyzowanego podejmowania decyzji ani do profilowania, o których mowa w art. 22 ust. 1 i 4 RODO. Oznacza to, że żadne decyzje dotyczące osób, których dane dotyczą nie będą zapadać wyłącznie automatycznie oraz nie stosuje się ich profilowania. Administrator nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Załącznik nr 6c do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Zawiadomienie osoby o naruszeniu ochrony danych osobowych

Miejski Ośrodek Kultury w Sulejowie
Adres: ul. Rynek 1, 97-330 Sulejów
Gruszczyce 21, 98-235 Błaszki
telefon: 513-006-574
e-mail: mok@sulejow.pl

Nr sprawy:

Adresat ……..

Informacja o naruszeniu Pani danych osobowych

Szanowny Pani/e!

Informujemy, że doszło do nieumyślnego naruszenia poufności Pani/a danych osobowych w ramach …… w dniu ……. Podmiot nieuprawniony uzyskał informacje, które nie powinny się znaleźć w jego posiadaniu.

Dane osobowe

Zakres danych osobowych obejmował dane zwykłe identyfikacyjne tj. imię i nazwisko oraz ……..

Możliwe konsekwencje
Utrata poufności danych we wskazanym wyżej zakresie może spowodować wykorzystanie danych osobowych w postaci upublicznienia i udostępnienia danych osobowych, w tym w sieci Internet, innym podmiotom i osobom. Upublicznienie takie może powodować następujące konsekwencje:

- ……..
- ……..
- ……..
-

Działania podjęte przez nas
Podmiot danych, któremu nieumyślnie udostępniono dane osobowe został wezwany do niewykorzystywania tych danych w sposób niezgodny z przepisami pod rygorem konsekwencji wynikających z przepisów rozporządzenia RODO, ustawy o ochronie danych oraz Kodeksu cywilnego. W związku z naruszeniem ochrony danych osobowych szkoła podjęła działania w zakresie przestrzegania procedur przez pracowników szkoły, w tym przeprowadzenie szkoleń w zakresie przetwarzania danych osobowych. Naruszenie ochrony danych osobowych zostało zgłoszone Prezesowi Urzędu Ochrony Danych Osobowych.

Co może Pani zrobić?
Każda osoba, której dane są przetwarzane ma prawo zażądać usunięcia jej danych jeśli te są przetwarzane bez odpowiedniej podstawy prawnej.

Zalecamy wykonanie następujących czynności:

- ……...
- ……...
- ……

Więcej informacji

Więcej informacji na temat przetwarzania danych osobowych można uzyskać kontaktując się z naszym inspektorem ochrony danych, Panią Aleksandrą Stańczyk pod adresem poczty elektronicznej: kontakt@wbsystem.pl

Dokładamy wszelkiej staranności, aby Pani/a dane osobowe były przetwarzane w sposób gwarantujący ich bezpieczeństwo. Zapewniamy, że przedmiotowe zdarzenie miało charakter incydentalny i wynikło z błędu ludzkiego, które było działaniem nieumyślnym. Podjęliśmy starania, aby skutki naruszenia były jak najmniej odczuwalne dla Pani/a, niemniej za całe zdarzenie serdecznie przepraszamy.

Załącznik nr 7
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

PROCEDURY BEZPIECZEŃSTWA FIZYCZNEGO I BEZPIECZEŃSTWA ORGANIZACJI

Procedura nadawania upoważnień do przetwarzania danych i uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków związanych z przetwarzaniem danych osobowych. Upoważnienie tworzy i nadaje w imieniu Administratora danych osobowych osoba na stanowisku ds. kadr, przed przystąpieniem pracownika do wykonywania czynności służbowych, zgodnie z zakresem czynności określonym w umowie o zatrudnieniu, zawartej pomiędzy Administratorem a pracownikiem. Po podpisaniu przez pracownika upoważnienie zostaje w dokumentacji Administratora dla potwierdzenia zgodności z przepisami o ochronie danych osobowych. Fakt wydania upoważnienia odnotowuje się w ewidencji osób upoważnionych. ***Załącznik nr 7a Upoważnienie do przetwarzania danych osobowych*** określa treść upoważnienia. ***Załącznik nr 7b Ewidencja osób upoważnionych do przetwarzania danych osobowych*** określa zakres informacji ujętych w ewidencji.

2. Zakres czynności określony w umowie o pracę/umowie zlecenia lub innym instrumencie prawnym wiążącym pracownika z pracodawcą jest integralną częścią upoważnienia.

3. Zmiana zakresu czynności na danych lub zmiana stanowiska może powodować konieczność nadania nowych upoważnień. Upoważnienia mają formę pisemną, a ich wzory mogą wynikać z wdrożonych u Administratora regulacji i procedur w zakresie spełnienia dziedzinowych wymagań prawnych. Polecenie do wykonywania czynności na danych osobowych może mieć formę umowy/porozumienia z osobą lub podmiotem, w których znajdują się odpowiednie klauzule bezpieczeństwa i zobowiązanie do zachowania danych w tajemnicy.

4. Uprawnienia w systemie informatycznym, w którym przetwarza się dane osobowe nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków związanych z przetwarzaniem danych osobowych z wykorzystaniem systemów informatycznych. Uprawnienia nadawane są przez osobę wskazaną przez dyrektora Miejskiego Ośrodka Kultury w Sulejowie. Administrator dba o aktualność

uprawnień w systemie informatycznym, w tym monitoruje je, zmienia i odbiera niezwłocznie
w przypadku zmiany stanowiska lub zakończenia zatrudnienia danego pracownika. Przetwarzanie informacji w systemie informatycznym określa Instrukcja zarządzania systemem informatycznym.

5. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zostaje zapoznany z zasadami ochrony danych osobowych w zakresie informacji zawartych Instrukcji zarządzania systemem informatycznym oraz w Polityce Ochrony Danych Osobowych i Bezpieczeństwa Informacji. Pracownik po zapoznaniu się ze wskazanymi wyżej zasadami podpsuje klauzulę poufności, której wzór stanowi ***Załącznik nr 7c Klauzula poufności.***

Szkolenia w zakresie ochrony danych osobowych i bezpieczeństwa informacji

1. Inspektor Ochrony Danych przeprowadza cykliczne szkolenia z zakresu tematyki ochrony danych osobowych, przetwarzania danych osobowych w systemach informatycznych, zasadach bezpieczeństwa oraz zagrożeniach i ryzykach dla bezpieczeństwa danych, w szczególności w przypadku zmiany istotnych warunków zewnętrznych (np. zmiany przepisów) lub wewnętrznych (np. wdrażane procedury i regulaminy).

2. Szkolenia pracowników realizowane są przez Inspektora Ochrony Danych, podmioty zewnętrzne, innych pracowników Administratora.

3. Szkolenia pracowników mają formę zdalną, w siedzibie Administratora, udostępnienia nagrań, skryptów i innych materiałów szkoleniowych.

4. Dla potrzeby udokumentowania spełnienia wymagań, o których mowa w pkt. 1-3 Administrator tworzy dokumentację szkolenia, składającą się przynajmniej z zakresu oraz listy osób obecnych na szkoleniu.

Obowiązki osób upoważnionych

1. Zbierając dane osobowe od osób, których dane dotyczą osoba upoważniona spełnia obowiązek informacyjny, o którym mowa w art. 13 lub 14 RODO. Treść obowiązku informacyjnego należy skonsultować z Inspektorem Ochrony Danych.

2. W celu ograniczenia dostępu do danych osobowych osób nieuprawnionych wszystkie osoby przetwarzające dane osobowe na polecenie Administratora danych osobowych:
   1) przetwarzają dane w zakresie zadań powierzonych im do realizacji zgodnie z otrzymanymi upoważnieniami i zakresem czynności;
   2) dbają o zapewnienie poufności rozmów w taki sposób, żeby treść tych rozmów nie mogła być usłyszana przez osoby nieuprawnione;
   3) nie dopuszczają do dostępu do danych osobowych i metod ich zabezpieczania przez osoby nieuprawnione w szczególności poprzez:

a) zakrywanie treści dokumentów w taki sposób, aby osoby trzecie znajdujące się w obszarze przetwarzania nie mogły zapoznać się z ich treścią,
b) bieżącej pracy tylko z dokumentami niezbędnymi do wykonania aktualnego zadania oraz odkładania dokumentów do przeznaczonych do tego segregatorów, szaf lub szuflad po zakończeniu pracy (zasada czystego biurka),
c) uniemożliwienie odczytywania przez osoby nieuprawnione treści wyświetlanych na monitorze poprzez odpowiednie ustawienie monitora i zastosowanie wygaszacza ekranu,
d) niszczenie dokumentów, ich projektów lub kopii w przeznaczonych do tego niszczarkach,
e) nieudostępnianie dokumentów zawierających dane osobowe osobom nieuprawnionym (**również realizując obowiązek dostępu do informacji publicznej na podstawie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej**),
f) niepozostawianie bez nadzoru osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe,
g) zamykanie pomieszczeń i niepozostawianie w drzwiach klucza,
h) niezwłoczne odbieranie dokumentów po ich wydrukowaniu;

4) zapewniają bezpieczeństwo wykorzystywanych systemów informatycznych w szczególności poprzez:
a) zachowanie w poufności identyfikatorów i haseł dostępowych do systemów informatycznych, w tym nieudostępnianie tych elementów innym osobom upoważnionym i osobom nieuprawnionym, nieprzechowywanie zapisanych identyfikatorów i haseł w obszarze stanowiska pracy, niedopuszczenie do możliwości odczytania wprowadzanego do systemu hasła przez osoby nieuprawnione,
b) niewprowadzanie zmian w udostępnionych systemach informatycznych bez wiedzy osoby odpowiedzialnej za ich funkcjonowanie,
c) nieinstalowanie jakichkolwiek programów bez wiedzy Administratora,
d) nieudzielania zdalnego dostępu do systemów informatycznych osobom nieuprawnionym,
e) korzystanie wyłącznie z programów udostępnionych przez Administratora w celu realizacji zadań,
f) korzystanie wyłącznie z zaufanych serwisów internetowych służących realizacji zadań,
g) korzystanie wyłącznie z zaufanych nośników danych udostępnionych przez Administratora,
h) stosowanie się do zaleceń producentów oprogramowania i sprzętu.

Przetwarzanie danych w zbiorach nieinformatycznych

1. Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nie użytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
5. Zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione.
6. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji.

Techniczne i organizacyjne środki bezpieczeństwa

1. Administrator wdraża środki techniczne i organizacyjne dla ochrony danych osobowych i zapewnienia bezpieczeństwa informacji w sposób adekwatny do ryzyka naruszenia praw i wolności osób, w tym utraty poufności, integralności i dostępności danych i informacji.
2. Określone środki techniczne i organizacyjne mogą być rekomendowane przez IOD w zakresie jego odpowiedzialności i najlepszej wiedzy.
3. Wykaz stosowanych przez Administratora środków technicznych i organizacyjnych określa się zgodnie z ***Załącznikiem nr 7d Opis technicznych i organizacyjnych środków bezpieczeństwa.***

Załącznik nr 7a

do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

……

(Administrator danych osobowych/

pieczątka zakładu pracy)

Upoważnienie do przetwarzania danych osobowych

UPOWAŻNIENIE Nr ……..……

do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urząd. Unii Europ. z dnia 04.05.2016 r. L 119/1)

z dniem …….

upoważniam Pana/-ą

……..…….

(imię i nazwisko)

zatrudnionego/-ą w Miejskim Ośrodku Kultury w Sulejowie w celu wykonywania czynności określonych na stanowisku

…….…….

(stanowisko)

zgodnie z zakresem czynności do umowy o pracę/zlecenia.

Upoważnienie wygasa z chwilą ustania zatrudnienia na ww. stanowisku lub odwołania.

Osoba upoważniona zobowiązana jest do zachowania poufności względem danych osobowych pozyskanych w ramach realizacji zadań służbowych w trakcie i po zakończeniu umowy wiążącej Administratora danych osobowych z osobą upoważnioną.

……..……

Podpis w imieniu Administratora danych osobowych

……..……

Podpis osoby upoważnionej

Data odwołania lub wygaszenia upoważnienia ……..……..

……..……

Podpis w imieniu Administratora danych osobowych

Załącznik nr 7b
do Polityki Ochrony Danych Osobowych
i Bezpieczeństwa Informacji

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Miejskim Ośrodku Kultury w Sulejowie					
Lp.	**Imię i nazwisko**	**Stanowisko**	**Forma współpracy (umowa o pracę, umowa zlecenie, umowa o dzieło, inne)**	**Data nadania upoważnienia**	**Data odwołania lub wygaszenia upoważnienia**
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Załącznik nr 7c
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Klauzula poufności

Sulejów dn. .....

.....
(imię i nazwisko)

.....
(stanowisko)

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych,w szczególności ogólnego 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), dalej jako „RODO".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez pracodawcę zadaniach,
- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez pracodawcę,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych przez pracodawcę zadań,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Miejskim Ośrodku Kultury w Gruszczycach zasadach dotyczących przetwarzania danych osobowych, określonych w Polityce Ochrony Danych Osobowych i Bezpieczeństwa Informacji i zobowiązuję się ich przestrzegać.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez pracodawcę za naruszenie obowiązków pracowniczych w rozumieniu art. 52 §1 pkt.1 Kodeksu Pracy lub RODO.

.....
(data i podpis pracownika)

Załącznik nr 7d
do Polityki Ochrony Danych Osobowych
i Bezpieczeństwa Informacji

Opis technicznych i organizacyjnych środków bezpieczeństwa

Opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych w Miejskim Ośrodku Kultury w Sulejowie	
Środki techniczne	
Środki organizacyjne	

Załącznik nr 8 do Polityki Ochrony Osobowych i Bezpieczeństwa Informacji

Analiza ryzyka

Analiza zagrożeń i ryzyka w Miejskim Ośrodku Kultury w Sulejowie określa środki zastosowane dla zapewnienia poufności, integralności i dostępności przetwarzanych danych osobowych i bezpieczeństwa informacji. Analiza ryzyka jest kluczowym elementem procesu bezpieczeństwa teleinformatycznego. Celem analizy jest zidentyfikowanie ryzyka, czyli prawdopodobieństwa wystąpienia zagrożeń dla przetwarzanych danych osobowych, wykorzystujących podatność systemu, określenie ich wielkości i wpływ na bezpieczeństwo systemu informatycznego oraz przetwarzanych danych. Analizą objęto wszystkie zasoby ze szczególnym uwzględnieniem systemu informatycznego.

1. METODA ANALIZY RYZYKA

W celu właściwego oszacowania ryzyka wybrano metodę macierzy. Metoda ta umożliwia rzetelną analizę. W podejściu tym ryzyko szacowane jest jakościowo w oparciu o wybrany poziom wymagań bezpieczeństwa. W celu scharakteryzowania wybranego poziomu posłużono się skalą 4-ro stopniową (0,1,2,3). W rzędach macierzy ujęto zasoby podlegające ochronie i podatności na zagrożenia dla dostępności, poufności i integralności. W poszczególne komórki macierzy wpisano rezultaty skutków utraty atrybutów bezpieczeństwa informacji, podatności zasobów na zidentyfikowane zagrożenia oraz wyniki ryzyka obliczonego dla każdego zasobu.

Tabela 1. Poziomy wpływu na dostępność, integralność, poufność

0. Brak wpływu
1. Mały wpływ (naruszenie dotyczy pojedynczych danych zwykłych)
2. Krótkotrwały poważny wpływ (naruszeni dotyczy danych specjalnych lub dużej ilości danych zwykłych i może narazić administratora na odpowiedzialność administracyjną
3. Poważny wpływ (jeżeli naruszenie dotyczy dużej ilości danych specjalnych oraz naraża administratora na odpowiedzialność karną oraz może spowodować konieczność wypłaty odszkodowań.

2. Zidentyfikowanie zasobów

W trakcie procesu identyfikacji zdecydowano, że zasoby podlegające analizie zostaną pogrupowane w sposób ujęty w tabeli poniżej:

Tabela 2. Zidentyfikowane zasoby

LP	Grupa zasobów
1	Budynki
2	Dokumentacja bezpieczeństwa
3	Personel
4	Inspektor Ochrony Danych
5	Administrator Systemu Informatycznego
6	Oprogramowanie
7	Sprzęt służący do przetwarzania informacji.
8.	Strona internetowa i BIP
9.	Elektroniczne zbiory danych przetwarzane na dyskach lokalnych
10.	Elektroniczne zbiory danych przechowywane i przetwarzane zdalnie
11.	Monitoring
12.	Papierowe zbiory danych

Grupy zasobów wymienione w tabeli nr 2 obejmują całość informacji, która może być przetwarzana w jednostce oraz zasoby niezbędne do jej przetwarzania. Wydzielenie grup w takiej formie wydaje się prawidłowe do przeprowadzenia poprawnie analizy ryzyka w odniesieniu do przetwarzanych informacji.

Zidentyfikowano podatności i zagrożenia dla poszczególnych grup zasobów i odniesiono do poszczególnych atrybutów bezpieczeństwa:

1. **Dostępności** – dane są zawsze dostępne dla osób upoważnionych.
2. **Integralności** – przetwarzane dane są zawsze aktualne i kompletne.
3. **Poufności** – użytkownik ma dostęp tylko do swoich dokumentów i danych do których został upoważniony.

3. WYMOGI OGÓLNE BEZPIECZEŃSTWA

W czasie przetwarzania danych osobowych w jednostce informacje występują w postaci:

1. plików lub informacji przechowywanych na dysku twardym komputera,

2. plików lub informacji przechowywanych w pamięci operacyjnej komputera,

3. plików lub informacji zapisanych na nośnikach komputerowych,

4. plików lub informacji przechowywanych w tzw. chmurze

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierających dane osobowe wymaga:

1. zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem,

2. ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem,

3. zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego,

4. zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników,

5. zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności,

6. zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

5. Potencjalne zagrożenia i podatności.

W dalszej części analizy ryzyka przeanalizowano szczegółowo potencjalne podatności i oraz zagrożenia dla przetwarzanych danych. Każdej kategorii nadano atrybuty poufności, dostępności i integralności i pod tym kątem wykonano macierz szacowania ryzyka. Określono wpływ na możliwość naruszenia praw i wolności osób których dane dotyczą. Następnie uwzględniając prawdopodobieństwo wystąpienia obliczono wartość ryzyka.

Przyjęte kryteria przedstawiono w tabelach poniżej:

Tabela 3. Poziom prawdopodobieństwa

1. Prawie niemożliwe	1 x 100 lat
2. Mało prawdopodobne	1 x 10 lat
3. Umiarkowanie możliwe	1 x 5 lat
4. Prawdopodobne	1 x rok
5. Prawie pewne	1 x miesiąc

Tabela 4. Progi akceptowalności ryzyka

1-27	Akceptowalne
28-36	Nieakceptowalne
37-45	Krytyczne

Identyfikacja prawdopodobieństwa występowania zagrożeń dla poufności, dostępności i integralności danych osobowych w odniesieniu do praw i wolności osób, których dane dotyczą.

Zasoby	Podatności	zagrożenia	wpływ na dostępność 0-3	wpływ na integralność 0-3	wpływ na poufność 0-3	wpływ na możliwość naruszenia praw i wolności	Prawdopo-dobieństwo	ryzyko	próg ryzyka	postępowanie z ryzykiem	zabezpieczenia do wdrożenia
Budynki	Awaryjność urządzeń infrastruktury budynku	awaria urządzeń infrastruktury budynku	1	0	0	1	3	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak ciągłości dyżurów pracowników odpowiadających za kontrolę dostępu oraz poprawne funkcjonowanie budynków i ich infrastruktury	dostęp do danych osób nieuprawnionych	1	0	1	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
		zbyt późne podjęcie działań minimalizujących skutki incydentu/awarii	1	0	1	2	3	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
		kradzież wyposażenia	3	0	1	4	2	8	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zapewnienia zasilania awaryjnego	brak zasilania	1	0	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka	zapewnienie poufności, integralności i dostępności po przez

										spełnia przyjęte kryteria akceptowania ryzyka	ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Katastrofy naturalne	zniszczenie budynku lub jego części	0	3	1	4	2	8	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
		zniszczenie wyposażenia	3	1	0	4	4	16	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Publiczny charakter jednostki	wandalizm	0	1	1	2	3	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

Dokumentacja bezpieczeństwa	Brak zasad ochrony informacji dla dokumentów tradycyjnych	ujawnienie, zniszczenie lub kradzież dokumentów podlegających ochronie	1	1	1	3	3	9	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad nadzoru nad systemem informatycznym	niewłaściwie zarządzany system informatyczny	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad ochrony informacji	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	1	1	1	3	3	9	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak planów ciągłości działania dotyczących systemu informatycznego	brak możliwości odtworzenia danych, utrata danych	1	2	1	4	2	8	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
	Brak planów ciągłości działania	niedziałający system informayczny	1	0	0	1	**2**	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępnośc po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
Personel	Brak profilaktyki zdrowotnej	choroby pracowników	1	0	0	1	3	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępnośc po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Choroby i wypadki losowe	niezdolność pracownika do pracy	1	0	1	2	4	8	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępnośc po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

	Brak ustalonych zastępstw między pracownikami	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	0	1	1	2	**2**	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak ustalonych zastępstw między pracownikami odpowiedzialnymi za ochronę i poprawne funkcjonowanie budynków i infrastruktury	niewłaściwe zarzadzanie kluczami i dostępem do pomieszczeń z danymi osobowymi	2	0	0	2	1	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak ustalonych zasad zastępstw pomiędzy administratorami systemów informatycznych	błędy administratora skutkujące zagrożeniem bezpieczeństwa informacji	1	1	1	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad ochrony informacji dla dokumentów tradycyjnych	pozostawienie dokumentów bez nadzoru	1	0	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
	Brak zasad ochrony informacji	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad nadzoru nad systemem informatycznym	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	0	1	1	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Kompetencje administratorów systemu	niewłaściwie zarządzany system informatyczny	1	0	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

	Niewłaściwe zarządzanie szkoleniami	brak świadomości pracowników wynikły z niewłaściwego zarządzania szkoleniami	2	0	0	2	1	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Niewłaściwe zarządzana strona strona internetowa placówki	błędy pracowników publikujących dane na stronie internetowej	1	0	0	1	1	1	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Kompetencje pracowników, praktykantów, stażystów	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	1	0	1	2	1	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
Inspektor Ochrony Danych	Brak dostatecznych kompetencji	niewłaściwe funkcjonowanie systemu ochrony danych w placówce,	0	1	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
		brak dostatecznych środków na szkolenia	2	2	1	5	2	10	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Choroby i wypadki losowe	niezdolność pracownika do pracy, utrudniona realizacja zadań związanych z przetwarzaniem danych w jednostce w razie awarii systemu	2	3	1	6	3	18	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak ustalonych zastępstw między pracownikami	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	2	1	1	4	2	8	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

		brak kontroli i utrudniona realizacja zadań związanych z przetwarzaniem danych w jednostce	2	2	0	4	3	12	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
		niedostateczny czas na właściwe wykonywanie wszystkich obowiązków	1	2	0	3	4	12	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
		konflikt interesów w przypadku łącznia niewłaściwych stanowisk	0	1	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
Administrator Systemu Informatycznego	Brak zastępowalności	przerwy w prawidłowym funkcjonowaniu systemu	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
	Choroby i wypadki losowe	brak natychmiastowej reakcji w przypadku wystąpienia awarii	2	1	0	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępnośc po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak ustalonych zastępstw między pracownikami	brak możliwości natychmiastowej reakcji w przypadku zaistnienia incydentu	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępnośc po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak dostatecznych kompetencji	niewłaściwie zarządzany system informatyczny	1	0	0	1	0	0	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępnośc po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

	Niewłaściwie zarządzana strona internetowa placówki	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	1	0	1	2	1	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad nadzoru nad systemem informatycznym	brak lub niewłaściwie nadanie uprawnienia do systemu informatycznego	1	1	1	3	1	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak dostatecznych kompetencji	brak lub niewłaściwe nadawanie uprawnień do systemu informatycznego	1	0	1	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
		brak możliwości realizacji zadań jednostki na rzecz osób których dane dotyczą	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
Oprogramowanie	Kompetencje administratorów systemu	niewłaściwie zarządzany system informatyczny	0	1	1	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Awaryjność oprogramowania lub sprzętu służącego do zarządzania stroną internetową	awarie oprogramowania i sprzętu	1	0	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
Sprzęt służący do przetwarzania informacji.	Awaryjność urządzeń służących do przetwarzania informacji	nie działający system informatyczny	1	2	0	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

	Brak zasilania urządzeń infrastruktury informatycznej	nie działający system informatyczny	0	2	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasilania	nie działający system informatyczny	2	0	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Awaryjność sprzętu lub oprogramowania służącego do zarządzania stroną internetową	awarie oprogramowania i sprzętu	1	0	1	2	3	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad nadzoru nad systemem informatycznym	niewłaściwie zarządzany system informatyczny	2	1	1	4	2	8	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
Strona internetowa i BIP	Awaryjność sprzętu lub oprogramowania służącego do zarządzania stroną internetową	awarie oprogramowania i sprzętu koniecznego do funkcjonowania strony	1	0	2	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad publikowania informacji w BIP i na stronie internetowej	niepublikowane informacje w BIP wymagane prawem	2	0	1	3	1	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Niewłaściwie zarządzana strona internetowa placówki	brak dostępu do BIP i strony internetowej	2	0	2	4	2	8	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

Elektroniczne zbiory danych przetwarzane na dyskach lokalnych	Awaryjność urządzeń służących do przetwarzania informacji	awarie komputerów na stanowiskach pracy, awarie serwerów, utrata danych	1	3	1	5	3	15	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Awaryjność oprogramowania lub sprzętu służącego do przetwarzania danych	awarie oprogramowania lub sprzętu	0	2	1	3	3	9	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak planów ciągłości działania systemu informatycznego	brak możliwości odtworzenia danych, utrata danych	0	2	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad nadzoru nad systemem informatycznym	brak lub niewłaściwie nadanie uprawnienia do systemu informatycznego	0	1	2	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
	Brak zasad ochrony informacji	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	1	1	1	3	3	9	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasilania urządzeń infrastruktury informatycznej	nie działający system informatyczny, utrata danych	0	1	0	1	3	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Wartość zasobów informatycznych	cyberprzestępczość	0	1	2	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Kompetencje administratorów systemu	niewłaściwie zarządzany system informatyczny	0	1	1	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom	zapewnienie poufności, integralności i dostępności

										ryzyka spełnia przyjęte kryteria akceptowania ryzyka	po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
Elektroniczne zbiory danych przechowywane i przetwarzane zdalnie	Awaryjność urządzeń służących do przetwarzania informacji	awarie komputerów, awarie serwerów	2	0	3	5	3	15	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Awaryjność sprzętu lub oprogramowania służącego do zarządzania stroną internetową	awarie oprogramowania i sprzętu	0	0	1	1	3	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak planów ciągłości działania systemu informatycznego	brak znajomości zasad postępowania w przypadku wystąpienia zdarzeń niebezpiecznych	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

	Brak ustalonych zasad zastępstw pomiędzy administratorami systemów informatycznych	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	1	0	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad nadzoru nad systemem informatycznym	niewłaściwie zarządzany system informatyczny	2	0	2	4	1	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad ochrony informacji	brak zabezpieczenia systemu informatycznego	0	1	0	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak zasad nadzoru nad systemem informatycznym	utrata danych	0	2	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
	Brak zasilania urządzeń infrastruktury informatycznej	nie działający system informatyczny	0	1	0	1	3	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Kompetencje administratorów systemu	niewłaściwie zarządzany system informatyczny	1	1	1	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Wartość zasobów informatycznych	cyberprzestępczość	3	2	1	6	2	12	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

Monitoring	Niewłaściwe zabezpieczenie pomieszczeń przed nieuprawnionym dostępem	nieuprawniony dostęp do urządzeń rejestrujących, zniszczenie nagrań	3	0	0	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Przerwy w zasilaniu	brak rejestracji obrazu	1	0	1	2	3	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak spójności z przepisami prawa dotyczących monitoringu	nieuprawnione stosowanie monitoringu, nieuprawnione przetwarzanie wizerunku osób postronnych	0	2	1	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Niewłaściwe zabezpieczenie nagrań	nieuprawnione, nielegalne udostępnienie nagrań	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
	Brak regulacji organizacyjnych i odpowiednich procedur	nieupowazniony dostęp osób do pomieszczeń, rejestratora i nagrań, nieuprawnione ujawnianie nagrań z monitoringu	1	1	0	2	2	4	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Awaryjność urządzeń służących do rejestracji obrazu	awarie sprzętowe, utrata brak nagrania	0	1	0	1	3	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
Papierowe zbiory danych	Brak zabezpieczeń dla dokumentów tradycyjnych	ujawnienie, zniszczenie lub kradzież dokumentów podlegających ochronie	2	1	1	4	3	12	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

	Katastrofy naturalne.	zniszczenie dokumentów papierowych	3	3	0	6	2	12	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Kompetencje pracowników, praktykantów, stażystów	błędy ludzkie skutkujące zagrożeniem bezpieczeństwa informacji	0	0	1	1	2	2	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Publiczny charakter jednostki.	kradzież wyposażenia, zniszczenie	2	1	0	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur
	Brak wyposażenia pomieszczeń w odpowiedni sprzęt do przechowywania dokumentów	dostęp do dokumentów osób nieupoważnionych, kradzież, zniszczenie	3	0	0	3	2	6	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie

										akceptowania ryzyka	przyjętych procedur
	Wrażliwość na wilgoć	zniszczenie dokumentów papierowych	0	1	0	1	3	3	akceptowane	zachowanie (akceptacja) ryzyka - poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka	zapewnienie poufności, integralności i dostępności po przez ciągłe sprawdzanie i ulepszanie przyjętych procedur

Tabela 5. Macierz ryzyka

6. ANALIZA POWYŻSZEJ MACIERZY POZWALA NA WYCIĄGNIĘCIE NASTĘPUJĄCYCH WNIOSKÓW:

W wyniku przeprowadzonej analizy ryzyka można stwierdzić, ze **ryzyko wystąpienia zagrożeń względem poufności, dostępności i integralności jest akceptowalne.** Ryzyko zidentyfikowane na poziomie akceptowalnym pozwala uznać system bezpieczeństwa danych osobowych i informacji jako bezpieczny i gwarantujący adekwatną do ryzyka ochronę.

Ocena skutków dla ochrony danych

Ocena skutków przetwarzania danych – DPIA Miejski Ośrodek Kultury w Sulejowie	
Data wykonania oceny	
Czynność przetwarzania zgodnie z RCPD	
Osoby zaangażowane w przetwarzanie	
Kategoria przetwarzanych danych	
Cel przetwarzania danych – kontekst	
Podstawa przetwarzania danych	
Adekwatność przetwarzania danych	
Realizacja obsługi praw osób	
Stosowane środki ochronne	

Załącznik nr 10
do Polityki Ochrony Danych
Osobowych i Bezpieczeństwa Informacji

Stan na dzień
(data
wykonania
audytu)

Audyt systemu ochrony danych osobowych

Audyt systemu ochrony danych osobowych w Miejskim Ośrodku Kultury w Sulejowie

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
I.	**I. ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH**							
I.1	Polityka w zakresie ochrony DO (procedury przetwarzania DO)	[ocena obszaru]	1. Czy opracowano i wdrożono politykę ochrony danych osobowych?	[ocena wymogu]			Informacja od ADO, IOD i pracownika ds. IT. Weryfikacja polityki w zakresie bezpieczeństwa	*art. 24 i 32 RODO; mot. 26,*

			2. Czy polityka ochrony DO, procedury wewnętrzne albo powtarzalne praktyki uwzględniają najważniejsze kwestie dotyczące zabezpieczeń organizacyjnych, mających wpływ na bezpieczeństwo przetwarzanych DO? W szczególności, czy odnoszą się do: a) wykorzystania pseudonimizacji i szyfrowania DO w systemach i aplikacjach IT? b) konieczności ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania DO? c) zdolności do szybkiego przywrócenia dostępności DO i dostępu do nich w razie incydentu fizycznego lub technicznego? d) regularnego	[ocena wymogu]			i ochrony DO. Potwierdzenie istnienia procedur dot. SZBI, inna dokumentacja lub dane potwierdzające, w szczególności dokumentacja: - opisująca procedury przetwarzania danych; - wskazująca działania, jakie należy podjąć (np. nadawanie praw dostępu, monitorowanie incydentów, back up, mechanizmy kryptograficzne, testy bezpieczeństwa, audyty, kontrole itp.); - określająca zasady i reguły postępowania, jakie należy zastosować. Istniejąca dokumentacja analizy ryzyka dla ochrony DO	*28, 29, 39, 74-78, 83 i 85 preambuły;* *Rozporządzenie KRI* *Standardy KZ*

			testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?				- kwerenda wyników analizy ryzyka z ostatniego okresu z uwzględnieniem rekomendacji odnoszących się do środków technicznych i organizacyjnych, zapewniających ochronę DO. Aktualizacja procedur – ustalenie dat ostatnich przeglądów i aktualizacji procedur. Uwaga: Politykę ochrony danych osobowych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań z zakresu ochrony danych osobowych w sposób zgodny z prawem i	
			3. Czy polityka ochrony DO podlega przeglądom i jest okresowo aktualizowana?	[ocena wymogu]				

							efektywny, w szczególności zapewniający odpowiedni stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Politykę ochrony DO może stanowić: - jeden dokument/procedura określająca całościowo ukształtowany w danej jednostce system ochrony DO, lub - suma szeregu dokumentów/procedur normujących w danym obszarze kwestie przetwarzania DO (np. instrukcja kancelaryjna, procedury rozpatrywania	

							skarg i wniosków, procedury udzielania zamówień publicznych lub procedury projektowania systemów teleinformatycznych).	
I.2	Wyznaczenie ADO	[ocena obszaru]	Czy w jednostce nastąpiło powierzenie zadań ADO wyznaczonym podmiotom (osobom/stanowiskom/usługodawcom)? Czy zadania te zostały powierzone w formie pisemnej?	[ocena wymogu]			Informacja od ADO lub IOD, dokument potwierdzających wyznaczenie IOD, zakres obowiązków, opis stanowiska pracy, umowa o świadczenie usług zawarta z osobą fizyczną lub innym podmiotem. Wskazanie osób/komórek organizacyjnych/podmiotów, którym powierzono zadania ADO w procedurach ODO.	*art. 4 pkt 7 RODO*

I.3	Szkolenia pracowników	[ocena obszaru]	Czy pracownicy jednostki zostali przygotowani do realizacji obowiązków zgodnie z zasadami RODO? W szczególności, czy zorganizowano szkolenia z zakresu przepisów o ochronie DO dla osób pełniących funkcje ADO, IOD oraz pracowników uczestniczących w przetwarzaniu DO?	[ocena wymogu]			Informacja od ADO i IOD. Plan szkoleń/sprawozdania. Dokumentacja potwierdzająca przeprowadzenie szkoleń, spotkań (w tym ich zakres).	*art. 36a ust. 2 lit. c uodo; wytyczne dot. IOD*
I.4	Upoważnienie do przetwarzania DO	[ocena obszaru]	1. Czy DO są przetwarzane wyłącznie przez osoby/podmioty działające na polecenie i z upoważnienia ADO oraz wyłącznie w zakresie niezbędnym do realizacji swoich zadań?	[ocena wymogu]			Informacja od ADO. W celu weryfikacji sposobu dokumentowania wydawania upoważnień do przetwarzania można poprosić o rejestr przetwarzania oraz o zestawienie wszystkich upoważnionych osób. Należy również zwrócić uwagę na status upoważnień	*art. 32 ust. 4 RODO*
			2. Czy ADO dokumentuje proces upoważniania do przetwarzania DO w sposób, który umożliwia ustalenie wszystkich osób zaangażowanych w procesy przetwarzania DO?	[ocena wymogu]				

							wydanych przed wejściem w życie RODO. Jeżeli nie zostały odwołane i są ważne, to czy zostały uwzględnione w aktualnej dokumentacji przetwarzania oraz czy spełniają wymogi RODO (integralność i poufność przetwarzania DO). Uwaga: ADO oraz podmiot przetwarzający podejmują działania w celu zapewnienia by każdy podmiot działający z upoważnienia ADO lub podmiotu przetwarzające go, który ma dostęp do DO, przetwarzał je wyłącznie na polecenie administratora,	

							chyba, że wymaga tego od niego prawo.	
I.5	Współadministrowanie DO	[ocena obszaru]	1. Czy jednostka zidentyfikowała wszystkie procesy przetwarzania DO, które mają więcej niż jednego ADO?	[ocena wymogu]			Informacja od ADO i IOD, Rejestr czynności przetwarzania, dokumentacja z inwentaryzacji procesów etc. Uwaga: Jeśli odpowiedź na to pytanie brzmi "NIE DOTYCZY" to nie ma konieczności weryfikowania pozostałych pytań w obszarze I.5. Współadministrowanie DO	*art. 26 RODO dobra praktyka*
			2. Czy w przypadku współadministrowania, cele i sposoby przetwarzania zostały określone wspólnie przez wszystkich współadministratorów?	[ocena wymogu]			Informacja od IOD. Dokumentacja z określenia celów i sposobów przetwarzania lub regulacje	*art. 26 ust. 1 RODO; mot. 79 preambuły.*

							prawne. Analiza umów/porozumień, przepisy w aktach prawnych lub inne dokumenty potwierdzające.	
			3. Czy zakresy odpowiedzialności dotyczącej wypełniania obowiązków przez współadministratorów: - zostały określone w sposób przejrzysty oraz - należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja uzgodnień między administratorami. Analiza dokumentacji określającej zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi, np. umowy/ porozumienia zawierające kwestie związane ze współadministrowaniem. Uwaga: W szczególności należy zwrócić uwagę na zakresy odpowiedzialno	*art. 26 RODO; mot. 79 preambuły.*

							ści współadministratorów w odniesieniu do: - wykonywania praw osoby, której dane dotyczą, w tym do - obowiązków informacyjnych, o których mowa w art. 13 i 14.	
			4. Czy wskazano punkt kontaktowy dla osób, których dane dotyczą? Czy zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą?	[ocena wymogu]			Informacja od współadministratorów i IOD. Analiza treści dokumentacji związanej ze współadministrowaniem. Weryfikacja wskazania/dostępności punktu kontaktowego.	*art. 26 RODO*
I.6	Podmioty przetwarzające	[ocena obszaru]	Czy w jednostce zidentyfikowano wszystkie procesy przetwarzania DO, w których przetwarzanie jest dokonywane przez podmiot przetwarzający? Czy zidentyfikowano wszystkie podmioty przetwarzające oraz wszystkie inne	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów DO oraz analiza umów zawartych z podmiotami przetwarzającymi. Wykaz wszystkich podmiotów	*art. 28 RODO;* *mot. 81 preambuły;*

			podmioty (usługodawców) przetwarzające w ich imieniu?				przetwarzających procesy przetwarzania danych ADO. Przykłady powierzenia przetwarzania to np.: a. powierzenie archiwizacji, b. usługi serwisowe systemów IT, c. serwisowanie systemu obsługi kasy zapomogowo-pożyczkowej, d. umowy na testy penetracyjne, e. zlecenie wyrobienia pieczątek.	
I.8	Umocowanie podmiotów przetwarzających	[ocena obszaru]	Czy wszystkie podmioty przetwarzające DO (w tym inne podmioty przetwarzające, które wykonują usługi na ich rzecz) zostały upoważnione przez ADO? Czy przetwarzanie DO zostało powierzone w formie pisemnej, w tym elektronicznej	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów czynności przetwarzania DO oraz analiza umów zawartych z podmiotami przetwarzającymi. Wykaz wszystkich	*art. 28 ust. 2-4, art. 30 RODO;* *mot. 81 preambuły; Standardy KZ*

			(np. zgoda ADO, umowa albo inny akt prawny)?				podmiotów przetwarzających DO. Analiza treści zgód wydanych przez ADO, informacje od podmiotów przetwarzających oraz ewentualne sprzeciwy ADO wobec zmian w zakresie podmiotów przetwarzających.	
I.9	Nadzór nad umowami przetwarzania DO	[ocena obszaru]	1. Czy dokonano inwentaryzacji umów powierzenia DO?	[ocena wymogu]				
			2. Czy wypracowano w jednostce wzory umów albo klauzul umownych związanych ze świadczeniem usług przetwarzania DO? Czy są one prawidłowe?	[ocena wymogu]				
I.10	Umowy o przetwarzanie DO	[ocena obszaru]	1. Czy umowy dot. przetwarzania DO dookreślają zgodę albo brak zgody na korzystanie z innych podmiotów przetwarzających? (art. 28 ust. 2 i 4 RODO)	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów DO oraz analiza wybranych umów zawartych z podmiotami przetwarzającymi na podstawie doboru próby. Wykaz wszystkich podmiotów przetwarzających procesy przetwarzania	*art. 28 ust 2-4 i 9, art. 30 ust. 2 oraz art. 32-36 RODO; mot. 81 preambuły;*
			2. Czy umowy dot. przetwarzania DO (art. 28 ust. 3 RODO) określają: - przedmiot i czas trwania przetwarzania, - charakter i cel przetwarzania, - rodzaj DO oraz	[ocena wymogu]				

			kategorie osób, których dotyczą, - obowiązki i prawa ADO, - osoby odpowiedzialne i właściwe do kontaktów roboczych po stronie ADO i podmiotu przetwarzającego?				danych. Uwaga: Elementy wymienione w art. 28 RODO, które powinny się znaleźć w umowie nie tworzą zamkniętego katalogu. W każdym przypadku o tym co powinno się znaleźć w umowie a co nie jest istotne decyduje konkretny charakter przetwarzanych danych (np. dane wrażliwe) oraz sposób ich przetwarzania (np. z wykorzystaniem internetu). Podczas doboru próby umów do	
			3. Czy przetwarzanie przez podmiot przetwarzający (w tym w zakresie przekazywania ich państwu trzeciemu) zostało ograniczone do jedynie udokumentowanych poleceń administratora? (art. 28 ust. 3 RODO lit. a)	[ocena wymogu]				
			4. Czy zobowiązano podmiot przetwarzający do zachowania tajemnicy albo poinformowano go o istnieniu takiego obowiązku? (art. 28 ust. 3 RODO lit. b)	[ocena wymogu]				

			5. Czy zobowiązano podmiot przetwarzający do podjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób, których dane dotyczą, a w szczególności zapewnienie: (art. 28 ust. 3 RODO lit. c) - pseudonimizacji i szyfrowania DO, - poufności, integralności, dostępności i odporności systemów i usług przetwarzania, - zdolności szybkiego przywrócenia dostępności DO w razie incydentu fizycznego lub technicznego, - regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić	[ocena wymogu]			badania szczegółowego należy uwzględnić również umowy zawarte przed wejściem w życie RODO. Podjęcie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw i wolności osób, których dane dotyczą – dot. umów outsourcingu utrzymania infrastruktury IT. Jeśli odpowiedź na to pytanie brzmi "NIE DOTYCZY to nie ma konieczności	

			bezpieczeństwo przetwarzania?				weryfikowania pozostałych pytań w obszarze I.10. Umowy o przetwarzanie DO.	
			6. Czy zobowiązano podmiot przetwarzający do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego? (art. 28 ust. 3 RODO lit. d)	[ocena wymogu]				
			7. Czy zobowiązano podmiot przetwarzający do wspomagania ADO, w tym do zapewnienia odpowiednich środków technicznych i organizacyjnych do wywiązywania się z obowiązku odpowiadania na żądania oraz do wykonywania praw osób, których danych	[ocena wymogu]				

			dotyczą? (art. 28 ust. 3 RODO lit. e)					
			8. Czy zobowiązano podmiot przetwarzający (art. 28 ust. 3 RODO lit. f) do wspomagania ADO w wywiązywaniu się z obowiązków w zakresie zapewnienia bezpieczeństwa DO (art. 32-34 RODO) oraz oceny skutków dla ochrony danych (art. 35-36 RODO), w tym zwłaszcza z: - obowiązku prowadzenia rejestru wszystkich kategorii czynności przetwarzania DO dokonywanych w imieniu ADO (art. 30 ust. 2 RODO), - obowiązku zgłaszania naruszenia ochrony DO (art. 33 ust. 2 RODO), - obowiązku współpracy i udzielania wyjaśnień ADO?	[ocena wymogu]				

			9. Czy zobowiązano podmiot przetwarzający do usunięcia albo zwrotu wszelkich DO oraz ich istniejących kopii po zakończeniu świadczenia usług, z wyjątkiem sytuacji, gdy obowiązek ich przechowywania wynika z przepisów szczególnych? (art. 28 ust. 3 RODO lit. g)	[ocena wymogu]				
			10. Czy zobowiązano podmiot przetwarzający do udostępnienia ADO wszelkich informacji niezbędnych do wykazania obowiązków wynikających z RODO oraz do współpracy, w tym poddania się ewentualnym kontrolom, audytom oraz inspekcjom prowadzonym przez ADO albo wskazane przez niego podmioty? (art. 28 ust. 3 RODO lit. h)	[ocena wymogu]				

I.11	Przekazywanie do państwa trzeciego lub organizacji międzynarodowej	[ocena obszaru]	1. W przypadku przekazywania danych do państw trzecich lub organizacji międzynarodowych: Czy ustalono osoby odpowiedzialne za podejmowanie decyzji w tym zakresie oraz wewnętrzne procedury postępowania?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja procedur. Przegląd procesów dotyczących przetwarzania danych, które są albo będą przekazywane do państw trzecich lub organizacji międzynarodowych. Uwaga: Przekazanie DO, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej następuje tylko, gdy (z zastrzeżeniem innych przepisów RODO) ADO i podmiot przetwarzający spełnią warunki określone w art.	*art. 44-49 RODO;* *mot. 6, 101-116 preambuły.*

							44-50 RODO, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Jeśli odpowiedź na to pytanie brzmi "NIE DOTYCZY to nie ma konieczności weryfikowania pozostałych pytań w obszarze I.11. Przekazywanie do państwa trzeciego lub organizacji międzynarodowej.	

			2. W przypadku przekazywania danych do państw trzecich lub organizacji międzynarodowych: Czy przekazywanie następuje po wykazaniu przez ADO albo podmiot przetwarzający, że: a) według Komisji Europejskiej, państwo trzecie lub dana organizacja międzynarodowa zapewnia odpowiedni stopień ochrony, b) zapewniono odpowiednie zabezpieczenia (w tym reguły korporacyjne), prawa osób, których dane dotyczą oraz skuteczne środki ochrony prawnej, c) państwo członkowskie lub organ nadzorczy wydało zezwolenie na podstawie art. 26 ust. 2 dyrektywy 95/46/WE do czasu zmiany, zastąpienia lub uchylenia zezwolenia (art. 46 ust. 5 RODO), lub d) spełniono jeden z	[ocena wymogu]			Informacja od ADO i IOD. Uwaga: Zgodnie z art. 45 ust. 8 RODO Komisja publikuje w Dzienniku Urzędowym Unii Europejskiej i na swojej stronie internetowej wykaz państw trzecich, terytoriów i określonych sektorów w państwie trzecim oraz organizacji międzynarodowych, co do których przyjęła decyzję stwierdzającą odpowiedni stopień ochrony lub jego brak. Art. 46 ust. 2 RODO wymienia odpowiednie zabezpieczenia, które gwarantują	

			warunków wymienionych w art. 49 RODO (tj. wyjątek w szczególnych sytuacjach).				ochronę DO w przypadku ich przekazywania. W przypadku pozostałych zabezpieczeń konieczne jest zezwolenie PUODO (art. 46 ust. 3).	
II. PRAWO DO PRZETWARZANIA DANYCH OSOBOWYCH								
II.1	Podstawa prawna przetwarzania DO	[ocena obszaru]	Czy dla wszystkich zbiorów danych/procesów przetwarzania danych zidentyfikowano podstawę prawną (warunki przetwarzania)? Czy zostało to udokumentowane w rejestrze czynności przetwarzania DO?	[ocena wymogu]			Wywiady z IOD i pozostałymi kierownikami właściwych komórek organizacyjnych. Przegląd rejestru czynności przetwarzania DO oraz przegląd zawartych tam podstaw prawnych upoważniających do przetwarzania DO (podanie przepisu prawa, umowy lub	*Warunki przetwarzania (art. 6 RODO), szczegółowe i dodatkowe warunki przetwarzania DO (art. 8-10 RODO mot. 40-57 preambuły).*

							zgody). Porównanie rejestru z wybranymi czynnościami przetwarzania DO.	
II.2	Identyfikacja celów przetwarzania DO	[ocena obszaru]	1. Czy zidentyfikowano określone w prawie cele przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD Dokument potwierdzający identyfikację (zestawienia, rejestr czynności przetwarzania DO itp.). Przykłady procesów: ZFŚS, rekrutacja, umowy cywilnoprawne pod warunkiem, że chcemy przetwarzać dane w innym celu niż tylko zawarcie umowy.	*art. 6 ust. 3 RODO*
			2. Jeżeli cel przetwarzania DO nie został określony w prawie, to czy przetwarzanie to jest niezbędne dla realizacji interesu publicznego lub władzy publicznej?	[ocena wymogu]				
II.3	Zgoda na przetwarzanie DO	[ocena obszaru]	1. Czy zidentyfikowano DO, dla których podstawą	[ocena wymogu]			Informacja od ADO lub IOD. Dobrą praktyką jest określenie	*art. 4 pkt 11 oraz art. 7 RODO;*

			przetwarzania jest zgoda?				wzoru zgody uwzględniające go wymogi RODO. Badanie powinno w szczególności objąć sprawdzenie udzielonych zgód oraz ewentualnego wzoru zgody. Dobrą praktyką jest również sformalizowany system zarządzania zgodami na przetwarzanie danych osobowych, który umożliwia rejestrację zgody, odnalezienie informacji o zgodach udzielonych przez jedną osobę oraz ich wycofanie.	*mot. 32, 42 i 43 preambuły;*
			2. Jeżeli wyłączną podstawą przetwarzania DO jest zgoda to: a) Czy treść zgody (w szczególności ewentualnego wzoru takiej zgody) pozwala na okazanie woli przetwarzania DO w sposób: - jednoznaczny (tj. konkretnie i wyraźnie odróżniający od pozostałych kwestii), dobrowolny (tj. bez uzależniania zgody od świadczenia usług niepowiązanych z przetwarzaniem danych), - zrozumiały (tj. w łatwo dostępnej formie, sformułowanie jasnym i prostym językiem, bez nieuczciwych warunków), - świadomy (tj. upewnieniem się co do tożsamości ADO oraz zamierzonych celów przetwarzania DO)?	[ocena wymogu]				

			b) Czy na wszystkie cele przetwarzania DO uzyskano zgodę osoby, której dane dotyczą? c) Czy poinformowano o prawie do wycofania zgody w dowolnym momencie? d) Czy wykazano (udokumentowano) wyrażenie zgody? e) Czy przewidziano tryb postępowania z DO dotyczącymi dzieci?					
			3. Czy istnieje system rejestrowania i zarządzania bieżącą zgodą na przetwarzanie DO?	[ocena wymogu]				
II.4	Spełnienie warunków przetwarzania DO	[ocena obszaru]	Czy dla wybranych procesów przetwarzania DO: a) spełnione zostały warunki przetwarzania, określone w podstawie prawnej przetwarzania, zawartej w rejestrze czynności? b) cele przetwarzania są zgodne z celami, w jakich zostały zebrane?	[ocena wymogu]			Ocena na podstawie wybranych procesów przetwarzania DO.	*art. 5, 6 i 11 RODO;* *mot. 39-48 oraz 50 preambuły.*

			c) dane są przetwarzane w sposób adekwatny, tj. wyłącznie w zakresie niezbędnym do realizacji celów ich przetwarzania? d) dane są przetwarzane w formie umożliwiającej identyfikację osoby, której dane dotyczą?					
II.5	Zaprzestanie przetwarzania DO	[ocena obszaru]	Czy zaprzestano przetwarzania DO niezwłocznie po stwierdzeniu: - braku podstaw do ich przetwarzania? - niezgodności celów przetwarzania DO z celami, w którym zostały zebrane?	[ocena wymogu]			Badanie wybranych przypadków po stwierdzeniu, że brak jest podstaw do dalszego przetwarzania DO.	*art. 6 RODO*
III. REALIZACJA PRAW OSOBY, KTÓREJ DANE DOTYCZĄ								
III.1	Procedura udzielania informacji osobom, których dane dotyczą DO	[ocena obszaru]	Czy opracowano procedurę udzielania informacji osobom, których dotyczą DO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd ustanowionych procedur.	*art. 5 ust. 1, 12, 13, 14, 15 RODO; mot. 39, 58, 59, 60, 61, 64, 68 preambuły; art. 3 ust. 3,*

								art.. 4 ust 3 uodo
III.2	Obowiązki informacyjne podczas pozyskiwania DO od osób, których dane dotyczą (klauzula informacyjna)	[ocena obszaru]	1. Czy opracowano treść klauzuli informacyjnej dla osób, od których DO będą pozyskiwane oraz czy jej treść spełnia wymogi RODO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd i analiza klauzul.	*art. 13 RODO; mot. 39, 58-63 preambuły*
			2. Czy przewidziano obowiązek przedstawienia stosownych informacji (klauzuli informacyjnej) najpóźniej w czasie pozyskiwania DO? Czy przewidziano możliwość odstąpienia od tego obowiązku po upewnieniu się, że osoba, której dane dot. dysponuje już tymi informacjami?	[ocena wymogu]				

			3. Czy wzór klauzuli zapewnia przedstawienie: a) tożsamości i danych kontaktowych ADO; b) danych kontaktowych IOD, gdy ma to zastosowanie; c) celów przetwarzania oraz podstawy prawnej przetwarzania; d) wykazania prawnie uzasadnionych interesów (jeżeli są one podstawą przetwarzania); e) odbiorców danych; f) ewentualnym zamiarze przekazywania danych do państwa trzeciego lub organizacji międzynarodowej oraz podjętych zabezpieczeniach w tym zakresie (patrz szczegółowo art. 14 ust. 1 lit. f RODO)?	[ocena wymogu]				

			4.Czy wzór klauzuli zapewnia rzetelność i przejrzystość przetwarzania DO poprzez przedstawienie informacji o: a) okresie przechowywania danych lub (jeżeli nie jest to możliwe) kryteria ustalania tego okresu; b) prawach dostępu do danych, sprostowania, usunięcia, ograniczenia, przetwarzania, wniesienia sprzeciwu i przenoszenia danych; c) prawie cofnięcia zgody na przetwarzanie danych (jeżeli jest ona jedyną podstawą dla ich przetwarzania); d) prawie wniesienia skargi do organu nadzorczego; e) przyczynach zażądania podania DO (np. wymóg ustawowy, umowny albo konieczność realizacji umowy/usługi), czy	[ocena wymogu]				

			jest to obowiązkowe oraz o ewentualnych skutkach niepodania DO; f) ewentualnym zautomatyzowanym podejmowaniu decyzji na podstawie DO, w tym o profilowaniu oraz o zasadach podejmowania tych decyzji, a także o znaczeniu i ewentualnych konsekwencjach dla osoby, której dane dotyczą.					
III.3	Obowiązki informacyjne podczas pozyskiwania DO w inny sposób niż bezpośrednio od osób, których dane dotyczą (klauzula informacyjna)	**[ocena obszaru]**	1. Czy opracowano klauzulę informacyjną dla osób, których dane będą przetwarzane, a których dane pozyskano w sposób inny niż od osoby, której dane dotyczą?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd wdrożonych klauzul.	*art. 12, 14 ust. 3 pkt a-c i ust.5, i art. 15 ust. 3 RODO;* *mot. 39, 58, 59,60,64 ,68 preambuły;* *art. 4 uodo;*
			2. Czy przewidziano obowiązek przedstawienia stosownej informacji (klauzuli informacyjnej) w rozsądnym terminie oraz najpóźniej: - w ciągu miesiąca od ich pozyskania,	[ocena wymogu]				

			- przy pierwszej komunikacji lub - przy pierwszym ujawnieniu DO innemu odbiorcy?					
			3. Czy przewidziano możliwość odstąpienia od ww. obowiązku po upewnieniu się, że (art. 14 ust. 5 RODO): - osoba, której dane dot. dysponuje już tymi informacjami? - udzielenie informacji jest niemożliwe albo wymaga niewspółmiernie dużego wysiłku? - pozyskanie lub ujawnienie jest wyraźnie uregulowane prawem? - zgodnie z prawem DO muszą pozostać poufne?	[ocena wymogu]					
			4. Czy przewidziano możliwość odstąpienia od ww. obowiązku po upewnieniu się, że (art. 4 uodo) służy to realizacji zadania publicznego, jest to niezbędne dla realizacji celów, publicznych	[ocena wymogu]				

			wymienionych w art. 23 ust. 1 RODO tylko w przypadkach, gdy przekazanie tych informacji uniemożliwi lub znacząco utrudni wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji realizowanego zadania publicznego lub naruszy ochronę informacji niejawnych?					
			5. Czy wzór klauzuli zapewnia informację o: a) tożsamości i danych kontaktowych ADO lub jego przedstawiciela, b) danych kontaktowych IOD (jeżeli został powołany), c) celach i podstawach prawnych przetwarzania DO, d) kategoriach odnośnych DO,	[ocena wymogu]				

			e) informacjach o odbiorcach lub kategoriach odbiorców DO, f) ewentualnym zamiarze przekazywania danych do państwa trzeciego lub organizacji międzynarodowej oraz podjętych zabezpieczeniach w tym zakresie (patrz szczegółowo art. 14 ust. 1 lit. f RODO)?					
			6. Czy wzór klauzuli zapewnia rzetelność i przejrzystość przetwarzania DO poprzez przedstawienie dodatkowych informacji o: a) okresie przechowywania DO lub kryteriach ustalania tego okresu, b) prawnie uzasadnionym interesie ADO lub osoby trzeciej (jeżeli są one podstawą przetwarzania), c) prawie dostępu do danych, sprostowania, usunięcia, ograniczenia	[ocena wymogu]				

			przetwarzania oraz wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, d) prawie do cofnięcia zgody w dowolnym momencie (jeżeli jest ona podstawą dla ich przetwarzania), e) prawie wniesienia skargi do organu nadzorczego, f) źródle pochodzenia DO oraz o pochodzeniu ich ze źródeł publicznie dostępnych (jeżeli miało to zastosowanie), g) ewentualnym zautomatyzowanym podejmowaniu decyzji na podstawie DO, w tym o profilowaniu oraz o zasadach podejmowania tych decyzji, a także o znaczeniu i ewentualnych konsekwencjach dla osoby, której dane dotyczą?					

III.4	Obowiązki informacyjne wobec osób, których dane były przetwarzane przed wejściem w życie RODO	[ocena obszaru]	1. Czy dokonano przeglądu DO aktualnie przetwarzanych pod względem konieczności wypełnienia obowiązków informacyjnych wobec osób, których dane są przetwarzane?	[ocena wymogu]			Informacja od ADO, IOD, przegląd projektów procedur oraz ewentualnej klauzuli informacyjnej. Dla oceny stopnia wypełnienia obowiązku informacyjnego zastosowanie znajduje treść ww. klauzul informacyjnych odnoszących się do pozyskiwania DO w inny sposób, niż bezpośrednio od osób, których dane dotyczą. Uwaga: w zakresie nieuregulowanym w art. 14 ust. 5 RODO ADO wykonujący zadanie publiczne nie przekazuje informacji,	*art. 14 RODO*
			2. Czy w przypadku stwierdzenia konieczności dopełnienia obowiązków informacyjnych wobec osób, których dane są już przetwarzane, dopełniono obowiązku informacyjnego, o którym mowa w art. 14 RODO?	[ocena wymogu]				

							jeżeli: **a)** służy to realizacji zadania publicznego **i** **b)** niewykonanie obowiązku jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 RODO [katalog celów publicznych], **oraz** **c)** przekazanie tych informacji: - uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania	

							publicznego **lub** - naruszy ochronę informacji niejawnych. ADO jest obowiązany poinformować osobę, której dane dotyczą na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 14 ust. 1, 2 i 4 RODO.	
III.5	Obowiązki informacyjne w przypadku zmiany celu przetwarzania DO.	[ocena obszaru]	1. Czy procedura udzielania informacji przewiduje obowiązek ponownego zastosowania klauzuli informacyjnej wobec osób, których DO zostały zebrane w innym celu niż zamierzony cel ich wykorzystania?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd projektów klauzul.	*art. 13 ust. 3 RODO;* *art. 3 uodo*

			2. Czy procedura ta uwzględnia odstąpienie od ww. obowiązku gdy zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku jest niezbędne dla realizacji celów publicznych, o których mowa w art. 23 ust. 1 RODO oraz przekazanie tych informacji: (a) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub (b) naruszy ochronę informacji niejawnych.	[ocena wymogu]				

III.6	Prawo dostępu do DO	[ocena obszaru]	1. Czy zapewniono realizację praw dostępu dla osób, których DO dotyczą, w tym czy wskazano podmiot właściwy w zakresie potwierdzania przetwarzania DO oraz udzielający dostępu do informacji o: a) celach przetwarzania DO, b) kategoriach odnośnych DO, c) odbiorcach lub kategoriach odbiorców, którym DO zostały lub zostaną ujawnione, d) planowanym okresie przechowywania DO, a gdy nie jest to możliwe, kryteriach ustalania tego okresu, e) prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania DO oraz do wniesienia sprzeciwu wobec takiego przetwarzania, f) prawie wniesienia	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO). W przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 RODO, wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, ADO wykonujący zadanie publiczne wzywa osobę,	*art. 15 RODO;* *art. 5 uodo;* *mot. 59, 63, 64 i 73 preambuły;* *wytyczne dot. przenoszenia.*

			skargi do organu nadzorczego, g) ewentualnych informacjach nt. źródła pozyskania DO, h) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz o zasadach podejmowania tych decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania, i) odpowiednich zabezpieczeniach, w przypadku gdy DO są przekazywane do państwa trzeciego lub organizacji międzynarodowej.				której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Stosuje się odpowiednio przepis art. 64 Kodeks postępowania administracyjnego (art. 5 ust. 2 *uodo*). ADO jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niewykonania obowiązków, o których mowa w art. 15 ust. 1-3 RODO (art. 5 ust. 4 *uodo*).	
			2. Czy przewidziano procedurę dla dostarczania kopii DO podlegających przetwarzaniu, w tym czy wskazano osoby za to odpowiedzialne?	[ocena wymogu]				
			3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz	[ocena wymogu]				

			konieczność udzielenia odpowiedzi bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?					
			4. Czy procedury przewidują możliwość odstąpienia od potwierdzania przetwarzania DO, gdy służy to realizacji zadania publicznego i niewykonanie tego potwierdzenia jest niezbędne dla realizacji celów publicznych, o których mowa w art. 23 ust. 1 RODO, oraz wykonanie tych obowiązków: - uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub - naruszy ochronę	[ocena wymogu]				

			informacji niejawnych.					
III.7	Prawo do sprostowania i usuwania danych	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające realizację wniosku o sprostowanie albo usunięcie DO podlegających przetwarzaniu?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO). W przypadku, gdy wykonanie obowiązków, o	*art. 16, 17 , 19 i 23 RODO;* *mot. 39, 59, 65, 66 156 preambuły.*
			2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności i możliwości dokonania sprostowania albo usunięcia danych?	[ocena wymogu]				
			3. Czy przewidziano obowiązek powiadomienia każdego odbiorcy, któremu ujawniono DO o fakcie ich sprostowania lub usunięcia?	[ocena wymogu]				

III.8			4. Czy procedury te uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]			których mowa w art	
	Prawo do ograniczenia przetwarzania	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające realizację wniosku o ograniczenie przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*art. 18, 19 i 23 RODO;* *mot. 59, 67, 156 preambuły.*
			2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności i możliwości ograniczenia przetwarzania DO oraz za ograniczenie przetwarzania tych danych?	[ocena wymogu]				
			3. Czy przewidziano obowiązek powiadomienia każdego odbiorcy, któremu ujawniono DO o fakcie ich sprostowania lub usunięcia?	[ocena wymogu]				
			4. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz	[ocena wymogu]				

			odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?					
III.9	Prawo do przenoszenia danych	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające realizację wniosku o przeniesienie DO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: prawo dot. wyłącznie danych przetwarzanych w sposób zautomatyzowany na podstawie zgody albo umowy. Ponadto prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Ado.	*art. 20 i 23 RODO;* *mot. 59, 68, 156 preambuły;* *wytyczne dot. przenoszenia.*
			2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności i możliwości przeniesienia DO oraz przeniesienie tych danych?	[ocena wymogu]				
			3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				

							Ponadto niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	
III.10	Prawo sprzeciwu wobec przetwarzania danych w zakresie profilowania oraz marketingu bezpośredniego	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające rozpatrzenie sprzeciwu wobec przetwarzania DO: - w tym profilowania w ramach realizacji interesu publicznego, sprawowania władzy publicznej lub prawnie uzasadnionych interesów ADO; - na potrzeby marketingu bezpośredniego, w tym profilowania?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*art. 21 i 23 RODO;* *mot. 59, 65, 70 i 73 preambuły.*
			2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności zaprzestania przetwarzania DO, w tym profilowania?	[ocena wymogu]				

			3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
III.11	Prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowany przetwarzaniu, w tym profilowaniu	[ocena obszaru]	1. Jeżeli w jednostce stosuje się zautomatyzowane podejmowanie decyzji na podstawie DO, to czy zapewniono procedury umożliwiające wyłączenie zainteresowanej osoby z automatycznego przetwarzania, w tym profilowania?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*art. 22 i 23 RODO;* *mot. 71, 72 preambuły*
			2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności zaprzestania przetwarzania DO, w tym profilowania?	[ocena wymogu]				
			3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a	[ocena wymogu]				

			najpóźniej w ciągu miesiąca?					
III.12	Przygotowanie DO do realizacji praw osób, których te dane dotyczą	[ocena obszaru]	Czy dokonano przeglądu procesów przetwarzania DO, w tym przetwarzających je systemów informatycznych w zakresie sprawnego zlokalizowania DO w celu realizacji praw osób, których dane dotyczą, w tym prawa: - dostępu do DO, - sprostowania i usuwania danych, - ograniczenia przetwarzania, - przeniesienia danych, - sprzeciwu wobec przetwarzania danych w zakresie profilowania oraz marketingu bezpośredniego, - wyłączenia od zautomatyzowanego przetwarzania danych?	[ocena wymogu]			Informacja od ADO, IOD i pracownika ds. IT, przegląd procedur, przegląd systemów IT oraz wybranych procesów przetwarzania DO.	*art. 20 ust. 2, 21 ust. 5 RODO*
IV. INSPEKTOR OCHRONY DANYCH								

IV.1	Powołanie IOD	[ocena obszaru]	1. Czy kierownik jednostki wyznaczył IOD?	[ocena wymogu]			Informacja od ADO lub IOD, dokument potwierdzających wyznaczenie IOD, zakres obowiązków, opis stanowiska pracy, umowa o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem. Uwaga, wyznaczenie IOD jest	*art. 37 ust. 1 RODO;* *art. 37 ust. 6 RODO* *mot. 97 preambuły;* *art. 8, 9, 10 i 158 uodo;* *wytyczn*

			2. Czy IOD został powołany w trybie określonym w uodo? W szczególności, czy dopełniono obowiązku zawiadomienia PUODO o powołaniu IOD albo o zmianie danych dot. IOD lub ADO?	[ocena wymogu]			obowiązkowe, gdy: a) przetwarzania dokonują organ lub podmiot publiczny (niezależnie od tego, jakie dane są przetwarzane). Przez podmiot publiczny rozumie się (1) jednostki sektora finansów publicznych, (2) instytuty badawcze, (3) Narodowy Bank Polski. b) główna działalność ADO lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;	*e dot. IOD*

							c) główna działalność ADO lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii DO lub DO dotyczących wyroków skazujących i czynów zabronionych. art. 37 ust. 1 RODO. Ponadto zgodnie z art. 10 a) Termin na zawiadomienie PUODO o wyznaczeniu IOD wynosi 14 dni od dnia wyznaczenia i można tego dokonać przez pełnomocnika. b) Wymaga się wskazania: - imienia, nazwiska oraz adresu poczty elektronicznej lub numer	

							telefonu inspektora. - imienia i nazwiska, nazwy albo firmy ADO oraz adresu zamieszkania, siedziby albo miejsca prowadzenia działalności - numeru REGON, jeżeli został nadany ADO lub podmiotowi przetwarzającemu. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Wg. art. 158 uodo: a) administrator	

							bezpieczeństwa informacji (ABI) zgłoszony do Generalnemu Inspektorowi Ochrony Danych Osobowych (tj. GIODO), do dnia 24 maja 2018 r. staje się IOD; b) aby dotychczasowy ABI stał się IOD na czas nieokreślony należy o tym zawiadomić PUODO do dnia 1 września 2018 r.; c) ADO, który do dnia wejścia w życie nowej uodo nie powołał ABI będzie miał obowiązek wyznaczenia IOD oraz zawiadamia PUODO do dnia 31 lipca 2018 r. Jeśli jednostka nie ma obowiązku	

							powołanie IOD i w związku z tym odpowiedzi na pytania pomocnicze brzmią "NIE DOTYCZY", to nie ma konieczności weryfikowania pozostałych pytań w obszarze V. Inspektor Ochrony Danych.	
			3. W przypadku wyznaczenia IOD spoza jednostki, czy powołano pracowników (albo zespół) do kontaktów roboczych ADO z IOD oraz do wypełniania obowiązków związanych z ochroną DO?	[ocena wymogu]			Informacja od ADO i IOD. Analiza umowy o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji ADO/podmiotu przetwarzającego.	*art. 38 ust. 2 RODO;* *wytyczne dot. IOD.*

							Uwaga: dotyczy tylko jednostek, w których IOD został wyznaczony spoza jednostki. Powołanie takiego zespołu nie jest obowiązkowe. Jeśli odpowiedź na to pytanie brzmi "NIE" to nie jest konieczne weryfikowanie pozostałych kwestii dotyczących zespołu	
			4. Czy wszystkie zadania IOD, o których mowa w art. 39 RODO (albo zadania ww. zespołu) zostały powierzone w formie pisemnej?	[ocena wymogu]			Informacja od ADO i IOD, regulamin organizacyjny, procedury wewnętrzne, umowa, opis stanowiska pracy. Informacja od pracodawcy. Analiza zakresu zadań IOD.	*art. 39 RODO;* *mot. 97 preambuły; wytyczne dot. IOD.*

IV.2	Kompetencje IOD	[ocena obszaru]	1. Czy osoba wyznaczona na IOD posiada odpowiednie kwalifikacje zawodowe, a w szczególności wiedzę nt. prawa i praktyk w dziedzinie ochrony DO oraz realizowanych zadań?	[ocena wymogu]			Informacja od ADO i IOD. Opis stanowiska pracy, cv, życiorys i doświadczenie IOD, szkolenia, dyplomy, certyfikaty zawodowe.	
			2. Jeżeli IOD jest pracownikiem jednostki, to czy jej kierownictwo uwzględniło potrzeby w zakresie utrzymania wiedzy fachowej (szkoleń i podnoszenia kompetencji)?	[ocena wymogu]			Informacja od ADO (kadry) i IOD. Budżet i plan szkoleń, indywidualny program rozwoju zawodowego, gdy IOD jest pracownikiem ADO. Uwaga: jeżeli IOD pełnił swoją funkcję dłuższy czas, to należy zwrócić uwagę czy był szkolony i podnosił kwalifikacje z zakresu przetwarzania DO? Dopuścić należy również różne formy	*art. 37 ust. 5 RODO;* *mot. 97 preambuły* *wytyczne dot. IOD.*

							samokształceni a.	
IV.3	Zasoby IOD	[ocen a obsza ru]	Czy zapewniono IOD odpowiednie zasoby do wykonywania swoich zadań? W tym zasoby: - kadrowe (np. zespół inspektora ochrony danych)? - infrastrukturalne (pomieszczenia, sprzęt, wyposażenie)? - informatyczne (konto poczty elektronicznej, konto w systemie elektronicznego obiegu dokumentacji)?	[ocena wymogu]			Informacja od ADO i IOD. Uwaga: Należy zwrócić uwagę na skrajnie niewystarczając e zasoby IOD do realizacji zwykłych zadań, np. brak wyposażenia albo usytuowanie miejsca stanowiska pracy IOD utrudniające realizację zadań. Powołanie zespołu IOD nie jest obowiązkowe, jednakże warto się zastanowić czy ilość danych przetwarzanych w danej	*art. 38 ust. 2 RODO;* *wytyczn e dot. IOD*

							jednostce umożliwi skutecznie wykonywać obowiązki samodzielnie IOD.	
IV.4	Niezależność IOD	[ocena obszaru]	1. Czy IOD jest bezpośrednio podległy najwyższemu kierownictwu jednostki?	[ocena wymogu]			Informacja od ADO i IOD. Statut, regulamin organizacyjny, zakres obowiązków, opis stanowiska pracy.	*art. 38 ust. 3 RODO;* *wytyczne dot. IOD*
			2. Czy pozostałe zadania i obowiązki IOD w jednostce (jeżeli są wykonywane) nie powodują konfliktu interesów z funkcją IOD w jednostce? Np. czy IOD nie zajmuje stanowiska kierowniczego (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy)?	[ocena wymogu]			Informacja od ADO lub IOD. Ponadto zakres zadań IOD, opis stanowiska pracy / umowa o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji ADO / podmiotu przetwarzające	*art. 38 ust. 6 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD*

							go, w szczególności analiza ich treści.	
			3. Czy ADO (albo jego przedstawiciel) zapewnił warunki dla niezależnej pracy IOD, w szczególności czy: - powstrzymano się od wydawania instrukcji w zakresie realizacji zadań przez IOD? - nie odwoływano, ani nie karano IOD w związku z wypełnianiem jego zadań?	[ocena wymogu]			Informacja od IOD oraz ewentualne wyjaśnienia od ADO.	*art. 38 ust. 3 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD.*
IV.5	Dostępność IOD	[ocena obszaru]	1. Czy dopełniono obowiązku zawiadomienia PUODO o danych kontaktowych IOD?	[ocena wymogu]			Informacja od ADO i IOD. Dokument potwierdzający zawiadomienie.	*art. 37 ust. 7, RODO;* *art. 10 uodo;* *wytyczne dot. IOD.*

			2. Czy dopełniono obowiązku publikacji danych kontaktowych IOD? Czy dane te są łatwe do odnalezienia i umożliwiają osobom, których dane dotyczą oraz organom nadzorczym nawiązanie kontaktu w łatwy sposób?	[ocena wymogu]			Informacja od ADO i IOD. Analiza stron www. jednostki, zakładki RODO/ochrona danych osobowych, która uwzględniałaby w szczególności dane osobowe IOD (adres korespondencyjny, telefon kontaktowy lub dedykowany adres email, dedykowana infolinia, formularz kontaktowy z IOD na stronie internetowej organizacji) oraz jego zadania.	*art. 37 ust. 7 RODO;* *art. 11 uodo;* *wytyczne dot. IOD.*
			3. Czy poinformowano pracowników jednostki o imieniu, nazwisku i danych kontaktowych IOD oraz o możliwości konsultacji w zakresie przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD. Analiza intranetu jednostki, komunikatów do pracowników, zakładek RODO/ochrona	*wytyczne dot. IOD*

							danych osobowych, która uwzględniałaby w szczególności dane osobowe IOD oraz jego zadania.	
IV.6	Warunki do realizacji zadań IOD	[ocena obszaru]	1. Czy IOD ma możliwość skutecznego, właściwego i niezwłocznego włączenia się we wszystkie procesy przetwarzania danych w jednostce, a w szczególności procesy związane z: a) określaniem zakresu, celów i sposobów tego przetwarzania, b) oceną skutków dla ochrony DO, c) identyfikacją i monitoringiem procesów przetwarzania, d) oceną prawidłowości przetwarzania, e) współpracą i kontaktami z PUODO, f) bezpośrednią obsługą osób, których dane są	[ocena wymogu]			Informacja od ADO i IOD. Analiza treści procedur, wytycznych, wskazówek oraz instrukcji wewnętrznych wskazujących na obowiązek współpracy komórek organizacyjnych z IOD w zakresie przetwarzania DO. Uwaga: włączanie IOD w procesy przetwarzania nie oznacza, że może on przejmować kompetencje ADO (jeżeli tak	*art. 38 i 39 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD.*

			przetwarzane, g) projektami, programami i zamówieniami publicznymi odnoszącymi się do kwestii przetwarzania DO, h) projektami regulacji prawnych oraz procedur wewnętrznych (tj. realizacją ochrony DO w fazie projektowania).				jest patrz punkt wyżej dot. konfliktu interesów IOD).	
			2. Czy procedury wewnętrzne nakładają na pozostałe komórki organizacyjne obowiązek współpracy z IOD, dzięki czemu może on uzyskać niezbędne wsparcie, w szczególności kadrowe, prawne, księgowe oraz informatyczne?	[ocena wymogu]			Informacja od ADO i IOD. Regulaminy organizacyjny i wewnętrzne Polityka/procedury ODO.	*art. 38 ust. 2 RODO;* *wytyczne dot. IOD.*
IV.5	Ocena regulacji wewnętrznych w zakresie ochrony DO przez IOD	[ocena obszaru]	Czy w ocenie IOD obowiązujące w jednostce procedury, polityki wewnętrzne lub powtarzalne praktyki są odpowiednie dla zapewnienia	[ocena wymogu]			Informacja od IOD. Wyniki wcześniejszych audytów/kontroli/sprawdzeń w przedmiotowym obszarze.	*art. 24 ust. 2, 32 i 39 RODO*

			skutecznej ochrony DO?					
V. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH								
V.1	Identyfikacja DO i zakresu ich przetwarzania w jednostce	[ocena obszaru]	Czy dokonano identyfikacji procesów, w których DO są lub będą przetwarzane? Czy zidentyfikowano zakres, w jakim DO są/będą przetwarzane?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur w zakresie przetwarzania DO, badanie wybranych, dokumentów i systemów przetwarzających, procesów przetwarzania danych oraz rejestrów czynności przetwarzania DO.	*Definicja DO oraz ich przetwarzania (art. 4 pkt 1 i 2 RODO).*

V.2	Rejestr czynności przetwarzania DO	[ocena obszaru]	1. Czy wyznaczono podmiot (pracownika albo kom. org.), któremu powierzono przygotowanie/prowadzenie rejestru czynności przetwarzania DO?	[ocena wymogu]			Informacja od ADO i/lub IOD. Analiza/oględziny rejestru. Uwaga: Prowadzenie rejestru czynności przetwarzania nie jest obowiązkiem powszechnym. Zgodnie z art. 30 ust. 5 RODO do prowadzenia rejestru zobowiązani są ADO i podmioty przetwarzające, którzy zatrudniają 250 lub więcej osób oraz gdy: - dokonują systematyczneg	*art. 30 ust. 1 RODO;* *mot. 82 preambuły;* *Standardy KZ.*
			2. Czy jest prowadzony rejestr czynności przetwarzania DO? Czy rejestr jest prowadzony w formie pisemnej, w tym elektronicznej?	[ocena wymogu]				

			3. Czy rejestr zawiera wszystkie elementy wymagane przez art. 30 ust. 1 RODO?	[ocena wymogu]			o przetwarzania mogącego powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, lub - dokonują przetwarzania szczególnych kategorii DO, o których mowa w art. 9 ust. 1 RODO, lub - przetwarzają DO dotyczące wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO. Rejestr musi być prowadzony w formie pisemnej, w tym elektronicznej. Dobra praktyka Brytyjskiego Organu nadzorczego ochrony DO do przygotowania	

							się do opracowania rejestru czynności: 1. Nazwy procesów biznesowych; 2. Informacja o podstawie prawnej przetwarzania danych; 3. Informacja o uprawnieniach osób, których dotyczy przetwarzanie danych; 4. Informacja o zautomatyzowanym przetwarzaniu DO w tym o profilowaniu; 5. Źródło, z którego ADO otrzymał DO; 6. Informacja o uzyskaniu zgody na przetwarzanie DO; 7. Miejsce przechowywania danych; 8. Informacja o zidentyfikowane	

							j konieczności przeprowadzeni a oceny skutków przetwarzania ochrony danych; 9. Informacja o naruszeniach ochrony DO; 10. Wskazanie technologii, aplikacji lub systemów informatycznyc h, w których następuje przetwarzanie DO; 11. Termin rozpoczęcia przetwarzania danych. Należy zwrócić uwagę, czy rejestr ten zawiera tylko dane wymagane art. 30 RODO, czy też jednostka rozszerzyła zakres danych ujmowanych w rejestrze? Jeśli tak, to zapytać o motywy	

							rozszerzenia katalogu danych wpisywanych do rejestr (tzn. chodzi o mot./względy praktyczne). Jeżeli jednostka świadomie zaplanowała rozszerzony zakres danych w rejestrze, to może to świadczyć o wyższym poziomie organizacji ochrony DO. Jeżeli brak jest obowiązku prowadzenia danego rejestru, to proszę zaznaczyć "NIE DOTYCZY".	
V.3	Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu ADO albo	[ocena obszaru]	1. Czy wyznaczono podmiot (pracownika albo kom. org.), któremu powierzono przygotowanie/ prowadzenie rejestru wszystkich kategorii czynności przetwarzania DO?	[ocena wymogu]			Weryfikacja dokumentów dot. rejestru wszystkich kategorii czynności. Weryfikacja zapisów umów powierzenia	*art. 30 ust. 2 RODO;* *mot. 82 preambuły.*

	przez podmiot przetwarzający		2. Czy opracowano rejestr wszystkich czynności przetwarzania DO? Czy jest on prowadzony w formie pisemnej/elektronicznej? Czy zawiera wszystkie elementy wymagane przez art. 30 ust. 2 RODO?	[ocena wymogu]			danych/wzoru umowy powierzenia danych. W przypadku, gdy jednostka jest również podmiotem przetwarzającym dane, to analiza rejestru wszystkich kategorii czynności. Uwaga: Prowadzenie rejestru nie jest obowiązkiem powszechnym. Jeżeli brak jest obowiązku prowadzenia danego rejestru, to należy zaznaczyć "NIE DOTYCZY".	
VI. OCENA SKUTKÓW PRZETWARZANIA DANYCH OSOBOWYCH								
VI.1	Zarządzanie ryzykiem dla ochrony DO	[ocena obszaru]	1. Czy istnieje procedura (albo powtarzalna praktyka) analizy ryzyka dla ochrony DO?	[ocena wymogu]			Informacja od ADO, IOD i pracownika ds. IT. Weryfikacja polityki w	*art. 24 i 32 RODO;*

			2. Czy prowadzona jest analiza ryzyka dla ochrony DO? Czy wyznaczono podmiot (osobę, stanowisko albo zespół) odpowiedzialny w tym zakresie?	[ocena wymogu]			zakresie bezpieczeństwa i ochrony DO. Potwierdzenie istnienia procedur dot. SZBI, inna dokumentacja lub dane potwierdzające, w szczególności dokumentacja: - opisująca procedury przetwarzania danych; - wskazująca działania, jakie należy podjąć (np. nadawanie praw dostępu, monitorowanie incydentów, back up, mechanizmy kryptograficzne, testy bezpieczeństwa, audyty, kontrole itp.); - określająca zasady i reguły postępowania, jakie należy zastosować. Aktualizacja procedur –	*mot. 26, 28, 29, 39, 74-78, 83 i 85 preambuły;* *Rozporządzenie KRI* *Standardy KZ*
			3. Czy polityka ochrony DO jest oparta o analizę ryzyka? Czy uwzględnia wnioski oraz rekomendacje wynikające z analizy ryzyka dla ochrony DO z ostatniego okresu?	[ocena wymogu]				
			4. Czy zastosowano wskazane w rekomendacjach (IOD albo innego właściwego podmiotu) środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanemu ryzyku?	[ocena wymogu]				

							ustalenie dat ostatnich przeglądów i aktualizacji procedur Istniejąca dokumentacja analizy ryzyka dla ochrony DO - kwerenda wyników analizy ryzyka z ostatniego okresu z uwzględnieniem rekomendacji odnoszących się do środków technicznych i organizacyjnych, zapewniających ochronę DO. Zaktualizowane procedury w zakresie DO powinny uwzględniać ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji,	

							nieuprawnionego ujawnienia lub nieuprawnionego dostępu do DO, przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Warto uwzględnić również skutki dla ochrony DO, wymienione w mot. 75 preambuły, tj. ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, które może wynikać z przetwarzania DO prowadzącego do uszczerbku fizycznego, szkód majątkowych lub	

							niemajątkowych - w szczególności, jeżeli przetwarzanie może skutkować dyskryminacją, kradzieżą tożsamości.	
VI.2	Ochrona danych w fazie projektowania oraz domyślna ochrona danych	[ocena obszaru]	1. Czy obowiązujące w jednostce pozostałe procedury, polityki wewnętrzne lub powtarzalne praktyki uwzględniają zasadę prywatności w fazie projektowania (privacy by design) oraz domyślnej ochrona danych (privacy by default)? W szczególności, czy ww. zasady znajdują odzwierciedlenie w procedurach jednostki odnoszących się do: - tworzenia prawa i regulacji wewnętrznych, - zarządzania projektami, - realizacji zamówień publicznych oraz - projektowania i modyfikacji systemów teleinformatycznych.	[ocena wymogu]			Informacja od ADO, IOD, Administratora Systemu Informacji (albo inny właściwy pracownik ds. IT). Wgląd w dokumentację z wykonanego przeglądu systemów (o ile taka została sporządzona). Uwaga: Każdy program, aplikacja lub system IT, wykorzystywany do przetwarzania DO, powinien mieć domyślne ustawienia przewidujące ochronę DO. Obowiązek	*art. 25 i 28 RODO;* *mot. 78 preambuły.*

			2. Czy dokumentacja jednostki zawiera potwierdzenie faktu zobowiązania wytwórców/dostawców aplikacji, usług i produktów do stosowania wymogów RODO? Np. czy w konkretnych przypadkach zawierania umów z podwykonawcami przewidziano: - konsultacje albo uczestnictwo osób pełniących funkcje ADO albo IOD? - obowiązek każdorazowego, szczegółowego uzasadnienia konieczności rozwiązań skutkujących przetwarzaniem DO? - zasadę minimalizowania ilości i zakresu i okresu przetwarzania DO?	[ocena wymogu]			zapewnienia domyślnej ochrony danych dotyczy ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Należy zobowiązywać wytwórców/dostawców aplikacji, usług i produktów, w ramach których przetwarzane są DO, by prawo do ochrony DO było uwzględniane już w fazie opracowywania i projektowania. Ponadto, ww. wytwórcy/dostawcy z należytym uwzględnieniem stanu wiedzy technicznej powinni zapewniać ADO	

							i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązkach ochrony danych. Zwrotnie, zasada uwzględniania ochrony danych w fazie projektowania i zasada domyślnej ochrony danych powinna być uwzględniana w przetargach publicznych. Ponadto: 1. W ustawieniach początkowych systemów przetwarzających DO, jako domyślne jest ustawiona ochrona prywatności, a zmiana takiego ustawienia może	

							następować jedynie na wyraźne żądanie użytkownika programu/systemu. 2. Domyślnie, czyli bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą – i to w kluczowym dla użytkownika momencie przyłączenia się do danego systemu. 3. Domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane (minimalizacja danych).	

VI.3	Identyfikacja istotnego ryzyka dla ochrony DO	[ocena obszaru]	Czy identyfikuje się operacje przetwarzania danych, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono, jako wysoki? Czy uwzględniono wyniki analizy ryzyka z ostatniego okresu?	[ocena wymogu]			Informacja od ADO i IOD. Należy zwrócić uwagę na charakter przetwarzanych danych (np. dane wrażliwe) oraz wyniki analizy ryzyka. Analiza ryzyka powinna odnosić się do wszystkich procesów wskazanych w rejestrze czynności przetwarzania.	*art. 35 RODO;* *mot. 84, 89-93 preambuły.*

VI.4	Ocena skutków przetwarzania dla ochrony DO	[ocena obszaru]	Czy dokonano oceny skutków dla ochrony danych: a) dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono, jako wysoki? (art. 35 ust. 1 RODO) b) wskazanych przez PUODO w wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny? (art. 35 ust. 4 RODO) c) po stwierdzeniu takiej potrzeby w trakcie przeglądu, o którym mowa w art. 35 ust. 11 RODO? Czy w badanym okresie stwierdzono taką potrzebę? d) po zaleceniu jej przez IOD w toku monitorowania przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD. Dokumentacja dotycząca analizy ryzyka oraz oceny skutków. Wykaz PUODO, o którym mowa w art. 35 ust. 4 i 5 RODO. - Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. poz. 827). Uwaga: zgodnie z wytycznymi dot. oceny skutków (str. 15) ocena ta powinna być dokumentowan	*art. 35 RODO;* *wytyczne dot. oceny skutków.*

							a. Ocena tych danych wymagana jest w szczególności w przypadku: a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; b) przetwarzania na dużą skalę szczególnych	

							kategorii DO, o których mowa w art. 9 ust. 1, lub DO dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.	
VI.5	Zakres oceny skutków przetwarzania dla ochrony DO	[ocena obszaru]	1. Czy ocena skutków zawiera następujące elementy: (art. 35 ust. 7 RODO) a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez	[ocena wymogu]			Weryfikacja opracowanej oceny skutków. Informacja od ADO i IOD. Uwaga: kryteria oceny, o których mowa w wytycznych dot. oceny skutków, tj. 1. Ewaluacja lub ocena (mot. 71 i 91	*art. 32 i 35 RODO* *wytyczne dot. oceny skutków.*

			ADO; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą; d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę DO i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.				preambuły); 2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne lub podobne istotne skutki (art. 35 ust. 3 lit. a RODO); 3. Systematyczne monitorowanie (art. 35 ust. 3 lit. c RODO); 4. Dane wrażliwe (art. 9 RODO); 5. Dane przetwarzane na dużą skalę (mot. 91 preambuły); 6. Dokonano porównania lub połączenia procesów przetwarzania danych; 7. Dane dotyczące osób wymagających szczególnej opieki (mot. 75 preambuły);	
			2. Czy podczas dokonywania oceny skutków uwzględniono wszystkie kryteria oceny, o których mowa w wytycznych dot. oceny skutków?	[ocena wymogu]				

							8. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych (art.35 ust. 1 i mot. 89 i 91 preambuły); 9. Transgraniczne przekazywanie danych poza Unię Europejską (mot. 116 preambuły); 10. Gdy przetwarzanie samo w sobie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy” (art. 22 i mot. 91 preambuły).	

VI.6	Zapewnienie udziału IOD w ocenie skutków przetwarzania dla ochrony DO	[ocena obszaru]	1. Czy ocena skutków przetwarzania była konsultowana z IOD?	[ocena wymogu]			Informacja od IOD. Dokumentacja świadcząca o konsultacjach i monitorowaniu wykonania oceny skutków, w tym pisma i notatki wewnętrzne. Uwaga: z art. 39 ust. 1 lit. c wynika obowiązek IOD udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych zgodnie z art. 35 RODO. Przypadki, w których IOD nie zgadza się oceną ADO lub ADO nie zgadza się z zaleceniami IOD, powinny być odnotowane w formie pisemnej (w formie notatki lub protokołu rozbieżności).	*art. 35 ust. 2, art. 39 ust. 1 lit. c RODO;* *wytyczne dot. oceny skutków.*
			2. Czy IOD monitorował wykonanie oceny skutków przetwarzania?	[ocena wymogu]				

VI.7	Uprzednie konsultacje	[ocena obszaru]	Jeżeli ocena skutków przetwarzania lub rekomendacja IOD w zakresie tej oceny wskazały na wysokie ryzyko przetwarzania, a ADO nie zastosował środków w celu jego zminimalizowania, to czy przed rozpoczęciem przetwarzania dokonano konsultacji z PUODO?	[ocena wymogu]			Informacja od ADO i IOD oraz pismo ws. konsultacji (zgodnie z art. 36 ust. 3 RODO).	*art. 36 RODO; mot. 94-96 preambuły; wytyczne dot. oceny skutków*
VII. NARUSZENIE OCHRONY DANYCH OSOBOWYCH								
VII.1	Podmioty właściwe w zakresie postępowania z naruszeniami ochrony DO	[ocena obszaru]	Czy ADO wyznaczył osoby właściwe w zakresie zgłaszania PUODO naruszeń ochrony DO, które skutkują ryzykiem naruszenia praw lub wolności osób fizycznych?	[ocena wymogu]			Informacja od ADO i IOD. Analiza treści przedmiotowej procedury (w tym ewentualnego wzoru zgłoszenia).	*art. 33 i 34 RODO; mot. 85-88 preambuły*

VII.2	Procedura postępowania z naruszeniami ochrony DO	[ocena obszaru]	Czy opracowano procedurę zgłaszania i postępowania z naruszeniami ochrony DO, która w szczególności uwzględnia: a) definicję naruszenia wymagającego zgłoszenia do organu nadzorczego? b) obowiązek niezwłocznego zgłaszania przez ADO naruszeń (w ciągu 72 godzin)? c) obowiązek dokumentowania wszelkich naruszeń ochrony DO, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych? d) wzór zgłoszenia spełniający wymaga art. 33 RODO? e) role oraz odpowiedzialność wszystkich podmiotów zaangażowanych w proces postępowania z naruszeniami DO? f) niezwłoczne zawiadomienie osoby,	[ocena wymogu]			Rejestr naruszeń ochrony danych. Analiza dokumentacji określających zakresy zadań i odpowiedzialności np. opisy stanowisk pracy, zakresy zadań. Analiza dokumentacji w zakresie naruszeń bezpieczeństwa (np. podrównanie z rejestrem incydentów bezpieczeństwa i procedurami SZBI). Uwaga: Analizując procedury należy zwrócić uwagę na podmioty decydujące i sposób określenia czy naruszenie jest naruszeniem i czy podlega	

			której dane dotyczą (jeżeli ma to zastosowanie)? g) prawnie uzasadniony interes organów ścigania, jeżeli przedwczesne ujawnienie naruszenia mogłoby utrudnić badanie jego okoliczności? g) wzór ww. zawiadomienia zgodnie z art. 34 RODO?				zgłoszeniu do organu nadzorczego (pożądany jest udział IOD w tym procesie). Np.: - powołano stały zespół, który rozpatruje indywidualne przypadki, - określono przykładowy katalog możliwych naruszeń/incydentów, które stanowią incydent podlegający zgłoszeniu. Procedury w zakresie zarządzania incydentami naruszenia ochrony DO (wszelkie odpowiednio wdrożone techniczne środki ochrony, w tym środki organizacyjne, które zapewniają	
VII.3	Rejestr naruszeń ochrony DO	[ocena obszaru]	Czy jest prowadzony rejestr naruszeń ochrony DO, który dokumentuje w szczególności : - wszystkie przypadki zgłoszeń, w tym tych, które nie podlegają obowiązkowi przekazania do PUODO, - podmioty podejmujące decyzje w związku ze zgłoszeniem oraz - sposób postępowania z poszczególnymi zgłoszeniami?	[ocena wymogu]				

							bieżącą identyfikację naruszeń ochrony DO i pozwalają szybko poinformować organ nadzorczy i osobę, której dane dotyczą o naruszeniu).	
VII.4	Zawiadomienia o naruszeniu ochrony DO	[ocena obszaru]	Jeżeli stwierdzono istotne naruszenia ochrony DO, to czy dopełniono obowiązku zawiadomienia PUODO oraz osoby, której dane dotyczą?	[ocena wymogu]			Informacja od ADO i IOD. Dowody potwierdzające stosowne zawiadomienia (jeżeli były one konieczne). W przypadku znacznej liczby incydentów badanie można ograniczyć do próby zawiadomień.	*art. 33 i 34 RODO; mot. 85-88 preambuły*

OGÓLNA OCENA SPEŁNIANIA OBOWIĄZKÓW W ZAKRESIE DANYCH OSOBOWYCH

Sporządził:

(data i podpis)

Zatwierdził:

(data i podpis)

PODSUMOWANIE OOCENY OBSZARÓW	OCENA					POZIOMY ZARZĄDZANIA
	POZYTYWNA	ZASTRZEŻENIA	NEGATYWNA	W REALIZACJI	NIE DOTYCZY	
I. ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH	0	0	0	0	0	PLANOWANIE I ORGANIZACJA PROCESU PRZETWARZANIA (tj. polityka ochrony danych osobowych i administrator), w tym administratorzy, współadministratorzy i podmioty przetwarzające.
II. PRAWO DO PRZETWARZANIA DANYCH OSOBOWYCH	0	0	0	0	0	PRZETWARZANIE DO (tj. procesy przetwarzania danych) i REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ
III. REALIZACJA PRAW OSOBY, KTÓREJ DANE DOTYCZĄ	0	0	0	0	0	
IV. INSPEKTOR OCHRONY DANYCH OSOBOWYCH	0	0	0	0	0	NADZÓR I MONITOROWANIE SYSTEMU OCHRONY DO (tj. mechanizmy zapewnienia, monitoringu i nadzoru nad procesem przetwarzania danych)
V. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA	0	0	0	0	0	
VI. OCENA SKUTKÓW PRZETWARZANIA DANYCH OSOBOWYCH	0	0	0	0	0	
VII. NARUSZENIE OCHRONY DANYCH OSOBOWYCH	0	0	0	0	0	

Łącznie:	**0**	**0**	**0**	**0**	**0**

Liczba ocen: **0** tj. 0%

Brakuje: **48** tj. 100%

Wykaz skrótów i aktów prawnych:		**Źródła internetowe, dostępne na dzień 18 września 2018 r.**
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz.U. UE L 119/1)	https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679&from=PL
mot. / preambuły	motyw preambuły do *RODO.*	https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2018.127.01.0002.01.POL
uodo	Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000)	http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000
Wytyczne dot. oceny skutków przetwarzania	Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (MP poz. 827)	http://www.monitorpolski.gov.pl/MP/2018/827

Rozporządzenie KRI	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. ws. Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 526 z późn. zm.)	http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20120000526
Standardy KZ	Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych	https://www.mf.gov.pl/c/document_library/get_file?uuid=f25c63b6-b229-4e4a-9194-ada9ea8799e7&groupId=764034
wytyczne dot. IOD	Wytyczne dotyczące inspektorów ochrony danych osobowych Grupy Roboczej art. 29 ds. Ochrony Danych (WP 243)	https://uodo.gov.pl/pl/10/7
wytyczne dot. oceny skutków ochrony DO	Wytyczne dot. oceny skutków dla ochrony danych (ang. Data Protection Impact Assessment – DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko”, do celów rozporządzenia 2016/679 Grupy Roboczej art. 29 ds. Ochrony Danych (WP 248)	https://uodo.gov.pl/pl/10/9
wytyczne dot. przenoszenia	Wytyczne dotyczące prawa do przenoszenia danych Grupy Roboczej art. 29 ds. Ochrony Danych (WP 242)	https://uodo.gov.pl/pl/10/6
UOD	Urząd Ochrony Danych Osobowych	https://uodo.gov.pl/pl

PUODO	Prezes Ochrony Danych Osobowych	
IOD	Inspektor ochrony danych	
ADO	Administrator Danych Osobowych	
ABI	Administrator bezpieczeństwa informacji – funkcjonujący do dnia 24.05.2018 r.	
DO	Dane osobowe	
SZBI	System zarządzania bezpieczeństwem informacji - w tym Polityka Bezpieczeństwa Informacji (PBI) w rozumieniu Krajowych Ram Interoperacyjności	
pracownik ds. IT	Kierownik komórki IT lub pracownik odpowiedzialny za obszary IT	
pracownik ds. kadr	Kadrowy/ kierownik komórki kadrowej lub pracownik odpowiedzialny za sprawy kadrowe gospodarcze (o ile nie wyodrębniono komórki ds. kadrowych)	
pracownik ds. gospodarczych	Kierownik komórki lub pracownik odpowiedzialny za sprawy gospodarcze (o ile nie wyodrębniono komórki ds. gospodarczych)	
pracownik ds. BHP	Kierownik komórki lub pracownik odpowiedzialny za sprawy BHP (o ile nie wyodrębniono komórki ds. BHP)	
kierownik jednostki	kierownik jednostki administracji publicznej/organ administracji publicznej	
jednostka	jednostka sektora finansów publicznych	

Instrukcja postępowania przy naruszeniach ochrony danych osobowych

§ 1. Celem niniejszej instrukcji jest określenie procedury postepowania w przypadkach naruszenia bezpieczeństwa przetwarzania danych osobowych, gdy naruszenie jest związane z:

1) danymi przetwarzanymi w formie tradycyjnej;
2) elektroniczna formą przetwarzania danych osobowych;
3) nieprawidłową pracą systemu informatycznego.

§ 2. Zakres podmiotowy stosowania niniejszej instrukcji obejmuje wszystkich pracowników oraz osoby mające dostęp do danych osobowych, przy pomocy których Administrator wykonuje swoje czynności.

§ 3. Naruszeniem bezpieczeństwa jest każdy stwierdzony fakt:

1) nieuprawnionego udostępniania instytucjom, podmiotom lub osobom danych osobowych;
2) sytuacje, gdy stan urządzeń, zbiorów danych, ujawnione metody pracy, sposób działania programu, jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie zabezpieczenia danych;
3) stwierdzone naruszenie zabezpieczenia systemu informatycznego, w tym m.in.:
   a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej),
   b) niewłaściwe parametry środowiska (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych),
   c) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia bezpieczeństwa,
   d) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   f) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,

g) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia,

h) niedopuszczalna manipulacja danymi w systemie,

i) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,

j) praca w systemie informatycznym, wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych (np. praca przy komputerze osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu),

k) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki",

l) podmienienie albo zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych,

m) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur ochrony danych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie dokumentów w drukarce lub na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych w celach prywatnych, itp.).

§ 4. 1. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia systemu bezpieczeństwa lub naruszenia ochrony danych osobowych, zobowiązany jest bezzwłocznie powiadomić przełożonego oraz Inspektora Ochrony Danych.

2. Miejsce zdarzenia należy pozostawić w stanie nienaruszonym.

3. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych osobowych, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego dokumentuje opis stanu faktycznego:

1) prowadzi korespondencję w formie mailowej, telefonicznie lub osobiście;
2) sporządza notatkę z oględzin miejsca zdarzenia (jeśli sytuacja tego wymaga);
3) odbiera pisemne wyjaśnienia od osoby, która ujawniła zdarzenie (jeśli sytuacja tego wymaga);
4) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia;
5) Administrator w zależności od zakresu naruszenia podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń;
6) uwzględniając skalę oraz skutki naruszenia, Administrator danych osobowych decyduje o powołaniu doraźnego zespołu i powiadomieniu o zdarzeniu Prezesa Urzędu Ochrony Danych Osobowych.

§ 5. 1. W przypadku naruszenia ochrony danych osobowych, Administrator danych osobowych wraz z Inspektorem Ochrony Danych ustala:

1) powagę naruszenia;
2) ocenia możliwe skutki naruszenia dla osób, których dane dotyczą uwzględniając, czy naruszenie może spowodować:

a) uszczerbek fizyczny,
b) szkody majątkowe,
c) szkody niemajątkowe;

3) czy osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
4) czy przetwarzane są dane osobowe szczególnej kategorii;
5) czy oceniane są czynniki osobowe, w szczególności:
   a) analizowane lub prognozowane aspekty dotyczące efektów pracy,
   b) sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań,
   c) wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
   d) przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
   e) czy przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

2. Wskazana powyżej ocena powinna określić czy naruszenie z dużym prawdopodobieństwem skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.

3. Kategorie naruszeń:

1) naruszenie ochrony danych osobowych, którego nie trzeba zgłaszać do organu nadzorczego, ponieważ jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
2) Naruszenie ochrony danych osobowych, które trzeba zgłosić do organu nadzorczego
   w ciągu 72 godzin, ale nie trzeba o nim informować osoby, której naruszenie dotyczyło – jeżeli: jest bardziej, niż „mało" prawdopodobne, że naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
3) Naruszenie ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o którym należy poinformować organ nadzorczy w ciągu 72 godzin oraz osoby, których to naruszenie może dotyczyć
   – niezwłocznie.

4. Wszystkie naruszenia ochrony danych osobowych, niezależnie od kategorii i skutku muszą zostać wpisane w wewnętrzny rejestr naruszeń, którego wzór stanowi ***Załącznik nr 11a Rejestr naruszeń bezpieczeństwa danych osobowych***. Rejestr ten prowadzony jest przez Inspektora Ochrony Danych.

§ 6. 1. W przypadku powołania zespołu doraźnego, który wyznacza Administrator w celu sprawnemu zaradzeniu skutkom naruszenia i minimalizacji skutków dla osób, których dane dotyczą jego pracą kieruje osoba wyznaczona przez Administratora.

2. Zespół z przeprowadzonych czynności sporządza protokół, w którym ujmuje skalę stwierdzonych naruszeń ochrony danych osobowych, przyczyny ich powstania oraz skutki, jakie wpłynęły lub wpłynąć mogą na stan zabezpieczenia i ochrony danych osobowych.

3. Protokół zawierać powinien wnioski określające zakres działań organizacyjnych i technicznych, zapobiegających w przyszłości naruszeniom ochrony danych osobowych.

4. Protokół przekazywany jest Administratorowi danych osobowych w celu akceptacji wniosków i zaleceń usprawniających zabezpieczenia ochrony danych.

5. Protokół przechowuje się wraz z rejestrem naruszeń bezpieczeństwa w celach kontrolnych.

6. Wzór protokołu określa ***Załącznik nr 11b Protokół stwierdzenia naruszenia ochrony danych osobowych***.

8. W przypadku stwierdzenia wystąpienia zdarzenia, które może powodować zakłócenia w funkcjonowaniu Przedszkola, Administrator przy udziale IOD wdraża procedury planu ciągłości działania lub inne działania mające na celu przywróceniu normalnego funkcjonowania jednostki.

9. Plan ciągłości działania określony został w ***Załączniku nr 11c Plan ciągłości działania.***

§ 7. 1. Nadużycie przez użytkownika postanowień niniejszej instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej, odszkodowawczej

do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Rejestr naruszeń bezpieczeństwa danych osobowych

Rejestr naruszeń bezpieczeństwa danych osobowych	
NAZWA ADMINISTRATORA	Miejski Ośrodek Kultury w Sulejowie
INSPEKTOR OCHRONY DANYCH	Aleksandra Stańczyk

Lp.	Czynność przetwarzania zgodnie z RCPD	Kategorie osób i danych osobowych (art. 6, art. 9, art. 10 RODO) oraz liczba osób, których dotyczyło naruszenie ochrony danych	Okoliczności naruszenia – opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia	Opis możliwych konsekwencji naruszenia danych osobowych	Opis środków zastosowanych lub planowanych do zastosowania przez administratora w celu ograniczenia skutków naruszenia	Czy zaistniał obowiązek zgłoszenia naruszenia do PUODO lub poinformowania osoby, której dane dotyczą. Jeśli tak - termin przekazania informacji.
1.						
2.						
3.						
4.						
5.						
6.						
7						

Załącznik nr 11b
do Polityki Ochrony Danych
Osobowych i Bezpieczeństwa Informacji

Protokół stwierdzenia naruszenia ochrony danych osobowych w Miejskim Ośrodku Kultury w Sulejowie

Działając na podstawie art. 32 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO), zespół doraźny w składzie:

1. .....
2. .....
3. .....

przeprowadził sprawdzenie systemu ochrony danych osobowych zmierzające do wyjaśnienia przyczyn oraz potencjalnych skutków zidentyfikowanego incydentu bezpieczeństwa informacji.

Realizując obowiązki wynikające z ustawy o ochronie danych osobowych oraz mając na względzie potrzebę ciągłego doskonalenia wewnętrznego systemu ochrony danych osobowych, zespół doraźny pragnie przedstawić powzięte ustalenia.

1. Przedmiot i zakres sprawdzenia:

.....
.....

2. Data rozpoczęcia i zakończenia sprawdzenia:

Data rozpoczęcia: .....
Data zakończenia: .....

3. Wykaz czynności podjętych w sprawdzeniu oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

a) .....
.....
b) .....
.....
c) .....
.....

4. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

.....
.....
.....

5. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

Stwierdzono naruszenia w zakresie:

a) .....
.....
b) .....
.....
c) .....
.....

6. Planowane lub podjęte działania przywracające stan zgodny z prawem:

Przypadek naruszenia	Status	Osoba / jednostka organizacyjna odpowiedzia-lna za ustalenie sposobu realizacji	Zakładany termin realizacji	Osoba/ jednostka organizacyjna odpowiedzia-lna za realizację rekomendacji	Zakładany termin realizacji rekomendacji	Uwagi
a) ……	Otwarte / Zamknięte					
b) ……	Otwarte / Zamknięte					
c) ……	Otwarte / Zamknięte					

7. Wnioski i zalecenia mające zapobiec w przyszłości naruszeniom ochrony danych osobowych

.....
.....
.....
.....

8. Załączniki stanowiące składową część sprawozdania:

- .....
- .....

Sporządził:

…… - członkowie zespołu
(data i podpis)

Zatwierdził:
…… - dyrektor
(data i podpis)

Załącznik nr 11c
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Plan ciągłości działania

z dnia L.p.	z dnia Funkcja	z dnia Opis działania	z dnia Potrzebne zasoby / odpowiedzialni
z dnia 1.	z dnia Zweryfikować zasadność zgłoszenia od użytkownika	z dnia Sprawdzić czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.	z dnia Zapewnić: z dnia - dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie. z dnia Odpowiedzialni IOD lub Administrator
z dnia 2.	z dnia Ustalić źródło awarii	z dnia Ustalić co jest przyczyną awarii: z dnia - przerwa w zasilaniu prądem, z dnia - brak połączenia z siecią Internet, z dnia - wadliwe działanie sprzętu,	z dnia Zapewnić: z dnia - dostęp do serwerowni oraz do sprzętu, który uległ awarii, z dnia - kontakt z osobą, która może w porze popołudniowej lub nocnej wydać klucze do pomieszczeń, z dnia - w przypadku awarii zasilania elektrycznego wezwać elektryka

		z dnia - wadliwe działanie aplikacji, z dnia - wadliwe działanie systemu, na którym uruchomiona jest aplikacja	z dnia Odpowiedzialny: Administrator
z dnia 3.	z dnia Określić skalę awarii	z dnia Ustalić, czy awaria powoduje zatrzymanie pracy: z dnia - jednego stanowiska pracy z dnia - jednego pomieszczenia pracy (np.: sala lekcyjna) z dnia - całego budynku	z dnia Zapewnić: z dnia - kontakt z kluczowymi osobami związanymi z danym pomieszczeniem z dnia Odpowiedzialny:Administrator
z dnia 4.	z dnia Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	z dnia Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchomione będą w dotychczasowej lokalizacji czy w lokalizacjach alternatywnych	z dnia Zapewnić: z dnia - możliwość uruchomienia dowolnych usług lokalizacji z dnia - infrastrukturę sieciową, zasilanie prądem z dnia Odpowiedzialni: Administrator lub IOD
z dnia 5.	z dnia Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację	z dnia W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np.: zdecydować o przeniesieniu	z dnia Zapewnić: z dnia - środki na zakup elementów niezbędnych do ponownego uruchomienia systemu z dnia Odpowiedzialni: Administrator

		aplikacji na stałe na inny komputer lub serwer	
z dnia 6.	z dnia Zweryfikować możliwość przeniesienia aplikacji na inny komputer lub serwer	z dnia Sprawdzić, czy aplikacja może być uruchomiona na którymś z działających poprawnie komputerów lub serwerów	z dnia Odpowiedzialni: Administrator
z dnia 7.	z dnia Przygotować komputer lub serwer zastępczy	z dnia Jako komputer lub serwer zastępczy można wykorzystać np.: komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na komputerze lub serwerze zastępczym należy przetestować jej działanie	z dnia Zapewnić: z dnia - maszynę dowolnego typu, która w podstawowym zakresie pozwoli na uruchomienie podstawowych usług. z dnia Odpowiedzialni: Administrator
z dnia 8.	z dnia Podjąć decyzje o terminie odtworzenia maszyny	z dnia W razie konieczności należy skontaktować się z właściwym pracownikiem korzystającym z urządzenia	z dnia Zapewnić: z dnia - kontakt z właściwym pracownikiem korzystającym z urządzenia z dnia Odpowiedzialni: Administrator
z dnia 9.	z dnia Przywrócić funkcjonowanie aplikacji / systemu	z dnia Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację	z dnia Zapewnić: z dnia - dostęp do najbardziej aktualnej wersji aplikacji z dnia - dostęp do aktualnej bazy danych kopii

		korzystając z kopii zapasowych.	z dnia Odpowiedzialni: Administrator
z dnia 10.	z dnia Sprawdzenie aplikacji / systemu	z dnia Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji / systemów zainstalowanych na komputerze lub serwerze	z dnia Odpowiedzialni Administrator lub IOD
z dnia 11.	z dnia Uruchomienie usługi w systemie informatycznym placówki	z dnia Po uruchomieniu usługi należy powiadomić, osoby korzystające z usługi	z dnia Zapewnić: z dnia - kontakt z osobami korzystającymi z usługi z dnia Odpowiedzialni: Administrator lub IOD

Załącznik nr 12
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji

Weryfikacja podmiotu przetwarzającego

Weryfikacja podmiotu przetwarzającego dane osobowe na zlecenie Miejskiego Ośrodka Kultury w Sulejowie	
NAZWA ADMINISTRATORA DANYCH OSOBOWYCH ORAZ JEGO DANE KONTAKTOWE	Miejski Ośrodek Kultury w Sulejowie adres: ul. Rynek 1, 97-330 Sulejów telefon: 513-006-574 e-mail: mok@sulejow.pl
NAZWA PODMIOTU PRZETWARZAJĄCEGO ORAZ JEGO DANE KONTAKTOWE	

Pytania wstępne			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
1.	Czy podmiot przetwarzający przyjął zatwierdzony kodeks postępowania?		
2.	Czy podmiot przetwarzający jest certyfikowany zgodnie z zatwierdzonym mechanizmem certyfikacji?		

3.	Czy podmiot przetwarzający jest certyfikowany innymi certyfikatami jakości lub w myśl norm ISO? Jeśli tak proszę podać w uwagach jaki to certyfikat.		
Organizacja wewnętrzna – osoby funkcyjne			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
4.	Czy podmiot przetwarzający wyznaczył Inspektora Ochrony Danych (IOD)?		
5.	Czy IOD został zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych?		
6.	Czy dane IOD zostały opublikowane na stronie podmiotu przetwarzającego?		
7.	Czy podmiot przetwarzający powołał lub wyznaczył inną osobę, która zajmuje się monitorowaniem przestrzegania przepisów dotyczących przetwarzania i ochrony danych osobowych?		
8.	Czy podmiot przetwarzający powołał lub wyznaczył Administratora Systemów Informatycznych (ASI) lub inną osobę, która opiekuje się infrastrukturą i siecią u podmiotu przetwarzającego z technicznego punktu widzenia?		
Zabezpieczenia organizacyjne- dokumentacja wewnętrzna			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
9.	Czy podmiot przetwarzający przeprowadził analizę ryzyka w zakresie podatności i zagrożeń związanych z wykorzystywanymi przez siebie zasobami, które będą wykorzystywane przy przetwarzaniu powierzonych danych osobowych?		
10.	Czy podmiot przetwarzający przeprowadził analizę ryzyka w zakresie zagrożeń dla praw i wolności podmiotów danych w związku z powierzanymi czynnościami?		
11.	Czy podmiot przetwarzający posiada i wdrożył polityki ochrony danych?		

12.	Czy podmiot przetwarzający posiada i wdrożył procedury postepowania w przypadku incydentów i naruszeń ochrony danych osobowych?		
13.	Czy podmiot przetwarzający posiada i wdrożył plany ciągłości działania?		
14.	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania?		
Zabezpieczenia organizacyjno-techniczne – upoważnienia i uprawnienia			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
15.	Czy osobom, które będą przetwarzały powierzone dane osobowe nadano upoważnienia do przetwarzania danych osobowych?		
16.	Czy osoby, które będą przetwarzały powierzone dane osobowe zostały przeszkolone z zakresu bezpieczeństwa informacji i danych osobowych?		
17.	Czy podmiot przetwarzający opracował i realizuje program szkoleń cyklicznych lub uzupełniających dla osób upoważnionych?		
18.	Czy osoby, które będą przetwarzały powierzone dane osobowe zostały zobowiązane do zachowania poufności tych danych, sposobów ich przetwarzania i zabezpieczenia?		
19.	Czy podmiot przetwarzający prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych?		
Zabezpieczenia organizacyjne – współpraca z podwykonawcami			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
20.	Czy podmiot przetwarzający korzysta z usług podwykonawców, którym powierza do przetwarzania dane osobowe?		
21.	Czy podmiot przetwarzający prowadzi rejestr/ewidencję podmiotów przetwarzających/dalszych podmiotów przetwarzających lub inny adekwatny dokument?		
22.	Czy podmiot przetwarzający przy wyborze swojego podwykonawcy przeprowadza działania weryfikujące, czy podwykonawca spełnia		

	wystarczające gwarancje wdrożenia odpowiednich środków zabezpieczających, by przetwarzania spełniało wymogi RODO i chroniło podmioty danych?		
23.	Czy podmiot przetwarzający przeprowadza doraźne lub bieżące audyty/kontrole swoich podwykonawców?		
Zabezpieczenia organizacyjne – zabezpieczenia fizyczne obszaru przetwarzania danych osobowych			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
24.	Czy obszar fizyczny, gdzie będą przetwarzane dane osobowe, został zabezpieczony przed dostępem osób nieuprawnionych?		
25.	Czy podmiot przetwarzający wprowadził regulacje ograniczające możliwość przebywania osób postronnych w obszarze, gdzie przetwarzane są dane osobowe?		
26.	Czy podmiot przetwarzający opracował i posiada politykę kluczy?		
27.	Czy obszar fizyczny, gdzie będą przetwarzane powierzone dane osobowe został objęty nadzorem monitoringu wizyjnego?		
28.	Czy obszar fizyczny, gdzie będą przetwarzane powierzone dane osobowe został objęty systemem alarmowym?		
29.	Czy obszar fizyczny, gdzie będą przetwarzane powierzone dane osobowe został wyposażony w systemy przeciwpożarowe?		
Zabezpieczenia organizacyjne – przechowywanie i niszczenie nośników danych			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
30.	Czy podmiot przetwarzający opracował i wdrożył zasady bezpiecznego przechowywania nośników danych osobowych?		
31.	Czy podmiot przetwarzający opracował i wdrożył politykę czystego biurka i lub czystego ekranu?		
32.	Czy podmiot przetwarzający opracował i wdrożył zasady wykonywania, przechowywania, weryfikacji i niszczenia kopii zapasowych nośników danych?		
33.	Czy podmiot przetwarzający opracował i wdrożył zasady niszczenia nośników danych osobowych?		

34.	Czy podmiot przetwarzający korzysta z usług wyspecjalizowanych podmiotów zajmujących się niszczeniem nośników zawierających dane poufne?		
Zabezpieczenia organizacyjno-techniczne – praca zdalna			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
35.	Czy podmiot przetwarzający dopuszcza pracowników do pracy zdalnej?		
36.	Czy podmiot przetwarzający opracował i wdrożył środki zabezpieczające umożliwiające prowadzenie bezpiecznej pracy zdalnej?		
Zabezpieczenia organizacyjno-techniczne – korzystanie ze sprzętu i urządzeń			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
37.	Czy podmiot przetwarzający opracował i wdrożył zasady korzystania ze sprzętu służbowego udostępnionego pracownikom?		
38.	Czy podmiot przetwarzający zezwala na wynoszenie sprzętu służbowego i/lub urządzeń przydzielanych pracownikom poza obszar przetwarzania danych osobowych?		
39.	Czy podmiot przetwarzający opracował i wdrożył zasady zabezpieczenia sprzętu służbowego i/lub urządzeń przydzielanych pracownikom wynoszonych poza obszar przetwarzania danych osobowych (np. szyfrowanie dysków)?		
40.	Czy podmiot przetwarzający pozwala na korzystanie ze służbowego sprzętu i urządzeń przydzielanych pracownikom do celów prywatnych?		
41.	Czy podmiot przetwarzający prowadzi ewidencję wydanego sprzętu służbowego i urządzeń przydzielanych pracownikom?		
42.	Czy podmiot przetwarzający zezwala na korzystanie z pendrive'ów i/lub urządzeń/dysków pamięci zewnętrznej przez pracowników?		

43.	Czy pracownicy mają możliwość instalacji własnego oprogramowania na urządzeniach/sprzęcie oddanych im w użytkowanie przez podmiot przetwarzający?		
44.	Czy podmiot przetwarzający rejestruje aktywność użytkowników sprzętu służbowego/urządzeń służbowych z wykorzystaniem tzw. Innych form monitoringu?		
Zabezpieczenia organizacyjno-techniczne – sprzęt			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
45.	Czy podmiot przetwarzający opracował i wdrożył zasady konserwacji sprzętu i urządzeń wykorzystywanych do przetwarzania danych osobowych?		
46.	Czy podmiot przetwarzający opracował i wdrożył zasady napraw w przypadku awarii lub uszkodzenia sprzętu i urządzeń wykorzystywanych do przetwarzania danych osobowych?		
47.	Czy do realizacji powyższych czynności podmiot przetwarzający korzysta z usług innych wyspecjalizowanych podmiotów?		
48.	Czy podmiot przetwarzający posiada pomieszczenie specjalne o statusie serwerowni?		
49.	Czy podmiot przetwarzający korzysta z pomieszczenia serwerowni wynajmowanego na zasadzie kolokacji od innego dostawcy?		
50.	Czy podmiot przetwarzający korzysta z serwerowni i serwera należącego do dostawcy zewnętrznego?		
51.	Czy z dostawcami usług, o których mowa powyżej zawarto umowy regulujące kwestie zabezpieczenia pomieszczenia serwerowni/ wynajmowanej powierzchni i maszyny fizycznej?		
52.	Czy podmiot przetwarzający opracował i wdrożył zasady zabezpieczenia pomieszczenia serwerowni, obejmujące zabezpieczenia środowiska serwerowni, dostępu, przeciwdziałające awarii zasilania, dostaw łącza Internet itp.		
53.	Czy maszyna fizyczna (serwer) została zabezpieczona przed nieuprawnioną ingerencją lub dostępem np. z wykorzystaniem firewall?		

54.	Czy firewall stosowany dla zabezpieczenia serwera został indywidualnie skonfigurowany (nie są wykorzystywane ustawienia defaultowe)?		
Zabezpieczenia techniczne – oprogramowanie			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
55.	Czy system operacyjny wykorzystywany na sprzęcie/urządzeniach podmiotu przetwarzającego jest regularnie aktualizowany zgodnie z zaleceniami dostawcy systemu?		
56.	Czy podmiot przetwarzający korzysta wyłącznie z oprogramowania dla którego posiada odpowiednie licencje, uprawniające do wykorzystywania oprogramowania w celach komercyjnych?		
57.	Czy na stacjach roboczych zostało zainstalowane oprogramowanie antywirusowe?		
58.	Czy wdrożono zasady dotyczące aktualizacji oprogramowania antywirusowego i baz sygnatur wirusów?		
59.	Czy wdrożono mechanizmy pozwalające na bieżącą lub doraźną weryfikację aktualności oprogramowania antywirusowego i baz sygnatur wirusów?		
60.	Czy podmiot przetwarzający korzysta z oprogramowania antyspamowego?		
61.	Czy podmiot przetwarzający korzysta z oprogramowania pozwalającego na bezpieczne przechowywanie kluczy logowania do różnych systemów przez użytkowników?		
Zabezpieczenia techniczne – sieć			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
62.	Czy podmiot przetwarzający korzysta z zapory sieciowej/firewall'a dla zabezpieczenia sieci wewnętrznej?		
63.	Czy zapora sieciowa/firewall stosowany dla zabezpieczenia sieci wewnętrznej został indywidualnie skonfigurowany (nie są stosowane ustawienia defaultowe)?		

64.	Czy podmiot przetwarzający udostępnia sieć Wi-Fi dla osób nieupoważnionych (np. gości)?		
65.	Czy oprogramowanie wykorzystywane do przetwarzania danych osobowych jest dostępne z poziomu wydzielonej sieci Wi-Fi dla osób nieupoważnionych (np. gości)?		
66.	Czy sieć wewnętrzna podmiotu przetwarzającego została zabezpieczona np. wykorzystaniem hasła lub identyfikacji MAC?		
67.	Czy podmiot przetwarzający korzysta z innych rozwiązań zabezpieczających sieć wewnętrzną przed nieuprawnioną ingerencją lub dostępem? Jeśli tak, w uwagach proszę napisać jakich.		
68.	Czy wyznaczono osobę odpowiedzialną za obserwację ruchu sieciowego lub czy opracowano i wdrożono zasady postępowania pozwalające na wykrywanie i reagowanie w przypadku peaków w ruchu sieciowym?		
Zabezpieczenia organizacyjno-techniczne – poczta elektorniczna			
Lp.	**Pytanie**	**Tak/Nie**	**Uwagi/komentarze**
69.	Czy podmiot przetwarzający opracował i wdrożył zasady korzystania z poczty elektronicznej przez pracowników?		
70.	Czy podmiot przetwarzający zezwala pracownikom na korzystanie z poczty elektronicznej do celów prywatnych		
71.	Czy podmiot przetwarzający wprowadził zabezpieczenia przed dostępem do poczty elektronicznej poza obszarem przetwarzania?		

Dodatkowe uwagi podmiotu przetwarzającego:

……
……
……

……
Podpis w imieniu Podmiotu przetwarzającego

Ocena Administratora Danych Osobowych (pozytywna/negatywna): ……
Podpis w imieniu Administratora danych osobowych……...

Załącznik nr 13

Wzór umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych,
stanowiąca uzupełnienie Umowy .....

zawarta w dniu ..... w ....., między:

..... („**Administrator**”)

a

..... („**Przetwarzający**”)

(dalej łącznie jako: „**Strony**”).

Mając na uwadze, że:
1. Administratorem danych osobowych przetwarzanych w ramach umowy powierzenia jest Miejski Ośrodek Kultury w Sulejowie.
2. Strony zawarły umowę ..... („**Umowa Podstawowa**”), w związku z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową
3. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora;
4. Strony, zawierając Umowę, dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO**.

Strony postanowiły zawrzeć Umowę o następującej treści:

1. Opis przetwarzania

1.1. Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych danych osobowych (dalej w skrócie zwanych też po prostu „**danymi**”).

1.2. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.

1.3. Charakter i cel przetwarzania wynikają z Umowy Podstawowej, w szczególności:

1.3.1. _charakter przetwarzania określony jest następującą rolą Przetwarzającego [*przykład: obsługa księgowa Administratora*],

1.3.2. _celem przetwarzania jest [*przykład: umożliwienie Administratorowi wywiązywania się z prawnych obowiązków związanych z prowadzeniem rachunkowości, a także w celu zarządzania finansowego Administratora*].

1.4. Przetwarzanie obejmować będzie następujące rodzaje danych osobowych:

Dane zwykłe:
(1) imię i nazwisko,
(2) numer ewidencyjny PESEL,
(3) adres e-mail,
(4) adres IP,
(5) numery telefonów,
(6) adres zamieszkania,
(7) data urodzenia,
(8) NIP,
(9) seria i numer dokumentu tożsamości,
(10 imiona rodziców,
(11) numer rachunku bankowego,
(12) .....

Dane szczególnych kategorii i dane karne:
(13) dokumentacja medyczna,
(14) ..... ,
(15) .....

Dane dzieci
(16) imię i nazwisko,
(17) data urodzenia,
(18) adres e-mail,
(19) pseudonim,
(20) .....

Dane nieustrukturyzowane
(21) kontent o potencjalnej i prawdopodobnej zawartości danych osobowych (wpisy, dokumenty tekstowe, obrazy, nagrania, filmy).

1.5. Przetwarzanie danych będzie dotyczyć następujących kategorii osób:
(1) pracownicy Administratora i podmiotów stowarzyszonych Administratora,
(2) klienci usługi/produktu Administratora określonych w Umowie Podstawowej,
(3) osoby, z którymi klienci Administratora wchodzą w interakcje społeczne,
(4) kontrahenci (odbiorcy i dostawcy) klientów administratora,
(5) odbiorcy korespondencji elektronicznej klientów Administratora,
(6) ..... ,
(7) ..... ,
(8) .....

2. Podpowierzenie

2.1. Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („**podpowierzenie**") w drodze pisemnej umowy podpowierzenia („**Umowa Podpowierzenia**") innym podmiotom przetwarzającym („**Podprzetwarzający**"), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

2.2. Dokonując podpowierzenia, Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

2.3. Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.

2.4. Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

3. Obowiązki Przetwarzającego

Przetwarzający ma następujące obowiązki:

3.1. Przetwarzający przetwarza dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

3.2. Przetwarzający oświadcza, że nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy – **EOG**). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

3.3. Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać dane poza EOG, informuje o tym Administratora w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

3.4. Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

3.5. Przetwarzający zapewnia ochronę danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.

3.6. Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego).

3.7. Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO (tzw. „**prawa jednostki”**). Przetwarzający oświadcza, że zapewnia obsługę praw jednostki w odniesieniu do powierzonych danych. Szczegóły obsługi praw jednostki zostaną między Stronami uzgodnione. Strony ustaliły procedurę obsługi praw jednostki odrębnym dokumentem.

3.8. Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32–36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób

dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

3.9. Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

3.10. Planując dokonanie zmian w sposobie przetwarzania danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO, i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i w takich terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych przez Przetwarzającego.

3.11. Przetwarzający zobowiązuje się do ograniczenia dostępu do danych wyłącznie do osób, których dostęp do danych jest potrzebny do realizacji Umowy i posiadających odpowiednie upoważnienie.

3.12. Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym rejestru czynności przetwarzania danych osobowych (wymóg art. 30 RODO). Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

3.13. Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

3.14. Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

4. Obowiązki Administratora

4.1. Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

5. Bezpieczeństwo danych

5.1. Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych, udostępnił ją Administratorowi i stosuje się do jej wyników co do organizacyjnych i technicznych środków ochrony danych.

5.2. Strony uzgodniły odrębnym dokumentem poziom zabezpieczeń Danych wymagany po stronie Przetwarzającego. Przetwarzający zapewnia i zobowiązuje się, że:

a) dokonał oceny przydatności pseudominizacji i szyfrowania i stosuje te techniki w takim zakresie, w jakim są potrzebne do zapewnienia poziomu bezpieczeństwa danych odpowiedniego do ustalonego ryzyka naruszenia praw lub wolności osób, przy ich przetwarzaniu

b) posiada zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności swoich systemów i usług przetwarzania;

c) posiada zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularnie testuje, mierzy i ocenia skuteczność stosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

5.3. Przetwarzający przedstawił Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obie Strony zachowują kopie przedstawionych dokumentów i dowody przedstawienia informacji dla potrzeb spełnienia wymogu rozliczalności.

6. Powiadomienie o Naruszeniach Danych Osobowych

6.1. Przetwarzający powiadamia Administratora o każdym podejrzeniu naruszenia ochrony danych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia lub jego braku.

6.2. Przetwarzający przesyła powiadomienie o stwierdzeniu naruszenia wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.

7. Nadzór

7.1. Administrator kontroluje sposób przetwarzania powierzonych danych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do:

a) wstępu do pomieszczeń, w których przetwarzane są dane, oraz

b) wglądu do dokumentacji związanej z przetwarzaniem danych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania danych oraz udostępnienia rejestrów przetwarzania (z zastrzeżeniem tajemnicy handlowej Przetwarzającego).

7.2. Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

7.3. Przetwarzający:
a) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,
b) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

8. Oświadczenia Stron

8.1. Administrator oświadcza, że jest Administratorem danych oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.

8.2. Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

8.3. Na żądanie Administratora Przetwarzający okaże Administratorowi stosowne referencje, wykaz doświadczenia, informacje finansowe lub inne dowody, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

9. Odpowiedzialność

9.1. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa.

9.2. Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

10. Okres Obowiązywania Umowy Powierzenia

10.1. Umowa została zawarta na czas obowiązywania Umowy Podstawowej z zastrzeżeniem terminu karencji usunięcia danych wskazanego w kolejnym artykule Umowy.

11. Usunięcie danych

11.1. Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych danych i jest zobowiązany do:

a) usunięcia danych i poinformowania Administratora na piśmie o dacie i sposobie, w jaki usunięto dane,

b) usunięcia wszelkich istniejących kopii lub zwrotu danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie danych,

11.2. Przetwarzający dokona usunięcia Danych po upływie …… dni od zakończenia Umowy Podstawowej, chyba że Administrator poleci mu to uczynić wcześniej.

12. Postanowienia końcowe

12.1. W razie sprzeczności między postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych między Administratorem a

Przetwarzającym należy regulować przez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

12.2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

12.3. Umowa podlega RODO oraz prawu polskiemu.

....

Administrator Przetwarzający