ZARZĄDZENIE NR 175/2019

Burmistrza Miasta Augustowa

z dnia 30 maja 2019 r.

w sprawie aktualizacji Polityki ochrony danych osobowych w Urzędzie Miejskim w Augustowie

Na podstawie art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27 kwietnia 2016 roku 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. U. UE L. 206. 119. 1) (dalej jako „RODO) zarządza się, co następuje:

§ 1.

Aktualizuje się Politykę ochrony danych osobowych w Urzędzie Miejskim w Augustowie do wymogów RODO, ustawy o ochronie danych osobowych z dn. 10 maja 2018 r. oraz ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO.

§ 2.

Polityka ochrony danych osobowych ma zastosowanie w Urzędzie Miejskim w Augustowie do wszystkich stanowisk pracy, gdzie przetwarzane są dane osobowe.

§3.

Z treścią Polityki ochrony danych osobowych zobowiązani są zapoznać się wszyscy pracownicy Urzędu Miejskiego w Augustowie przetwarzający dane osobowe.

§ 4.

Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Augustowie do przestrzegania zasad wynikających z Polityki ochrony danych osobowych.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Mirosław Karolczuk

Polityka ochrony danych osobowych w Urzędzie Miejskim w Augustowie

z siedzibą przy ul. 3 Maja 60, 16-300 Augustów

Spis treści

Zakres i podstawa stosowania

Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" (dalej: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Urzędzie Miejskim w Augustowie (dalej: Urząd lub Administrator).
Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia 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).
Bezpieczeństwo danych osobowych ma na celu zapewnienie ich poufności, dostępności, integralności oraz rozliczalności, poprzez wdrożenie niezbędnych do tego celu środków technicznych i organizacyjnych.

Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie procesy i czynności przetwarzania danych zarówno w formie elektronicznej jak i papierowej.

Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby, przy pomocy których administrator danych wykonuje swoje czynności, mające dostęp do danych osobowych. Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.

Zawartość

Polityka zawiera:
a) opis zasad ochrony danych obowiązujących w Urzędzie,
b) odwołania do załączników uszczegóławiających.

Odpowiedzialność

§ 1

Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Administrator, tj. Burmistrz Miasta Augustowa.

§ 2

Odpowiedzialnymi za nadzór i monitorowanie przestrzegania Polityki są Inspektor Ochrony Danych (dalej: IOD) oraz Administrator Systemów Informatycznych (dalej: ASI).

§ 3

Odpowiedzialnymi za stosowanie niniejszej Polityki są wszyscy pracownicy Urzędu w zakresie powierzonych im obowiązków, uprawnień, odpowiedzialności, upoważnień i pełnomocnictw.

§ 4

Urząd zapewnia zgodność postępowania kontrahentów Urzędu z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Urząd.

Skróty i definicje

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

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).

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane szczególne oznaczają 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.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 16 roku życia.

Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Administrator oznacza osobę kierownika Urzędu, który samodzielnie lub wspólnie z innymi administratorami ustala cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający oznacza organizację lub osobę, której Urząd powierzył przetwarzanie danych osobowych (np. zewnętrzna obsługa BHP, usługodawca IT).

Profilowanie 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.

Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD lub **Inspektor** oznacza Inspektora Danych Osobowych.

RDCP lub **Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Organ nadzorczy oznacza Prezesa Urzędu Ochrony Danych Osobowych („PUODO”).

Ochrona danych osobowych w Urzędzie – zasady ogólne

§ 1

Ochrona danych w Urzędzie oparta jest o:

1) Legalność – Urząd dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
2) Bezpieczeństwo – Urząd zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
3) Prawa jednostki – Urząd umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4) Rozliczalność – Urząd dokumentuje to, w jaki sposób spełnia obowiązek, aby w każdej chwili móc wykazać zgodność.

§ 2

Zasady ochrony danych w Urzędzie:

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).

§ 3

System ochrony danych osobowych w Urzędzie składa się z następujących elementów:

1) **Inwentaryzacja danych**. Urząd dokonuje identyfikacji zasobów danych osobowych w Urzędzie, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym:
a) przypadków przetwarzania danych zwykłych, danych szczególnych i danych karnych,
b) przypadków przetwarzania danych osób, których Urząd nie identyfikuje (dane niezidentyfikowane),
c) przypadków przetwarzania danych dzieci,
d) profilowania,
e) współadministrowania danymi.

2) **Rejestr**. Urząd opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w Urzędzie. Rejestr jest narzędziem rozliczania zgodności ochrony danych w Urzędzie.

3) **Podstawy prawne**. Urząd zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
b) Inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Urząd przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora lub osoby, której dane osobowe dotyczą.

4) **Obsługa praw jednostki**. Urząd spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
a) ***obowiązki informacyjne***. Urząd przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków,
b) ***możliwość wykonania żądań***. Urząd weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających,
c) ***obsługa żądań***. Urząd zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i udokumentowane,
d) ***zawiadamianie o naruszeniach***. Urząd stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych oraz Prezesa Urzędu Ochrony Danych Osobowych.

5) **Minimalizacja**. Urząd posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:
a) zasady zarządzania adekwatnością danych,
b) zasady reglamentacji i zarządzania dostępem do danych,
c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

6) **Bezpieczeństwo**. Urząd zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii,
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,

d) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych w ramach zarządzania incydentami.

7) **Przetwarzający**. Urząd posiada zasady doboru przetwarzających dane na rzecz Urzędu, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8) **Eksport danych**. Urząd posiada zasady weryfikacji, czy Urząd nie przekazuje danych do państw trzecich lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

9) **Privacy by design**. Urząd zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w Urzędzie 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.

10) **Przetwarzanie transgraniczne**. Urząd posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

Inwentaryzacja

6.1 Dane zwykłe, dane szczególne i dane karne

Urząd identyfikuje przypadki, w których przetwarza lub może przetwarzać dane zwykłe, dane szczególne lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. Przetwarzanie danych zwykłych oparte jest o podstawy wskazane w art. 6 RODO. W chwili zidentyfikowania przypadku przetwarzania danych szczególnych lub danych karnych Urząd postępuje zgodnie z przyjętymi przepisami prawa zasadami w tym zakresie lub w szczególnych przypadkach w oparciu o zgodę osoby na przetwarzanie takich danych. Całość procesu przetwarzania opiera się o przesłanki określone w art. 9 ust. 2 i art. 10 RODO.

6.2 Dane niezidentyfikowane

Urząd identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane. Do głównych procesów przetwarzania danych niezidentyfikowanych dochodzi w ramach stosowanego monitoringu wizyjnego, którego reguły działania ustala odrębna instrukcja postępowania dostępna na stronie Urzędu oraz w miejscach oznaczonych tabliczką informującą o objęciu terenu czy pomieszczeń monitorowaniem.

6.3 Profilowanie

Urząd identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Urząd postępuje zgodnie z przyjętymi zasadami w tym zakresie. Profilowanie odbywa się wyłącznie po wyczerpaniu przynajmniej jednej z przesłanek art. 22 ust. 2 RODO.

6.4 Współadministrowanie

Urząd 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 wg 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.

Rejestr czynności przetwarzania danych osobowych

§ 1

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.

§ 2

Urząd prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane.

§ 3

Rejestr jest jednym z podstawowych narzędzi umożliwiających Urzędowi rozliczanie większości obowiązków ochrony danych.

§ 4

W Rejestrze dla każdej czynności przetwarzania danych, którą Urząd uzna za odrębną dla potrzeb Rejestru, Urząd odnotowuje co najmniej:
1) Nazwę czynności.
2) Cel przetwarzania.
3) Kategorię osób.
4) Kategorię danych.
5) Podstawę prawną przetwarzania.
6) Źródło danych.
7) Planowany termin usunięcia danych.
8) Nazwę współadministratora i dane kontaktowe.
9) Nazwę podmiotu przetwarzającego i dane kontaktowe.
10) Kategorię odbiorców.
11) Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
12) Informację o przekazaniu danych poza EU/EOG.

§ 5

Wzór Rejestru stanowi ***Załącznik nr 1 Rejestr Czynności Przetwarzania Danych.*** Rejestr ma formę pisemną, w tym formę elektroniczną. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Urząd rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

§ 6

Prowadzenie Rejestru powierza się IOD, który dokonuje wpisów aktualizacyjnych na wniosek ze strony pracownika Urzędu, który zamierza podjąć przetwarzanie danych w ramach nowego procesu czy nowej kategorii danych. Pracownik Urzędu jest zobligowany do niezwłocznego złożenia takiego wniosku do IOD po uzyskaniu informacji o zmianach na swoim stanowisku pracy w związku z przetwarzaniem danych. Zmiany takie mogą być wymuszone w szczególności nowymi aktami prawa pociągającymi za sobą konieczność realizacji nowych zadań w tym związanych z przetwarzaniem danych.

§ 7

Załącznik nr 2 Wniosek o wpis aktualizacyjny do RCPD określa zakres minimalny informacji zamieszczanych we wniosku. Wnioski oraz Rejestr przechowuje się wraz z całością dokumentacji wymienionej w Polityce do wglądu dla pracowników Urzędu, kontrolerów Urzędu Ochrony danych Osobowych oraz w uzasadnionych przypadkach do wiedzy osób wnioskujących o taki wgląd.

§ 8

Jeżeli przetwarzanie odbywa się zgodnie z art. 28 RODO, na zlecenie innego administratora, prowadzony jest rejestr wszystkich kategorii czynności przetwarzania ewidencjonowany na rzecz każdego z administratorów zgodnie z ***Załącznikiem nr 3 Rejestr Kategorii Czynności Przetwarzania Danych***.

Podstawy przetwarzania

§ 1

Urząd dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Urzędu), Urząd dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Przy zgodzie – wskazując jej zakres; gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty np. umowę, porozumienie administracyjne; żywotne interesy – wskazując kategorie zdarzeń, w których się zmaterializują; uzasadniony cel – wskazując konkretny cel, np. dochodzenie roszczeń.

§ 2

Urząd 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.).

§ 3

Zgody stanowią część akt spraw i jako takie podlegają nadzorowi. ***Załącznik nr 4 Zgoda na przetwarzanie danych*** 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.

§ 4

Każdy pracownik Urzędu przetwarzając dane osobowe ma obowiązek znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Urzędu, pracownik ma obowiązek znać konkretny realizowany przetwarzaniem interes Urzędu.

Sposób obsługi praw osób i obowiązków informacyjnych

§ 1

Urząd dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

§ 2

Urząd ułatwia osobom korzystanie z praw poprzez różne działania, w tym zamieszczenie na stronie internetowej urzędu oraz siedzibie urzędu i dokumentach, informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Urzędzie, w tym wymaganiach dotyczących identyfikacji oraz metodach kontaktu z Urzędem w tym celu.

§ 3

Osoba w celu realizacji swoich praw składa pisemny wniosek wskazując osobę, której dane dotyczą oraz żądanie zgodnie z ***Załącznikiem nr 5 Wniosek - prawa osób, których dane dotyczą***.

§ 4

W przypadku uznania żądania za ewidentnie 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.

§ 5

Urząd dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

§ 6

Urząd wprowadza adekwatne metody identyfikacji i uwierzytelnienia osób dla potrzeb realizacji praw osoby i obowiązków informacyjnych. Podstawowym narzędziem identyfikacji i uwierzytelnienia jest wgląd do dokumentu tożsamości osoby, której dane dotyczą, a na rzecz której to osoby ma nastąpić realizacja jej praw i obowiązków informacyjnych. Urząd prowadzi rejestr żądań w formie papierowej lub elektronicznej zgodnie z ***Załącznikiem nr 6 Rejestr żądań***.

§7

W celu realizacji praw osoby Urząd zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Urząd, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany. Mechanizmy te w szczególności określa dokumentacja techniczna czy podręcznik użytkownika każdego z systemów elektronicznego przetwarzania danych.

Obowiązki informacyjne

§ 1

Urząd określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

§ 2

Urząd informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

§ 3

Urząd informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby. Udostępnia się osobie treść klauzuli informacyjnej m.in. bezpośrednio w Urzędzie w miejscu uzyskania danych od osoby (stanowisko obsługi interesanta), drogą komunikacji na odległość (e-mail, telefon) i na stronie internetowej Urzędu. ***Załącznik nr 7 Ogólna Klauzula Informacyjna*** określa zawartość merytoryczną dostępną dla osoby, od której bezpośrednio zbiera się dane osobowe.

§ 4

Urząd nie informuje osoby o przetwarzaniu jej danych, przy pozyskaniu danych o tej osobie niebezpośrednio od niej, jeśli 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.

§ 5

Urząd określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka informująca o objęciu obszaru monitoringiem wizyjnym).

§ 6

Urząd informuje osobę o planowanej zmianie celu przetwarzania danych.

§ 7

Urząd informuje osobę przed uchyleniem ograniczenia przetwarzania danych.

§ 8

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

§ 9

Urząd bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko praw lub wolności tej osoby.

Żądania osób

11.1 Prawa osób trzecich

Realizując prawa osób, której dane dotyczą, Urząd 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 handlową, dobra osobiste), Urząd może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

11.2 Nieprzetwarzanie

Urząd informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

11.3 Odmowa

Urząd informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia i o prawach osoby z tym związanych.

11.4 Dostęp do danych

Na żądanie osoby dotyczące dostępu do jej danych Urząd 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. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Urząd nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

11.5 Kopie danych

Na żądanie Urząd wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Urząd wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowania jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

11.6 Sprostowanie danych

Urząd dokonuje sprostowania danych na żądanie osoby. Urząd ma prawo odmówić sprostowania, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.

11.7 Uzupełnienie danych

Urząd uzupełnia i aktualizuje dane na żądanie osoby. Urząd ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Urząd nie musi przetwarzać danych, które są Urzędowi zbędne). Urząd może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych

przez Urząd procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11.8 Usunięcie danych

Na żądanie osoby Urząd usuwa dane, gdy:
a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
b) zgoda na ich przetwarzanie została cofnięta a nie ma innej podstawy prawnej przetwarzania,
c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
d) dane były przetwarzane niezgodnie z prawem,
e) konieczność usunięcia wynika z obowiązku prawnego,
f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. udział w konkursie na stronie internetowej).

Urząd 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:
a) jeżeli przetwarzanie danych jest konieczne do korzystania z prawa do wolności wypowiedzi i informacji,
b) jeżeli przetwarzanie danych jest konieczne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa,
c) jeżeli przetwarzanie danych jest konieczne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
d) jeżeli przetwarzanie danych jest istotne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
e) jeżeli przetwarzanie danych jest konieczne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych,
f) jeżeli przetwarzanie danych jest konieczne do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Urząd, Urząd podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Urząd informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.9 Ograniczenie przetwarzania

Urząd dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich stosowania,
c) Urząd nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
d) Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Urzędu zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu. W trakcie ograniczenia przetwarzania Urząd przechowuje dane, natomiast nie przetwarza ich (ni 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. Urząd informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Urząd informuje osobę o odbiorcach danych, na żądanie tej osoby.

11.10 Przenoszenie danych

Na żądanie osoby Urząd 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 Urzędowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Urzędu.

11.11 Sprzeciw w szczególnej sytuacji

Jeżeli osoba zgłosi umotywowany jej szczególna sytuacją sprzeciw względem przetwarzania jej danych, a dane są przetwarzane przez Urząd w oparciu o uzasadniony interes Urzędu lub o powierzone Urzędowi zadanie w interesie publicznym, Urząd uwzględni sprzeciw, o ile nie zachodzą po stronie Urzędu ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

11.12 Sprzeciw przy celach statystycznych

Jeżeli Urząd przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Urząd uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

11.13 Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu

Jeżeli Urząd 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 , Urząd zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Urzędu, chyba że taka automatyczna decyzja:
a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Urzędem,
b) jest wprost dozwolona przepisami prawa,
c) opiera się na wyraźnej zgodzie osoby odwołującej się.

Minimalizacja

Urząd dba o minimalizację przetwarzania danych pod kątem:
a) adekwatności danych do celów (ilość danych i zakresu przetwarzana),
b) dostępu do danych,
c) czasu przechowywania danych.

12.1 Minimalizacja zakresu

Urząd zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach RODO.

12.2 Minimalizacja dostępu

Urząd 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. Urząd stosuje kontrolę dostępu fizycznego, m.in. poprzez ograniczenie dostępu do pomieszczeń serwerowni czy archiwum zakładowego. Urząd 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. Urząd dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż na raz na rok. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w ***Załączniku nr 8 do Polityki – Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji.***

12.3 Minimalizacja czasu

Urząd wdraża mechanizmy kontroli cyklu życia danych osobowych w Urzędzie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów informatycznych Urzędu, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się w kopiach zapasowych systemów i informacji przetwarzanych przez Urząd. 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

Urząd zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Urząd.

13.1 Analiza ryzyka i adekwatność środków bezpieczeństwa.

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

Urząd 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. Analiza ryzyka jest wykonywana przy udziale IOD oraz ASI.

Szacowanie ryzyka przeprowadzane jest z uwzględnieniem potencjalnych skutków naruszenia praw lub wolności osób, których dane osobowe są przetwarzane w ramach prowadzonej działalności. Metodyka szacowania ryzyka opisana jest w ***Załączniku nr 14 Metodyka szacowania ryzyka.***
Analiza ryzyka dla czynności przetwarzania danych lub ich kategorii jest dokumentowana w ***Załączniku nr 15 Analiza ryzyka.***

13.2 Ocena skutków dla ochrony danych

Urząd dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. Urząd przeprowadza ocenę skutków planowanych operacji przetwarzania niezależnie od wyników analizy ryzyka jeśli:
a) proces przetwarzania danych opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej,
b) proces przetwarzania danych odnosi się do przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych karnych;
c) proces przetwarzania danych odbywa się z wykorzystaniem systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Urząd stosuje metodykę oceny skutków przyjętą w ***Załączniku nr 16 Ocena skutków dla ochrony danych*** i z wykorzystaniem tego załącznika dokumentuje przeprowadzenie oceny skutków. Ocena skutków przetwarzania danych jest wykonywana przy udziale IOD oraz ASI, którzy tworzą zespół oceniający. 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. Wskazanie przez zespół oceniający skutki 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) zespół mnożące je przez siebie otrzymuje skalę powagi ryzyka, gdzie:
a) wartość od 1 do 3 oznacza ***niską powagę***,
b) wartość od 4 do 8 oznacza ***średnią powagę***,
c) wartość od 9 do 18 oznacza ***wysoką powagę***.

Stwierdzenie ***niskiej powagi*** umożliwia zespołowi oceniającemu skutki przetwarzania wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka.
Stwierdzenie ***średniej powagi*** umożliwia zespołowi oceniającemu skutki przetwarzania wybór planu reakcji na ryzyko w oparciu o monitorowanie ryzyka oraz działanie obniżające przynajmniej jedną z maksymalnych wartości (P), (I), (R).
Stwierdzenie ***wysokiej powagi*** umożliwia zespołowi oceniającemu skutki przetwarzania 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).

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

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.

13.3 Środki bezpieczeństwa

Urząd stosuje środki bezpieczeństwa ustalone w ramach analizy ryzyka i adekwatności środków bezpieczeństwa oraz oceny skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Urzędzie i są bliżej opisane w procedurach przyjętych przez Urząd dla tych obszarów.

13.4 Audyt systemu ochrony danych

Zgodnie z art. 32 RODO Urząd ocenia skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania poprzez wykonywanie planowych audytów zgodności przetwarzania danych z przepisami. Audyty są wykonywane przez IOD lub zespół powołany przez ADO w obszarach, w których występują wątpliwości co do skuteczności ochrony danych. Zakres obszarów podlegających sprawdzeniu zawarty jest w ***Załączniku nr 17 Audyt systemu ochrony danych***.

13.5 Zgłaszanie naruszeń

Urząd 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.
Urząd w celu wypełnienia obowiązków spoczywających na administratorze wprowadza instrukcję postępowania w przypadku wystąpienia naruszenia jako ***Załącznik nr 18 Instrukcja postępowania przy naruszeniu danych.***
W celu udokumentowania nadzoru nad zgłaszaniem naruszeń ochrony danych w Urzędzie stosuje się ***Załącznik nr 19 Rejestr naruszeń bezpieczeństwa***. Zgłoszenie naruszenia do PUODO odbywa się poprzez interaktywny formularz dostępny na oficjalnej stronie organu nadzorczego www.uodo.gov.pl.

Przetwarzający

§ 1

Urząd posiada zasady doboru i weryfikacji przetwarzających dane na rzecz Urzędu 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 Urzędzie.

§ 2

Urząd przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące ***Załącznik nr 21 Wzór umowy powierzenia przetwarzania danych***, a każda umowa jest odnotowana w ***Załączniku nr 22 Rejestr umów powierzenia przetwarzania danych osobowych***.

§ 3

Proces do realizacji i nadzoru powierzono IOD, a każdy pracownik Urzędu, który zamierza zawrzeć z podmiotem zewnętrznym umowę skutkującą powierzeniem danych powinien powiadomić o tym fakcie IOD, który opiniuje treść umowy powierzenia przetwarzania danych, a po jej podpisaniu odnotowuje ją w ewidencji umów powierzenia.

§ 4

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

Eksport danych

Urząd rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Urząd okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodnie z prawem ochrony danych rozwiązania równoważne.

Projektowanie prywatności

Urząd 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 Urząd 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.

Załączniki

Załącznik nr 1 Rejestr Czynności Przetwarzania Danych
Załącznik nr 2 Wniosek o wpisanie czynności do RCPD
Załącznik nr 3 Rejestr Kategorii Czynności Przetwarzania Danych
Załącznik nr 4 Zgoda na przetwarzanie danych
Załącznik nr 5 Wniosek o realizację praw osób, których dane dotyczą
Załącznik nr 6 Rejestr żądań
Załącznik nr 7 Ogólna Klauzula Informacyjna
Załącznik nr 8 Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji
Załącznik nr 9 Upoważnienie do przetwarzania danych osobowych
Załącznik nr 10 Wniosek o nadanie / cofnięcie upoważnienia do przetwarzania danych osobowych
Załącznik nr 11 Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 12 Wniosek o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym
Załącznik nr 13 Klauzula poufności
Załącznik nr 14 Metodyka szacowania ryzyka
Załącznik nr 15 Analiza ryzyka
Załącznik nr 16 Ocena skutków dla ochrony danych
Załącznik nr 17 Audyt systemu ochrony danych
Załącznik nr 18 Instrukcja postępowania przy naruszeniu danych
Załącznik nr 19 Rejestr naruszeń bezpieczeństwa
Załącznik nr 20 Protokół sprawdzenia ochrony danych
Załącznik nr 21 Wzór umowy powierzenia przetwarzania danych
Załącznik nr 22 Ewidencja umów powierzenia przetwarzania danych osobowych

Załącznik nr 1
Rejestr Czynności Przetwarzania Danych

***Kolorem niebieskim oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO**

	1	2	3	4	5	6	8	9
LP.	**Nazwa czynności przetwarzania**	**Jednostka organizacyjna (departament, dział itp.)**	**Cel przetwarzania**	**Kategorie osób**	**Kategorie danych**	**Podstawa prawna**	**Planowany termin usunięcia kategorii danych** *(jeżeli jest to możliwe)*	**Nazwa współadministratora i dane kontaktowe** *(jeśli dotyczy)*
			Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**		**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt a**
1								

10	11	12	13	14	15	16
Nazwa podmiotu przetwarzajacego i dane kontakowe *(jeśli dotyczy)*	**Kategorie odbiorców** *(innych niż podmiot przetwarzajacy)*	**Nazwa systemu lub oprogramowania**	**Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1** ***(jeżeli jest to możliwe)***	**DPIA (jeśli tak, lokalizacja raportu)**	Transfer do kraju trzeciego lub org. międzynarodowej	
					Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	**Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**
Art.. 30 ust. 1 pkt d	**Art.. 30 ust. 1 pkt d**		**Art.. 30 ust. 1 pkt g**		**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**

Załącznik nr 2
Wniosek o wpis do RCPD

Augustów, dn. ……

Wniosek o wpis do RCPD

Wnoszę o **wpisanie / usunięcie / aktualizację*** czynności przetwarzania danych do RCPD.

……
Nazwa czynności przetwarzania danych

……
Jednostka organizacyjna (wydział, dział, stanowisko itp.)

……
Cel przetwarzania

……
Kategorie osób

……
Kategorie danych

……
Podstawa prawna

……
Źródło danych

……
Planowany termin podjęcia oraz usunięcia przetwarzania kategorii danych

……
Informacja o współadministratorach, podmiotach przetwarzających i możliwych odbiorcach (jeśli dotyczy)

……
Opis środków technicznych i organizacyjnych środków bezpieczeństwa

……
Informacja o przekazaniu danych poza EU/EOG

……
Data i podpis wnioskującego

***Niepotrzebne skreślić**

Zarządzenie nr 3
Załącznik nr 3 Rejestr Kategorii Czynności Przetwarzania Danych

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

	1	2	3	4	5	6
LP.	**Kategorie przetwarzań**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)**	**Administrator**			
			Nazwa i dane kontaktowe administratora	**Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)**	**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			

7	8	9	10	11
Czas trwania przetwarzania	**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**	**Podprzetwarzający (podwykonawca) - jeśli dotyczy**	
			Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	**Kategorie podpowierzonych przetwarzań**
	Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		

Załącznik nr 4
Zgoda na przetwarzanie danych

Augustów, dn. ……

Zgoda na przetwarzanie danych osobowych

Ja, niżej podpisany zostałem poinformowany 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 przez Administratora danych:

Burmistrza Miasta Augustowa – kierownika Urzędu Miejskiego w Augustowie z siedzibą przy ul. 3 Maja 60, 16-300 Augustów

w celu
……
……
poniżej wymienionych moich danych osobowych
……
……
i poświadczam ten fakt własnoręcznym podpisem pod klauzulą „Wyrażam zgodę na przetwarzanie danych".

Oświadczam, że zapoznałem się z treścią klauzuli informacyjnej o przetwarzaniu danych osobowych umieszczonej na drugiej stronie druku niniejszej zgody.

Wyrażam zgodę na przetwarzanie danych

……..
Data i własnoręczny podpis

Cofam zgodę na przetwarzanie danych

……
Data i własnoręczny podpis

Załącznik nr 4
Zgoda na przetwarzanie danych

KLAUZULA INFORMACYJNA O PRZETWARZANIU DANYCH OSOBOWYCH

W związku z wejściem w życie w dniu 25 maja 2018 roku 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 (określane jako „RODO") informujemy o zasadach przetwarzania Państwa danych osobowych.

1) Informujemy, że Administratorem Państwa danych osobowych przetwarzanych w Urzędzie Miejskim w Augustowie jest Burmistrz Miasta Augustowa. Siedziba Administratora znajduje się przy ul. 3 Maja 60, 16-300 Augustów. Kontakt z Administratorem jest możliwy pod numerem tel. 87 643 42 10 lub mailowo urząd.miejski@urzad.augustow.pl.
Burmistrz Miasta Augustowa reprezentuje Miasto i jest kierownikiem Urzędu Miejskiego w Augustowie.
2) Kontakt do inspektora ochrony danych, e-mail iod@urzad.augustow.pl
3) Pani/Pana dane osobowe będą przetwarzane w celu umożliwienia kontaktu oraz realizacji spraw, które zostały zgłoszone Administratorowi na podstawie udzielonej zgody z art. 6 ust. 1 lit. a RODO.
4) ADO przetwarza Państwa dane osobowe w ściśle określonym, minimalnym zakresie niezbędnym do osiągnięcia celu, o którym mowa powyżej. W szczególnych sytuacjach ADO może przekazać/powierzyć Państwa dane innym podmiotom. Podstawą przekazania/powierzenia danych są przepisy prawa lub właściwie skonstruowane, zapewniające bezpieczeństwo danym osobowym, umowy powierzenia danych do przetwarzania (np. z podmiotami sektora teleinformatycznego i telekomunikacyjnego).
5) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.
6) Dane osobowe przetwarzane w Urzędzie Miejskim w Augustowie przechowywane będą przez okres niezbędny do realizacji celu dla jakiego zostały zebrane lub do wycofania zgody.
7) Każda osoba w stosunku do danych osobowych pobranych za zgodą ma możliwość:
- dostępu do danych osobowych jej dotyczących,
- żądania ich sprostowania,
- usunięcia lub ograniczenia przetwarzania,
- wniesienia sprzeciwu wobec przetwarzania.
8) Osoba której dane przetwarzane są na podstawie zgody wyrażonej przez tę osobę ma prawo do cofnięcia tej zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
9) Przysługuje Państwu prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO (ul. Stawki 2, 00-193 Warszawa)
10) Podanie danych ma charakter dobrowolny, a ich niepodanie może skutkować brakiem realizacji celu określonego w zgodzie.

Wniosek o realizację praw osób, których dane dotyczą

Dane osoby wnioskującej:	**Dane osoby, której dane dotyczą (jeżeli inne niż wnioskodawcy):**
…… (imię i nazwisko)	**……** (imię i nazwisko)
…… (adres zamieszkania)	**……** (adres zamieszkania)

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

***niepotrzebne skreślić**

☐ 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
w imieniu Urzędu Miejskiego w Augustowie

……..
Data i podpis osoby wnioskującej

Załącznik nr 6
Rejestr żądań

Rejestr żądań - wniosków o realizację praw osób, których dane dotyczą					
NAZWA ADMINISTRATORA	Burmistrz Miasta Augustowa – kierownik Urzędu Miejskiego w Augustowie				
DANE INSPEKTORA OCHRONY DANYCH	Robert Stańczyk				
Data przyjęcia wniosku	**Imię i nazwisko osoby wnioskującej**	**Imię i nazwisko osoby, której dane dotyczą (jeśli inne niż osoby wnioskującej)**	**Podstawa prawna (art.15-22 RODO)**	**UWAGI**	**Termin oraz sposób realizacji**

Załącznik nr 7
Ogólna Klauzula Informacyjna

KLAUZULA INFORMACYJNA O PRZETWARZANIU DANYCH OSOBOWYCH

W związku z wejściem w życie w dniu 25 maja 2018 roku 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 (określane jako „RODO") informujemy o zasadach przetwarzania Państwa danych osobowych.

1) W związku z zapisami art. 13 oraz art. 14 RODO informujemy, że Administratorem Państwa danych osobowych (dalej również jako „ADO") przetwarzanych w Urzędzie Miejskim w Augustowie jest

Burmistrz Miasta Augustowa
ul. 3 Maja 60
16 – 300 Augustów

Burmistrz Miasta Augustowa reprezentuje Miasto i jest kierownikiem Urzędu Miejskiego w Augustowie.

2) Kontakt do inspektora ochrony danych, e-mail iod@urzad.augustow.pl

3) Do zakresu działania samorządu należy wykonywanie zadań publicznych o charakterze gminnym, niezastrzeżonych ustawami na rzecz organów administracji rządowej. Urząd Miejski w Augustowie gromadzi Państwa dane w celu realizacji zadań wynikających z przepisów prawa, a w szczególności z ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2018 r., poz. 130). Podstawa prawna przetwarzania Państwa danych wynika z szeregu ustaw dziedzinowych (sektorowych) oraz obowiązków i zadań zleconych przez instytucje nadrzędne wobec ADO.

4) ADO przetwarza Państwa dane osobowe w ściśle określonym, minimalnym zakresie niezbędnym do osiągnięcia celu, o którym mowa powyżej. W szczególnych sytuacjach ADO może przekazać/powierzyć Państwa dane innym podmiotom. Podstawą przekazania/powierzenia danych są przepisy prawa (np. wymiar sprawiedliwości, administracja skarbowa, instytucje związane z obsługą szeroko pojętych funduszy unijnych, podmioty związane z obsługą sfery socjalnej – ZUS, PFRON) lub właściwie skonstruowane, zapewniające bezpieczeństwo danym osobowym, umowy powierzenia danych do przetwarzania (np. z podmiotami sektora teleinformatycznego i telekomunikacyjnego).

5) Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

6) Dane osobowe przetwarzane w Urzędzie Miejskim w Augustowie przechowywane będą przez okres niezbędny do realizacji celu dla jakiego zostały zebrane oraz zgodnie z terminami archiwizacji określonymi przez ustawy kompetencyjne lub ustawę z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2017 r., poz. 1257) i ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2018 r., poz. 217), w tym Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

7) Każda osoba, z wyjątkami zastrzeżonymi przepisami prawa, ma możliwość:
- dostępu do danych osobowych jej dotyczących,
- żądania ich sprostowania,
- usunięcia lub ograniczenia przetwarzania,
- wniesienia sprzeciwu wobec przetwarzania.

8) Osoba której dane przetwarzane są na podstawie zgody wyrażonej przez tę osobę ma prawo do cofnięcia tej zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

9) Przysługuje Państwu prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (ul. Stawki 2, 00-193 Warszawa)

10) W zależności od sfery, w której przetwarzane są dane osobowe w Urzędzie Miejskim w Augustowie, podanie danych osobowych jest wymogiem ustawowym lub umownym. W szczególnych przypadkach ich podanie jest warunkiem zawarcia umowy. O szczegółach podstawy gromadzenia danych osobowych i ewentualnym obowiązku lub dobrowolności ich podania oraz potencjalnych konsekwencjach niepodania danych, informowani Państwo będziecie przez referat merytoryczny/stanowisko załatwiające poszczególne sprawy w Urzędzie Miejskim w Augustowie.

PROCEDURY BEZPIECZEŃSTWA FIZYCZNEGO I BEZPIECZEŃSTWA INFORMACJI

Spis treści

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. Wniosek o wydanie upoważnienia jest kierowany do Inspektora Ochrony Danych (IOD) przez przełożonego osoby, która powinna uzyskać upoważnienie lub w przypadku osób pracujących na samodzielnym stanowisku na wniosek zainteresowanego. IOD przygotowuje treść upoważnienia w dwóch egzemplarzach do zaopiniowania i podpisu Administratorowi. Po akceptacji Administratora, IOD przekazuje upoważnienia pracownikowi do podpisu potwierdzającego odbiór upoważnienia. Jeden egzemplarz zostaje w dokumentacji Administratora dla potwierdzenia zgodności z przepisami o ochronie danych osobowych. Drugi egzemplarz upoważnienia IOD przekazuje pracownikowi. Fakt wydania upoważnienia IOD odnotowuje w ewidencji osób upoważnionych. ***Załącznik nr 9 Upoważnienie do przetwarzania danych osobowych*** określa treść upoważnienia. Na zasadach opisanych powyżej następuje cofnięcie upoważnienia lub jego rozszerzenie. Druk wzoru wniosku o wydanie upoważnienia określa ***Załącznik nr 10 Wniosek o nadanie, cofnięcie upoważnienia do przetwarzania danych osobowych***, a ***Załącznik nr 11 Ewidencja osób upoważnionych do przetwarzania danych osobowych*** określa zakres informacji ujętych w ewidencji.
2. 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. Wniosek o wydanie uprawnienia jest kierowany do Administratora przez przełożonego osoby, która powinna uzyskać uprawnienie pracy w systemie informatycznym lub w przypadku osób pracujących na samodzielnym stanowisku na wniosek zainteresowanego. Po akceptacji Administratora wniosek przekazywany jest do Administratora Systemów Informatycznych (ASI). ASI powiadamia ustnie lub w formie elektronicznej (np. wiadomość e-mail) przełożonego pracownika oraz zainteresowanego o nadaniu uprawnień w systemie informatycznym. Wnioski pozytywnie zaopiniowane przez Administratora są zagregowane i pod nadzorem ASI. Na zasadach opisanych powyżej następuje cofnięcie uprawnienia czy jego rozszerzenie. Druk wzoru wniosku o wydanie uprawnienia określa ***Załącznik nr 12 Wniosek o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym***.
3. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zostaje zapoznany z zasadami ochrony danych osobowych opisanych w Polityce ochrony danych osobowych. Pracownik po zapoznaniu z zasadami podpsuje klauzulę poufności, której wzór stanowi ***Załącznik nr 13 Klauzula poufności.***
4. Każdy z pracowników Urzędu jest przeszkolony z zakresu tematyki ochrony danych osobowych przez IOD po podjęciu zatrudnienia oraz w razie zmiany istotnych warunków zewnętrznych (np. zmiany przepisów) lub wewnętrznych (np. zmiana stanowiska pracy).

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem.
1. Hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,

- hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
- hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
- hasło nie może być jednakowe z identyfikatorem użytkownika,
- hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

2. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
3. Hasło powinno być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.
4. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie ASI oraz IOD.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie.

Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

Zasady postępowania z hasłami administracyjnymi

1. W stosunku do haseł administracyjnych stosuje się zaostrzone standardy bezpieczeństwa. Szczególna ochrona dotyczy haseł:
a) administracyjnych do systemów, aplikacji, baz danych;
b) do zarządzania urządzeniami sieci teleinformatycznej (switch, router, firewall);
c) wykorzystywanych do szyfrowania danych.
2. Do przechowywania haseł zapisanych w formie papierowej stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury, tzw. koperty bezpieczne.
3. Koperty z hasłami administracyjnymi przechowuje się w miejscu zapewniającym dostęp tylko osobom upoważnionym.
4. Koperty z hasłami administracyjnymi podlegają ścisłej ewidencji prowadzonej przez Administratora Danych Osobowych lub osobę upoważnioną przez Administratora.
5. Ewidencja haseł administracyjnych prowadzona jest w formie rejestru w formie papierowej lub elektronicznej, który zawiera;
a) numer ewidencyjny;
b) oznaczenie przynależności hasła administracyjnego zawartego w kopercie (nazwa systemu, zasobu, komputera);
c) imię i nazwisko, pełnioną funkcję osoby składającej kopertę (właściciela hasła);
d) datę złożenia koperty;
e) imię i nazwisko osoby przyjmującej kopertę na przechowanie;
f) datę wygaśnięcia ważności hasła zawartego w kopercie;
g) adnotację o wydaniu koperty z hasłem (użyciu awaryjnym).
6. Dane umieszczone na bezpiecznej kopercie zawierają:
a) numer koperty adekwatny do numeru ewidencyjnego podanego w rejestrze haseł;
b) oznaczenie przynależności hasła administracyjnego zawartego w kopercie (nazwa systemu, zasobu, komputera);
c) imię i nazwisko, pełnioną funkcję osoby składającej kopertę (właściciela hasła);
d) datę złożenia koperty z hasłem;
e) imię i nazwisko osoby przyjmującej kopertę na przechowanie;
f) datę wygaśnięcia ważności hasła zawartego w kopercie;
g) adnotację o wydaniu koperty z hasłem.
7. Za aktualność przechowywanych haseł odpowiedzialny jest Administrator Danych Osobowych lub osoba upoważniona przez Administratora.
8. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej akceptacji Administratora lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.
9. Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.

Zasady zabezpieczania haseł

1. Haseł nie powinno się przechowywać w systemach, aplikacjach, bazach danych, skryptach i plikach konfiguracyjnych w postaci jawnej, nie zapewniającej im poufności.
2. Haseł nie powinno się przesyłać za pomocną narzędzi i usług teleinformatycznych w postaci jawnej, nie zapewniającej im poufności.
3. Należy stosować bezpieczną procedurę przekazywania haseł użytkownikom.
4. Zabronione jest przechwytywanie lub odgadywanie haseł innych użytkowników.
5. Hasła należy utrzymywać w tajemnicy również po upływie ich ważności.

6. Zabronione jest wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych).

Klucze kryptograficzne

1. W przypadku transmisji danych osobowych wrażliwych lub informacji poufnych Administratora zaleca się wykorzystywanie kluczy kryptograficznych służących do zabezpieczenia danych.
2. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada Administrator Danych Osobowych lub osoba upoważniona przez Administratora.
3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia, należy bezzwłocznie powiadomić Administratora Danych Osobowych oraz IOD.
5. Dane osobowe wrażliwe lub informacje poufne Administratora, w przypadku których nie stosuje się kluczy kryptograficznych, należy przesyłać wyłącznie pocztą elektroniczną po zabezpieczeniu pliku hasłem. Hasło przekazywane jest odbiorcy innym kanałem dystrybucyjnym.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora.
2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
3. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.
Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych płyty CD, pendrive i inne, zawierających dane osobowe.
4. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.

Zarządzenie bezpieczeństwem sieci

1. Należy zapewnić, że infrastruktura sieciowa jest właściwie chroniona, adekwatnie do zagrożeń mogących powodować utratę bezpieczeństwa przetwarzania danych osobowych.
2. Dane osobowe przesyłane poprzez publiczną sieć telekomunikacyjną powinny być zabezpieczone środkami kryptograficznej ochrony.
3. Administrator systemu informatycznego powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez:
a) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
4. Wewnętrzna adresacja IP, konfiguracja oraz informacja o systemach powiązanych nie powinna być ujawniana osobom nieuprawnionym bez akceptacji ze strony uprawnionej do tego celu osoby.
5. Podłączanie do infrastruktury sieciowej nieautoryzowanych urządzeń takich jak modemy, urządzenia sieciowe, w tym urządzenia sieci bezprzewodowych jest zabronione.
6. Użytkownikom należy zapewnić dostęp tylko do tych usług infrastruktury teleinformatycznej (np. dostęp do Internetu, zdalny dostęp, poczta elektroniczna) do których zostali autoryzowani.

7. Należy zapewnić, że osoby nie będące pracownikami nie posiadają nieautoryzowanego i niekontrolowanego dostępu do infrastruktury teleinformatycznej.
8. Należy zapewnić, że niezabezpieczone usługi infrastruktury teleinformatycznej, pozwalające przesyłać hasła w postaci niezabezpieczonej np. telnet lub ftp, nie są wykorzystywane i są zablokowane.
9. Sieci bezprzewodowe podłączone do infrastruktury teleinformatycznej powinny być autoryzowane, udokumentowane, monitorowane oraz odpowiednio zabezpieczone.

Zasady korzystania ze służbowej poczty elektronicznej

1. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie oraz w tym może być dostępna na łamach witryny internetowej Administratora Danych Osobowych.
2. Konto e-mail służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora Danych Osobowych może podlegać rejestrowaniu i monitorowaniu. Informacje przesyłane za pośrednictwem sieci (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
3. Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania odbiorów w kopii (pole UDW).
4. Zabronione jest:
a) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
b) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora Danych;
c) odbieranie przesyłek z nieznanych źródeł;
d) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
e) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;
f) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
g) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu informatycznego;
h) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
i) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora Danych lub do poszukiwania dodatkowego zatrudnienia.

Korzystanie z sieci Internet

1. Sieć, w której pracują urządzenia komputerowe oraz działają systemy informatyczne Administratora musi być odseparowana od sieci publicznej zaporą ogniową (firewall) lub urządzeniem typu UTM.
2. Systemy informatyczne przetwarzające dane osobowe powinny korzystać z szyfrowanych protokołów wymiany danych np. https.
3. Dostęp użytkowników do sieci publicznej powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Dostęp do protokołu wymiany plików np. ftp możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.
5. Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez Inspektora Ochrony Danych.

Zasady postępowania z nośnikami elektronicznymi i sprzętem komputerowym podczas pracy poza obszarem przetwarzania danych

Każdy użytkownik wymiennych nośników elektronicznych lub komputerów przenośnych ponosi całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz jest zobowiązany do stosowania się do poniższych zasad:
1. Zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora.
2. Obowiązkiem Administratora Danych Osobowych jest stosowanie szyfrowania dysków twardych oraz nośników wymiennych w celu zabezpieczenia przed wyciekiem danych osobowych.
3. Komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować.
4. Użytkownik wykonując czynności zawodowe lub umowne w domu powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich.
5. Zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem.
6. Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora.
7. W przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do Administratora Danych Osobowych lub Inspektora Ochrony Danych.
8. Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi systemu informatycznego.

Użytkowanie sprzętu komputerowego, oprogramowania i nośników danych

1. Do sprzętu komputerowego zalicza się między innymi:
a) komputery stacjonarne,
b) komputery przenośne (notebooki),
c) urządzenie mobilne np. tablety, smartphony
d) drukarki,
e) sprzęt sieciowy np. switch, router,
f) sprzęt serwerowy,
g) monitory,
h) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator Danych Osobowych lub osoba upoważniona przez Administratora odpowiada za poprawne działanie sprzętu komputerowego. Czynność tą Administrator Danych Osobowych może wykonywać poprzez pracowników lub współpracowników Administratora lub poprzez podmioty zewnętrzne.
3. Administrator Danych Osobowych lub ASI odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.
4. Administrator Danych Osobowych lub ASI jest zobowiązany do prowadzenia ewidencji posiadanego sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją.
5. Administrator Danych Osobowych lub ASI ma obowiązek przechowywać karty gwarancyjne oraz klucze i licencje do oprogramowania.
6. Administrator Danych Osobowych lub ASI prowadzi rejestr wydanego sprzętu komputerowego wraz z wyszczególnieniem użytkownika. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
7. Administrator ma prawo instalować wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.
8. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
9. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania. Zalecane jest aby użytkownik nie posiadał uprawnień administracyjnych na komputerze.
10. Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

Procedura zdalnego dostępu do systemów informatycznych

Do nawiązywania zdalnych połączeń administracyjnych muszą być stosowane:
a) rozwiązania komunikacyjne bazujące na bezpiecznych standardach komunikacji zapewniające szyfrowanie transmisji;
b) ASI oraz użytkownik systemu musi zezwolić na autoryzacje zdalnego połączenia poprzez podanie id sesji oraz hasła dostępowego;
c) użytkownik inicjujący zdalne połączenie zobowiązany jest nadzorować proces zdalnego połączenia;
d) po zakończeniu pracy zdalnej sesja musi zostać zamknięta.
W przypadku możliwości technicznych Administratora akceptuje się możliwość wykorzystania protokołu VPN umożliwiającego podłączenie do sieci Administratora bez każdorazowej autoryzacji użytkownika. Utworzenie konta VPN możliwe jest tylko i wyłącznie za zgodą Administratora Danych Osobowych. Rozwiązanie służące do komunikacji VPN musi mieć możliwość logowania sesji zdalnych użytkowników.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Kopie zapasowe powinny być kontrolowane przez Administratora Danych Osobowych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.
2. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
3. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.
2. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.
3. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

Zabezpieczenie systemu informatycznego przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

Wszystkie urządzenia informatyczne (komputery, serwery, urządzenia sieciowe), na których zainstalowane jest oprogramowanie służące do przetwarzania danych osobowych, powinny być zasilane z wydzielonej sieci oraz zabezpieczone przed krótkotrwałymi zanikami napięcia, przepięciami itp., przy pomocy zasilaczy awaryjnych (UPS). Minimalny czas podtrzymania zasilania za pomocą zasilaczy awaryjnych nie może być krótszy niż 15 minut. W przypadku urządzeń serwerowych zalecany czas podtrzymania to min. 2 godziny.

Sposób zabezpieczenia systemu informatycznego przez działalnością szkodliwego oprogramowania

1. Systemy informatyczne należy chronić przed szkodliwym oprogramowaniem (np. wirusy, trojany, bomby logiczne, robaki) poprzez stosowanie odpowiednich środków technicznych i organizacyjnych
2. Zidentyfikowanymi obszarami systemów informatycznych Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, elektroniczne nośniki informacji, dostęp do sieci publicznej, poczta e-mail.
3. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, siec lokalna lub elektroniczne nośniki informacji.
4. Stacje robocze, komputery przenośne, serwery muszą być objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Administratora.
5. Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia. Możliwość zatrzymania usługi systemu antywirusowego posiada jedynie Administrator lub ASI.
6. Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików pod kątem występowania oprogramowania złośliwego.
7. System antywirusowy musi posiadać możliwość automatycznego skanowania każdego zewnętrznego elektronicznego nośnika informacji, który jest podłączany do urządzenia komputerowego.
8. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z Administratorem systemu.
9. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
b) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;
c) samodzielną ingerencję w zawartość pliku w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem.

Procedura usuwania awarii sprzętu lub oprogramowania

1. W przypadku wystąpienia awarii systemu informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii Administratorowi danych lub osobie odpowiedzialnej za obsługę informatyczną.
2. Administrator danych lub osoba odpowiedzialna za obsługę informatyczną zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.
3. Po usunięciu awarii Administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
a) uruchomienia systemu informatycznego;
b) kontroli poprawności jego funkcjonowania;
c) kontroli integralności danych.
4. W przypadku stwierdzenia uszkodzenia danych zgromadzonych w systemie, Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).
5. W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, osoba przekazująca sprzęt ze strony Kancelarii zobowiązana jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności.

Sposób realizacji wymogów odnotowania informacji o odbiorcach, którym dane zostały udostępnione

Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom, w rozumieniu art. 4 pkt 9 rozporządzenia RODO, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Konserwacja i naprawa sprzętu komputerowego, systemów informatycznych oraz nośników informacji Administratora ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzenia lub naruszenia bezpieczeństwa.
2. Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów.
3. Naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora przeprowadzane są, o ile to możliwe, przez upoważnionych pracowników Administratora lub upoważnione firmy zewnętrzne.
4. Naprawy, konserwacje i zmiany w systemie informatycznym Administratora przeprowadzane przez serwisanta zewnętrznego prowadzone są pod nadzorem Administratora Danych Osobowych lub osoby upoważnionej przez Administratora w siedzibie Administratora (jeśli to możliwe) lub poza siedzibą Administratora, po uprzednim usunięciu elementów zawierających dane osobowe, o ile nie wiąże się to z nadmiernymi utrudnieniami.
5. Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Administratorem a tymże podmiotem, z uwzględnieniem klauzuli powierzenia przetwarzania danych lub klauzuli dotyczącej zachowania w poufności przez wykonawcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.
6. W przypadku zdalnej obsługi serwisowej systemów informatycznych Administratora, porty komunikacyjne powinny być włączane jedynie na wyraźne żądanie dostawcy takich usług, za zgodą Administratora systemu informatycznego i muszą być ponownie odłączone tuż po zakończeniu prac serwisowych.
7. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie zgodnie z procedurami Administratora.

Postanowienia końcowe

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.
2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany Dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.
3. Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Dokumentacji przetwarzania danych osobowych.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
5. W sprawach nieuregulowanych w niniejszej procedurze bezpieczeństwa zastosowanie mają przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy rozporządzenia RODO.

Załącznik nr 9
Upoważnienie do przetwarzania danych osobowych

Augustów, dn. ……

UPOWAŻNIENIE Nr ……
do przetwarzania danych osobowych

Na podstawie art. 29 RODO z dniem …… upoważniam Panią/Pana

……
(imię i nazwisko)

zatrudnioną/zatrudnionego w ……
(nazwa komórki organizacyjnej)
do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków zgodnie z zakresem czynności na stanowisku:

……
(zajmowane stanowisko)

Upoważnienie wygasa z chwilą ustania zatrudnienia na wyżej wymienionym stanowisku.

……
Podpis Administratora Danych Osobowych

……
Podpis osoby upoważnionej

Uwaga:
Niniejsze upoważnienie zostało sporządzone w dwóch jednobrzmiących egzemplarzach, które otrzymują:
- Osoba upoważniona
- Administrator

Augustów, dn. ……

Wniosek
o nadanie / cofnięcie upoważnienia do przetwarzania danych osobowych

Wnioskuję o wydanie/ cofnięcie***** upoważnienia

Pani /Panu ……
(imię i nazwisko pracownika)

zatrudnionej/emu na stanowisku ……..

do przetwarzania danych osobowych wynikających z zakresu czynności i obowiązków pracowniczych z powodu:

☐ Podjęcia pracy na stanowisku

☐ Zmiany stanowiska

☐ Naruszenia zasad i sposobu przetwarzania danych osobowych

……
Data i podpis kierownika wydziału
/pracownika na samodzielnym stanowisku pracy

*** niepotrzebne skreślić**

Ewidencja osób upoważnionych do przetwarzania danych osobowych					
Lp.	**Imię i nazwisko**	**Stanowisko/Zakres**	**Komórka organizacyjna**	**Data nadania upoważnienia**	**Data ustania upoważnienia**
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					

Augustów, dn. ……

Wniosek
o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym

Wnioskuję o nadanie / rozszerzenie/ cofnięcie***** uprawnienia

Pani /Panu ……
(imię i nazwisko pracownika)

zatrudnionej/emu na stanowisku ……..

do przetwarzania danych osobowych w poniższym systemie / systemach* (jeśli to możliwe - opisać zakres w systemie):

……
……
……
……
……
……

……
Data i podpis Kierownika Wydziału
/pracownika na samodzielnym stanowisku pracy

Akceptuję / nie akceptuję wniosku*

……
Data i podpis w imieniu Administratora

*** niepotrzebne skreślić**

Załącznik nr 13
Klauzula poufności

Augustów, ...

.....
(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 Administratora Danych zadaniach,
- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora Danych,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora Danych,
- 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 u Administratora Danych zasadach dotyczących przetwarzania danych osobowych, określonych w polityce bezpieczeństwa i zobowiązuję się ich przestrzegać.

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

.....
Data i podpis oświadczającego

Metodyka szacowania ryzyka

Metoda polega na identyfikacji kluczowych czynności przetwarzania. Następnie należy zidentyfikować dla każdej z czynności zagrożenia w kontekście aspektów: poufności, integralności, dostępności oraz ocenić prawdopodobieństwo jego wystąpienia posługując się jakościowymi określeniami;

1- Rzadkie
2- Mało prawdopodobne
3- Możliwe
4- Prawdopodobne
5- Prawie pewne

oraz oszacować skutek wystąpienia ryzyka poprzez przyporządkowanie jakościowych określeń;

A - Bardzo niski
B - Niski
C - Średni
D - Wysoki
E - Bardzo wysoki

Poziomy prawdopodobieństw są odpowiednio połączone w macierzy. Dla poszczególnych kombinacji tych dwóch parametrów określone są konkretne ryzyka, przyjmujące wartości punktowe w skali od 1 do 4, gdzie:

4 – Krytyczny – poziom ryzyka nietolerowany, wymaga natychmiastowego działania

3 – Zagrożony – poziom ryzyka nieakceptowany, działanie może zostać przesunięte w czasie ale wymaga stałego monitorowania

2 – Akceptowalny – poziom ryzyka nieakceptowany, działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania

1 – Niski – poziom ryzyka akceptowany, działanie podejmowane w zależności od wymaganych nakładów

Etapy szacowania ryzyka

1. Inwentaryzacja czynności przetwarzania danych.
2. Inwentaryzacja zasobów IT oraz stosowanych zabezpieczeń technicznych
3. Identyfikacja zagrożeń w aspektach poufności, integralności i dostępności
4. Ocena prawdopodobieństwa wystąpienia zagrożenia
5. Ocena skutku wystąpienia zagrożenia
6. Określenie poziomu ryzyka
7. Określenie charakteru, kontekstu, celu przetwarzania danych
8. Opis podjętych działań mające na celu minimalizację prawdopodobieństwa wystąpienia zagrożenia

Tabela określająca poziom ryzyka

			SKUTEK				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			A	B	C	D	E
PRAWDOPODOBIEŃSTWO	Prawie pewne	5	2	3	**4**	**4**	**4**
	Prawdopodobne	4	2	3	3	**4**	**4**
	Możliwe	3	**1**	2	3	3	**4**
	Małoprawdopodobne	2	**1**	2	2	3	3
	Rzadkie	1	**1**	**1**	2	2	3

Załącznik nr 15
Analioza ryzyka

ID	Zidentyfikowane ryzyko	Opis podjętych działań minimalizujących	Zagrożona poufność	Zagrożona integralność	Zagrożona dostępność	Technologia przetwarzania	Plan postępowań z ryzykiem

Arkusz ryzyk - elektroniczne

Ryzyko	Czy duży zakres?	Prawdopodobieństwo	Ocena skutku wystąpienia zagrożenia	Ryzyko (na podstawie tabeli)	Czy wysokie ryzyko z dużym prawdopodobieństwem?
1	2	3	4	5	6
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie
	Nie				Nie

Ryzyko	Czy duży zakres?	Prawdopodobieństwo	Ocena skutku wystąpienia zagrożenia	Ryzyko (na podstawie tabeli)	Czy wysokie ryzyko z dużym prawdopodobieństwem?
1	2	3	4	5	6
	Nie	0	0	0	Nie
	Nie	0	0	0	Nie
	Nie	0	0	0	Nie
	Nie	0	0	0	Nie
	Nie	0	0	0	Nie
	Nie	0	0	0	Nie
	Nie	0	0	0	Nie

MACIERZ RYZYKA

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA	Skutek dla osoby, której dane dotyczą				
	1 Bardzo niski - Osoby, których dane dotyczą nie odczują negatywnych skutków.	**2 Niski** - Osoby, których dane dotyczą mogą napotkać niedogodności, które są w stanie rozwiązać	**3 Średni** - Osoby, których dane dotyczą mogą napotkać zauważalne trudności, które nakładem niewielkich środków i czasu są w stanie rozwiązać	**4 Wysoki** - Osoby, których dane dotyczą mogą mieć znaczące trudności z naprawieniem szkód wywołanych wystąpieniem ryzyka	**5 Bardzo Wysoki** - Osoby, których dane dotyczą mogą napotkać trudnosci krytyczne oraz takie, z których nie będą w stanie rozwiązać
5 PRAWIE PEWNE Zdarzenie jest praktycznie możliwe oraz jego wystąpienie jest pewne w określonej perspektywie czasu	2	3	4	4	4
4 PRAWDOPODOBNE Zdarzenie jest praktycznie możliwe oraz jest wysoce prawdopodobne, że może wystąpić	2	3	3	4	4
3 MOŻLIWE Zdarzenie jest praktycznie możliwe oraz jego wystąpienie przewidujemy, że może wystąpić, lecz oczegujemy, że nie wystąpi	1	2	3	3	4
2 MAŁOPRAWDOPODOBNE Zdarzenie jest teoretycznie możliwe, ale takie lub podobne zdarzenie nie wystąpiło w przeszłości	1	1	2	2	3
1 RZADKIE Zdarzenie jest teoretycznie możliwe, ale takie okoliczności, które mogły by spowodować jego wstąpienie nie zakładamy, że mogą wystąpić	1	1	1	1	2

4 – Krytyczny; 3 – Zagrożony; 2 – Akceptowalny; 1 – Niski

Ocena skutków przetwarzania danych - DPIA		
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		
Zagrożenia dla poufności (P) **Skala od 0 do 4 = 1** **od 5 do 8 = 2** **od 9 do 12 = 3**	1. nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe	
	2. ujawnienie haseł dostępu do zasobów z danymi osobowymi	
	3. nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik	
	4. utrata nośnika zawierającego dane osobowe	
	5. klęska żywiołowa, w wyniku której utracono poufność danych osobowych	
	6. nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym lub innym	
	7. udostępnianie danych osobowych osobom nieupoważnionym	
	8. wejście w posiadanie danych osobowych przez osobę nieuprawnioną	
	9. pokonanie zabezpieczeń fizycznych lub programowych	
	10. naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych	

	11. podsłuch lub podgląd danych osobowych	
	12. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy	
	Stwierdzony poziom zagrożenia dla poufności wg skali od 1 do 3	
Zagrożenia dla integralności (I) **Skala od 0 do 4 = 1** **od 5 do 8 = 2** **od 9 do 12 = 3**	1. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego	
	2. błędy, pomyłki	
	3. awarie sprzętowe (serwer i inne komponenty)	
	4. awarie oprogramowania	
	5. brak kopii bezpieczeństwa	
	6. brak narzędzi, urządzeń i innych składników wspomagających integralność (np. brak archiwum)	
	7. zaniechania organizacyjne personelu	
	8. uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych	
	9. celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych	
	10. działanie złośliwego oprogramowania (wirusy)	
	11. pożar, zalanie, ekstremalna temperatura, itp.	
	12. zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny)	
	Stwierdzony poziom zagrożenia dla integralności wg skali od 1 do 3	
Zagrożenia dla rozliczalności (R) **Skala od 0 do 4 = 1** **od 5 do 8 = 2** **od 9 do 12 = 3**	1. brak kontroli nad dokumentami wykonywanymi na stanowisku w zakresie ich kopiowania i drukowania	
	2. brak formalizacji zastępstw pracowniczych	
	3. możliwość wprowadzenia zmian w treści dokumentu zawierającego dane osobowe	
	4. błędy oprogramowania lub sprzętu	
	5. nieprzydzielenie użytkownikom indywidualnych zasobów informacyjnych	
	6. brak ciągłości w administracji systemem informatycznym	
	7. brak mechanizmów okresowej kontroli zasad wspierających rozliczalność	
	8. możliwość zniszczenia lub uszkodzenia danych w sposób zamierzony	
	9. brak rejestracji udostępnienia danych osobowych	
	10. możliwość wyłudzenia dostępu do danych (np. podszywanie się pod innego użytkownika)	
	11. przebywanie w strefach przetwarzania osób nieupoważnionych w trakcie lub po pracy	
	12. wykonywanie pracy w sposób zdalny	
	Stwierdzony poziom zagrożenia dla rozliczalności wg skali od 1 do 3	

Powaga ryzyka	**Poufność (P)** **Integralność (I)** **Rozliczalność (R)**		**Mnożnik** **(P) x (I) x (R)**		**Stwierdzona powaga ryzyka** **Skala** **od 1 do 3 = niska** **od 4 do 8 = średnia** **od 9 do 18 = wysoka**	
Plan reakcji na ryzyko						
Ryzyko szczątkowe **jeśli (P) x (I) x (R) = 27**						
Metoda monitorowania ryzyka						
Konsultacje z UODO						
Podpisy osób uczestniczących w ocenie skutków przetwarzania danych						

Ocena spełniania obowiązków w zakresie ochrony danych osobowych w Urzędzie Miejskim w Augustowie

Załącznik nr 17 Audyt systemu ochrony danych

	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. 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 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 - 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 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).	*art. 24 i 32 RODO;* *mot. 26, 28, 29, 39, 74-78, 83 i 85 preambuły;* *Rozporządzenie KRI* *Standardy KZ*
			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 testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?	[ocena wymogu]				
			3. Czy polityka ochrony DO podlega przeglądom i jest okresowo aktualizowana?	[ocena wymogu]				
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 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 przetwarzającego, który ma dostęp do DO, przetwarzał je wyłącznie na polecenie administratora, chyba, że wymaga tego od niego prawo.	*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]				

	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.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 prawne. Analiza umów/porozumień, przepisy w aktach prawnych lub inne dokumenty potwierdzające.	*art. 26 ust. 1 RODO; mot. 79 preambuły.*
			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 odpowiedzialności współadministratorów w odniesieniu do: - wykonywania praw osoby, której dane dotyczą, w tym do - obowiązków informacyjnych, o których mowa w art. 13 i 14.	*art. 26 RODO; mot. 79 preambuły.*
			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 podmioty (usługodawców) przetwarzające w ich imieniu?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów DO oraz analiza umów zawartych z podmiotami przetwarzającymi. Wykaz wszystkich podmiotów 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.	*art. 28 RODO;* *mot. 81 preambuły;*
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 (np. zgoda ADO, umowa albo inny akt prawny)?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów czynności przetwarzania DO oraz analiza umów zawartych z podmiotami przetwarzającymi. Wykaz wszystkich podmiotów przetwarzających DO. Analiza treści zgód wydanych przez ADO, informacje od podmiotów przetwarzających oraz ewentualne sprzeciwy ADO wobec zmian w zakresie podmiotów przetwarzających.	*art. 28 ust. 2-4, art. 30 RODO;* *mot. 81 preambuły; Standardy KZ*
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]				

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.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 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 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 weryfikowania pozostałych pytań w obszarze I.10. Umowy o przetwarzanie DO.	*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 kategorie osób, których dotyczą, - obowiązki i prawa ADO, - osoby odpowiedzialne i właściwe do kontaktów roboczych po stronie ADO i podmiotu przetwarzającego?	[ocena wymogu]				
		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 bezpieczeństwo przetwarzania?	[ocena wymogu]				
		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 dotyczą? (art. 28 ust. 3 RODO lit. e)	[ocena wymogu]				
		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]				

	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.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. 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.	*art. 44-49 RODO;* *mot. 6, 101-116 preambuły.*
			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 warunków wymienionych w art. 49 RODO (tj. wyjątek w szczególnych sytuacjach).	[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 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 zgody). Porównanie rejestru z wybranymi czynnościami przetwarzania DO.	*Warunki przetwarzania (art. 6 RODO), szczegółowe i dodatkowe warunki przetwarzania DO (art. 8-10 RODO mot. 40-57 preambuły).*
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: ZFSS, 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 przetwarzania jest zgoda?	[ocena wymogu]			Informacja od ADO lub IOD. Dobrą praktyką jest określenie wzoru zgody uwzględniającego 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.	*art. 4 pkt 11 oraz art. 7 RODO;* *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)? 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?	[ocena wymogu]				
			3. Czy istnieje system rejestrowania i zarządzania bieżącą zgodą na przetwarzanie DO?	[ocena wymogu]				

	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:
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? 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?	[ocena wymogu]			Ocena na podstawie wybranych procesów przetwarzania DO.	*art. 5, 6 i 11 RODO;* *mot. 39-48 oraz 50 preambuły.*
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 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.	[ocena wymogu]				

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:
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, - przy pierwszej komunikacji lub - przy pierwszym ujawnieniu DO innemu odbiorcy?	[ocena wymogu]				
		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 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?	[ocena wymogu]				
		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, 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)?	[ocena wymogu]				
		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 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?	[ocena wymogu]				

	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:
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, 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.	*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]				
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 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.	[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, 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*).	*art. 15 RODO;* *art. 5 uodo;* *mot. 59, 63, 64 i 73 preambuły;* *wytyczne dot. przenoszenia.*
			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 konieczność udzielenia odpowiedzi bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
			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 informacji niejawnych.	[ocena wymogu]				

	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:
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 których mowa w art	*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]				
			4. Czy procedury te uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
III.8	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 odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
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. Ponadto niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*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]				
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]				

	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:
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 najpóźniej w ciągu miesiąca?	[ocena wymogu]				
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 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; 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.	*art. 37 ust. 1 RODO;* *art. 37 ust. 6 RODO* *mot. 97 preambuły;* *art. 8, 9, 10 i 158 uodo;* *wytyczne dot. IOD*
			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]				
			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. 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	*art. 38 ust. 2 RODO;* *wytyczne dot. IOD.*
			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.*

	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:
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.	*art. 37 ust. 5 RODO;* *mot. 97 preambuły* *wytyczne dot. IOD.*
			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 samokształcenia.	
IV.3	Zasoby IOD	[ocena obszaru]	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 niewystarczające 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 jednostce umożliwi skutecznie wykonywać obowiązki samodzielnie IOD.	*art. 38 ust. 2 RODO;* *wytyczne dot. 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 przetwarzającego, w szczególności analiza ich treści.	*art. 38 ust. 6 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD*
			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 danych osobowych, która uwzględniałaby w szczególności dane osobowe IOD oraz jego zadania.	*wytyczne dot. IOD*
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 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).	[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 jest patrz punkt wyżej dot. konfliktu interesów IOD).	*art. 38 i 39 RODO;* *mot. 97 preambuły;* *wytyczne dot. 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 skutecznej ochrony DO?	[ocena wymogu]			Informacja od IOD. Wyniki wcześniejszych audytów/kontroli/sprawdzeń w przedmiotowym obszarze.	*art. 24 ust. 2, 32 i 39 RODO*

	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:
V.	**V. REJESTROWANIE CZYNNOSCI 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?	NIE			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 systematycznego 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 zidentyfikowanej konieczności przeprowadzenia oceny skutków przetwarzania ochrony danych; 9. Informacja o naruszeniach ochrony DO; 10. Wskazanie technologii, aplikacji lub systemów informatycznych, 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".	*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?	NIE				
			3. Czy rejestr zawiera wszystkie elementy wymagane przez art. 30 ust. 1 RODO?	NIE				
V.3	Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu ADO albo przez podmiot przetwarzający	[ocena obszaru]	1. Czy wyznaczono podmiot (pracownika albo kom. org.), któremu powierzono przygotowanie/ prowadzenie rejestru wszystkich kategorii czynności przetwarzania DO?	NIE			Weryfikacja dokumentów dot. rejestru wszystkich kategorii czynności. Weryfikacja zapisów umów powierzenia 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".	*art. 30 ust. 2 RODO;* *mot. 82 preambuły.*
			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?	NIE				

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:
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 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 – 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.	*art. 24 i 32 RODO;* *mot. 26, 28, 29, 39, 74-78, 83 i 85 preambuły;* *Rozporządzenie KRI* *Standardy KZ*
		2. Czy prowadzona jest analiza ryzyka dla ochrony DO? Czy wyznaczono podmiot (osobę, stanowisko albo zespół) odpowiedzialny w tym zakresie?	[ocena wymogu]				
		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]				
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 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).	*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]				
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.*

	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:
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 dokumentowana. 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.	*art. 35 RODO;* *wytyczne dot. oceny skutków.*
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 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.	[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 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); 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).	*art. 32 i 35 RODO* *wytyczne dot. oceny skutków.*
			2. Czy podczas dokonywania oceny skutków uwzględniono wszystkie kryteria oceny, o których mowa w wytycznych dot. oceny skutków?	[ocena wymogu]				
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*

	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:
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). 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 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 bieżącą identyfikację naruszeń ochrony DO i pozwalają szybko poinformować organ nadzorczy i osobę, której dane dotyczą o naruszeniu).	
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, 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?	[ocena wymogu]				*art. 33 i 34 RODO;* *mot. 85-88 preambuły*
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]				
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*

OGOLNA OCENA SPEŁNIANIA OBOWIĄZKOW W ZAKRESIE DANYCH OSOBOWYCH

Sporządził:

(data i podpis)

Zatwierdził:

(data i podpis)

Formularz oceny spełniania obowiązków wynikających z rozporządzenia ws.
ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)
oraz ustawy o ochronie danych osobowych (uodo)

1.	Formularz oceny RODO został opracowany przez międzyresortowy zespół roboczy audytorów wewnętrznych i kontrolerów z Kancelarii Prezesa Rady Ministrów, Ministerstwa Sprawiedliwości, Ministerstwa Rodziny, Pracy i Polityki Społecznej oraz Ministerstwa Finansów. Jest to podsumowanie dotychczasowych doświadczeń ww. jednostek oraz wypracowanych materiałów wewnętrznych w zakresie przygotowania służb audytu i kontroli do realizacji zadań związanych z oceną systemu ochrony danych osobowych (dalej: DO).
2.	Celem opracowania niniejszego formularza jest metodyczne wsparcie służb audytu i kontroli w jednostkach administracji państwowej. Jest to materiał o charakterze generalnym, dlatego może być wykorzystywany przez wszystkie jednostki administracji (w tym rządowej i samorządowej) jako merytoryczna pomoc w realizacji zadań kontrolnych i audytowych.
3.	Materiał przedstawia najważniejsze zagadnienia, których może dotyczyć ocena. Prezentowane obszary badania / zagadnienia i pytania kontrolne oraz wskazówki metodyczne nie są wyczerpujące ani obowiązkowe, powinny być więc różnicowane i dostosowywane w zależności do rodzaju, charakteru i skali przetwarzania DO w danej jednostce. Mając to na uwadze zachęcamy Państwa do swobodnego uzupełniania i modyfikowania formularza zgodnie z własną metodyką działania, przyjętymi celami audytu lub kontroli oraz charakterystyką przetwarzania DO w badanej jednostce.
4.	Formularz składa się z 49 obszarów badania (łącznie 111 wymogów), które pogrupowano w VII rozdziałach skupiających się na kolejnych perspektywach zarządzania systemem ochrony danych osobowych, tj.: - planowaniu i organizacji tego systemu (rozdz. I. Organizacja systemu ochrony DO, w tym administratorzy, współadministratorzy i podmioty przetwarzające), - zapewnieniu poprawności procesów przetwarzania (rozdz. II. Prawo do przetwarzania DO i III. Realizacja praw osoby, której dane dotyczą) oraz - mechanizmach monitorowania i nadzoru nad tym procesem (rozdz. IV. Inspektor Ochrony Danych, V. Rejestrowanie czynności przetwarzania, VI. Ocena skutków przetwarzania DO, VII. Naruszenie ochrony DO).
5.	Konstrukcja formularza wymusza dokonanie podsumowania i oceny na poziomie zdefiniowanych obszarów, ale wykorzystanie tych ocen nie jest obowiązkowe. Podobnie zdefiniowana skala ocen (pozytywna, zastrzeżenia, negatywna, w realizacji, nie dotyczy), również może być stosownie modyfikowana, w zależności od przyjętej metodyki badania (np. spełnia, częściowo spełnia albo nie spełnia wymogów, uwaga, ryzyko naruszenia procedur, itp.). Niezależnie od przyjętej metodyki ocen, ma ona wskazać te obszary, które wymagają szczególnej uwagi ze strony Administratora Danych Osobowych (dalej: ADO) lub Inspektora Ochrony Danych (dalej: IOD), a także te obszary, do których należy wrócić w przypadku konieczności powtórnego badania, np. po stwierdzeniu istotnych słabości, uchybień lub nieprawidłowości). Opcję NIE DOTYCZY warto wykorzystywać, gdy badana jednostka nie jest objęta danym wymogiem (np. ze względu na nikłą skalę przetwarzania danych tego typu) albo gdy z innych względów świadomie ograniczono zakres badania. Dodatkową pomocą metodyczną jest wskazanie bardziej szczegółowych (111) wymogów, które wynikają z RODO, uodo albo zidentyfikowanej dobrej praktyki (ocena: TAK, NIE, ND., W REALIZACJI). Ocena spełniania poszczególnych wymogów ma wspomagać audytora lub kontrolera w dokonaniu oceny danego obszaru. Należy jednak pamiętać, że w każdym przypadku ocena obszaru powinna uwzględniać kontekst danego ustalenia, a w szczególności charakter DO, zakres ich przetwarzania oraz przyczyny i skutki ewentualnych niezgodności z wymogami. Dlatego też, nie we wszystkich przypadkach brak spełniania wymogów będzie się kończyć oceną negatywną albo zastrzeżeniami. Dotyczy to zwłaszcza przypadków, gdy nie zmniejszyła się ochrona praw i wolności osób których przetwarzanie dotyczy.
6.	Podsumowaniem formularza jest ocena ogólna, znajdująca się na jego końcu. Ocena ogólna powinna podsumować funkcjonowanie systemu ochrony DO oraz odnieść się do najważniejszych kwestii, problemów, uwag i zastrzeżeń. Można w niej również zaznaczyć czy, kiedy oraz w jakim obszarze ocena systemu powinna zostać powtórzona. Pomocą dla formułowania oceny ogólnej jest tabela podsumowująca liczbę ocen. Uzyskane dane ilościowe mogą być użyteczną pomocą poglądową, jednak każdorazowo należy uwzględnić, że nie odzwierciedlają one w pełni rozłożenia ryzyka związanego z ocenami negatywnymi uzyskanymi w konkretnych dla danej jednostki obszarach. Ryzyko to nie jest równomiernie rozłożone na wszystkie obszary. W zależności od badanej jednostki (tj. rodzaju DO oraz charakterystyki ich przetwarzania) inne obszary mogą być uznane za kluczowe i to oceny w tych obszarach będą decydować o ocenie ogólnej. Ocena ogólna ułatwia odniesienie jej do ocen poszczególnych obszarów oraz konkretnych wymogów. Jednak zamieszczenie jej w formularzu nie jest konieczne, zwłaszcza jeżeli ocena albo stosowne podsumowanie badanych obszarów zostanie zamieszczone w innym dokumencie (np. raporcie, sprawozdaniu lub wystąpieniu pokontrolnym). W takich przypadkach niniejszy formularz służy jedynie jako pomoc / narzędzie w audycie albo kontroli i należy go odpowiednio zmodyfikować.

Instrukcja postępowania w przypadku naruszenia bezpieczeństwa przetwarzania danych osobowych

§1

Celem niniejszej instrukcji jest określenie procedury postepowania w przypadkach naruszenia bezpieczeństwa przetwarzania danych osobowych, gdy naruszenie:
- jest związane z danymi przetwarzanymi w formie tradycyjnej
- jest związane z elektroniczna formą przetwarzania danych osobowych

§ 2

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

§ 3

Naruszeniem bezpieczeństwa przetwarzania danych osobowych jest każdy stwierdzony fakt:
a) nieuprawnionego udostępniania instytucjom, podmiotom lub osobom danych osobowych,
b) stwierdzone naruszenie zabezpieczenia systemu informatycznego,
c) sytuacje, gdy stan urządzeń, zbiorów danych, ujawnione metody pracy, sposób działania programu, jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie zabezpieczenia danych.

§ 4

1. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest bezzwłocznie powiadomić bezpośredniego przełożonego.
2. Miejsce zdarzenia należy pozostawić w stanie nienaruszonym.
3. W przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych, Administrator z pomocą IOD prowadzi postępowanie wyjaśniające, w toku którego dokumentuje opis stanu faktycznego:
   - sporządza notatkę z oględzin miejsca zdarzenia,
   - odbiera pisemne wyjaśnienia od osoby, która ujawniła zdarzenie,
   - podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony,
   - w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń,
   - uwzględniając skalę oraz skutki naruszenia ochrony, Administrator decyduje o powołaniu doraźnego zespołu i powiadomieniu o zdarzeniu Prezesa Urzędu Ochrony Danych.

§ 5

1. Administrator wraz z IOD ustala:
   a. powagę naruszenia,
   b. ocenia możliwe skutki naruszenia dla osób, których dane dotyczą uwzględniając, czy naruszenie może spowodować:
      - uszczerbek fizyczny,
      - szkody majątkowe,
      - szkody niemajątkowe,

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

2. Ocena wykonana zgodnie z w/w punktami powinna określić czy naruszenie z dużym prawdopodobieństwem skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.
3. **Kategorie naruszeń:**
   a. naruszenie ODO, którego nie trzeba zgłaszać do organu nadzorczego, ponieważ jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
   b. Naruszenie ODO, 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,
   c. Naruszenie ODO, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o którym należy poinformować organ nadzorczy oraz osoby, których to naruszenie może dotyczyć – niezwłocznie.

4. Wszystkie naruszenia, niezależnie od kategorii i skutku muszą zostać wpisane w wewnętrzny rejestr naruszeń, którego wzór stanowi ***Załącznik nr 19 Rejestr naruszeń bezpieczeństwa***.

§ 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, 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 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 20 Protokół sprawdzenia ochrony danych***.

§ 8

1. Nadużycie przez użytkownika postanowień niniejszej Instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.
2. W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy rozporządzenia RODO oraz Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

Załącznik nr 19
Rejestr naruszeń bezpieczeństwa

Rejestr naruszeń					
NAZWA ADMINISTRATORA	Burmistrz Miasta Augustowa – kierownik Urzędu Miejskiego w Augustowie				
INSPEKTOR OCHRONY DANYCH	Robert Stańczyk				
Czynność przetwarzania zgodnie z RCPD	**Kategorie osób i danych osobowych (art. 6, art. 9, art. 10 RODO) oraz liczba wpisów**	**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**

PROTOKÓŁ SPRAWDZENIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 32 ust. 1 rozporządzenia ogólnego, zespół doraźny w składzie:

1. ……
2. ……
3. ……

przeprowadził w Urzędzie Miejskim w Augustowie 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 administratora danych, 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) .....
.....
d) .....
.....

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 odpowiedzialna za ustalenie sposobu realizacji	Zakładany termin realizacji	Osoba/jednostka organizacyjna odpowiedzialna za realizację rekomendacji	Zakładany termin realizacji rekomendacji	Uwagi
a)	otwarte					
b)	otwarte					
c)	otwarte					

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

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

8. Załączniki stanowiące składową część sprawozdania:

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

Sporządził:

…… - członkowie zespołu doraźnego
(data i podpis)

Zatwierdził:

…… – w imieniu Administratora
(data i podpis)

Załącznik nr 21
Wzór umowy powierzenia przetwarzania danych

Umowa Nr .....

Zawarta w dniu ..... r. w…….. pomiędzy:
……. zwanym w dalszej części niniejszej umowy „Zleceniodawcą” reprezentowanym przez: .....
a
..... zwanym w dalszej części niniejszej umowy „Wykonawcą” reprezentowanym przez:
..... o następującej treści:

§ 1
Powierzenie przetwarzania danych osobowych

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy ..... a ....., o ..... Zleceniodawca powierza Wykonawcy trybie art. 28 ust.3 rozporządzenia 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). zwanego dalej RODO przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
3. Powierzone dane zawierają informacje o osobach fizycznych będących osobami fizycznymi.
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2
Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych: ……..
2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie , o której mowa w § 1 ust. 1 i w sposób zgodny z niniejszą Umową.

§ 3
Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 28 RODO.
2. Wykonawca oświadcza, że:
1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają właściwy do zagrożeń poziom bezpieczeństwa,
3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.
3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
2) każdym nieupoważnionym dostępie do danych osobowych,
3) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.

6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcia uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.
9. Wykonawca może „podpowierzyć" usługi objęte umową, o której mowa w § 1 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą Zleceniodawcy.

§4

Odpowiedzialność Wykonawcy

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów RODO lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§5

Czas obowiązywania Umowy powierzenia

Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia ……. .

§ 6

Warunki wypowiedzenia Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

§ 7

Rozwiązanie Umowy

Wykonawca, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 i niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§8

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§9

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego.

§10

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

§ 11

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....	.....
Zleceniodawca	Wykonawca

Rejestr umów powierzenia danych osobowych

NAZWA ADMINISTRATORA	Urząd Miejski w Augustowie – Burmistrz Miasta Augustowa
INSPEKTOR OCHRONY DANYCH	Robert Stańczyk

Lp.	Nazwa i dane kontaktowe podmiotu przetwarzającego	Data podpisania umowy	Data zakończenia umowy	Zakres i kategoria powierzonych danych osobowych	Podstawa powierzenia danych (umowa, porozumienie, przepis, inna (jaka?))
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					