Załącznik nr 1 Zarządzenia Nr 4.2018

Dyrektora Biblioteki- Centrum Informacji i Kultury

Gminy Stare Juchy

Z dnia 23 maja 2018r.

**POLITYKA OCHRONY DANYCH**

**W BIBLIOTECE- CENTRUM INFORMACJI I KULTURY**

**GMINY STARE JUCHY   
Z DNIA 23 MAJA 2018R.**

**Definicje**

**RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

**Ustawa o ochronie danych osobowych** – ustawa z dnia ??? o ochronie danych osobowych (Dz.U. z 2018 poz. ???).

**ADO, Administrator Danych Osobowych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

**Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

**Przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

**Dane szczególne** – dane osobowe, o których mowa w art. 9 ust. 2 RODO – ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

**Podmiot danych** – osoba, której dane dotyczą, właściciel danych osobowych.

**Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

**Osoba upoważniona** – osoba wykonująca zadania polegające na przetwarzaniu, w formie tradycyjnej lub elektronicznej, danych osobowych na wyraźne polecenie ADO i jest upoważniona do wykonywania tych czynności.

**Odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (strona trzecia: wszystkie podmioty za wyjątkiem: podmiotu danych, ADO, podmiotu przetwarzającego, osób upoważnionych). Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, **nie są jednak uznawane za odbiorców**; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

**Osoba nieuprawniona** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe z naruszeniem przepisów o ochronie danych osobowych, lub poza wyraźnym uprawnionym poleceniem ADO. Osobami uprawnionymi do dostępu do danych są podmiot danych oraz ADO, podmiot przetwarzający, osoba upoważniona w zakresie, w jakim jest to zgodne z RODO.

**Organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych.

**Państwo trzecie** – państwo nienależące do Unii Europejskiej, a po uwzględnieniu RODO w Porozumieniu o Europejskim Obszarze Gospodarczym, państwo trzecie będzie oznaczało państwo spoza **Europejskiego Obszaru Gospodarczego.**

**Usługi społeczeństwa informacyjnego – każda usługa świadczona za wynagrodzeniem, na odległość, drogą elektroniczną, pozbawioną charakteru materialnego, realizowana na indywidualne żądanie usługobiorcy**

**Wyraźne polecenie administratora – oznacza powierzenie zadań wymagających przetwarzania danych osobowych osobie fizycznej, niezależnie od formy prawnej, w szczególności poprzez zawarcie umowy o pracę, określenie zadań w ramach zakresu czynności lub dokumencie równoważnym, powierzenie pełnienia funkcji wraz z określeniem zadań lub zlecenie zadań w formie umowy cywilnoprawnej.**

# Informacje ogólne

## Administrator danych osobowych

Administratorem danych osobowych jest Biblioteka – Centrum Informacji i Kultury Gminy Stare Juchy, który ustala cele i sposoby przetwarzania danych osobowych.

## Kontekst funkcjonowania

Biblioteka jest instytucją kultury posiadającą osobowość prawną. Dostęp do biblioteki i jej zasobów jest prawem powszechnym.

Celem działania biblioteki jest w szczególności zaspokajanie potrzeb oświatowych, kulturalnych i informacyjnych społeczeństwa oraz uczestniczenie w upowszechnianiu i popularyzowaniu wiedzy i kultury. Cele te wynikają z charakteru biblioteki będącej instytucją wyższej użyteczności publicznej. Cele bibliotek są realizowane przede wszystkim poprzez gromadzenie i udostępnianie czytelnikom materiałów bibliotecznych.

Zgodnie z obowiązującymi przepisami do podstawowego zakresu zadań biblioteki zalicza się:

1. gromadzenie, opracowywanie, przechowywanie i ochronę materiałów bibliotecznych,
2. obsługę użytkowników, przede wszystkim udostępnianie zbiorów oraz prowadzenie działalności informacyjnej, zwłaszcza informowanie o zbiorach własnych, innych bibliotek, muzeów i ośrodków informacji naukowej, a także współdziałanie z archiwami w tym zakresie.

## Podstawowe zasady przetwarzania danych osobowych

Administrator danych osobowych przetwarza dane osobowe z poszanowaniem następujących

zasad:

1. legalizmu, która oznacza przetwarzanie danych osobowych w oparciu o podstawę prawną i zgodnie z prawem,
2. rzetelności i przejrzystości, która oznacza transparentność procesów przetwarzania, w tym spełnianie praw podmiotów danych i przejrzyste informowanie o przetwarzaniu danych osobowych,
3. ograniczenia celu przetwarzania, oznaczającą przetwarzanie wyłącznie takiej ilości danych osobowych i takiego rodzaju danych, które są niezbędne do osiągnięcia celu przetwarzania,
4. ograniczenia przechowywania, która oznacza przetwarzanie danych osobowych przez okres nie dłuższy niż jest to niezbędne do osiągnięcia celu przetwarzania,
5. prawidłowości, która oznacza podejmowanie działań w celu przetwarzania jedynie prawidłowych danych i ich uaktualniania,
6. integralności i poufności, która oznacza przyjęcie takich metod przetwarzania i zabezpieczenia, aby zapewnić ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, ujawnieniem osobom nieuprawnionym, oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,
7. rozliczalności, która oznacza możliwość wykazania spełnienia przestrzegania wyżej wymienionych zasad.

## Obszar przetwarzania danych osobowych

Obszarem przetwarzania danych osobowych są wszystkie pomieszczenia, w których realizowana jest podstawowa działalność Administratora Danych Osobowych. Przetwarzanie danych osobowych może być wykonywane także w innych miejscach, w których jest to niezbędne w celu realizacji zadań Administratora Danych Osobowych.

## Kategorie osób, których dane dotyczą

1. Administrator Danych Osobowych w szczególności przetwarza dane osobowe:
2. swoich pracowników (zatrudnionych na podstawie umowy o pracę) i osób fizycznych, którym zleca zadania na podstawie umów cywilnoprawnych, stosownych pełnomocnictw, aktów powołania wynikających z przepisów prawa i tym podobnych instrumentów prawnych,
3. czytelników,
4. uczestników organizowanych konkursów,
5. oraz innych osób fizycznych, a także pracowników lub przedstawicieli osób prawnych w szczególności w przypadkach:
   * którym zleca realizację zadań na podstawie zawartych umów,
   * w zakresie uzyskanych zgód na przetwarzanie danych osobowych,
   * do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora w zakresie dozwolonym przepisami prawa,
   * w zakresie ustalenia, dochodzenia lub obrony roszczeń,
6. Szczegółowe określenie kategorii osób, których dane są przetwarzane znajduje się w prowadzonym przez Administratora Danych Osobowych rejestrze czynności przetwarzania.

## Określenie wartości zasobów danych osobowych

Administrator Danych Osobowych przetwarza dane osobowe, w tym dane szczególne w zakresie niezbędnym do realizacji wykonywanych zadań i spełnienia obowiązków nałożonych przepisami prawa.

Uwzględniając treść art. 24 i 32 oraz motywu 75 i 76 RODO Administrator Danych Osobowych określił następujące wartości przetwarzanych zasobów informacyjnych zawierających dane osobowe:

* **niską** – dla pomocniczych zbiorów i zestawów danych osobowych, spisów spraw, ewidencji korespondencji itp., które zawierają podstawowe informacje o podmiotach danych, takie jak imię i nazwisko oraz dane teleadresowe,

których ujawnienie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą, pozbawieniem przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi tylko w sytuacji zgromadzenia dodatkowych danych o podmiocie danych,

* **średnią** – dla zbiorów i zestawów danych, w których przetwarzane są dane osobowe zawierające podstawowe informacje o podmiotach danych, takie jak imię i nazwisko, dane teleadresowe, oraz informacje dotyczące rodzaju czynności podejmowanych przez ADO na rzecz tych osób,

których ujawnienie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą, pozbawieniem przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi tylko w sytuacji zgromadzenia dodatkowych danych o podmiocie danych,

* **wysoką** – dla zbiorów i zestawów danych, w których przetwarzane są dane osobowe, w tym dane szczególne, dane o wyrokach skazujących, naruszeniach prawa lub powiązanych środkach bezpieczeństwa, lub ilość i rodzaj przetwarzanych danych pozwala na tworzenie profili osobistych (np. dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się),

których ujawnienie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą, podmioty danych mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi.

## Role w systemie przetwarzania danych osobowych

**Administrator Danych Osobowych (ADO)** - Biblioteka – Centrum Informacji i Kultury Gminy Stare Juchy, którego zadania realizuje Dyrektor Biblioteki,

**Podmiot przetwarzający** – podmiot, któremu powierzono przetwarzanie danych osobowych na podstawie umowy powierzenia lub innego instrumentu prawnego,

**Osoba upoważniona** – osoba realizująca zadania wymagające przetwarzania danych osobowych na wyraźne polecenie Administratora Danych Osobowych; wyraźne polecenie administratora może być zawarte, między innymi w umowie, zakresie czynności lub upoważnieniu do przetwarzania danych osobowych

**Administrator Systemu Informatycznego** – osoba lub podmiot, której powierzono w szczególności nadawanie i odbieranie uprawnień w systemie informatycznym i odpowiedzialność za sprawne funkcjonowanie tego systemu,

**Użytkownik Systemu Informatycznego –** osoba lub podmiot przetwarzająca dane osobowe w systemie informatycznym, na wyraźne polecenie Administratora Danych Osobowych, posiadająca własny, unikalny login do systemu,

**Inspektor Ochrony Danych (IOD)** – osoba lub pracownik podmiotu zewnętrznego wyznaczony przez Administratora Danych Osobowych, w szczególności do realizacji zadań określonych w art. 39 RODO.

# Instrukcja gromadzenia i przetwarzania danych osobowych

## Instrukcja ogólna gromadzenia danych osobowych

1. Osoba upoważniona, gromadząca dane osobowe upewnia się, że:
   1. posiada aktualną, wynikającą z art. 6, art. 9 lub art. 10 RODO podstawę prawną do przetwarzania danych osobowych – podstawy prawne przetwarzania danych osobowych wskazane są w Rejestrze Czynności przetwarzania danych osobowych,
   2. posiada konkretny cel przetwarzania danych osobowych wynikający z działalności ADO,
   3. ilość i rodzaj gromadzonych danych osobowych jest stosowny i adekwatny do celu przetwarzania lub jest zgodny z zakresem przewidzianym przepisami prawa,
   4. zgromadziła prawidłowe (merytorycznie poprawne) dane osobowe,
   5. wie przez jaki okres czasu będzie przetwarzała dane osobowe – czas ten nie może być dłuższy niż jest to wymagane obowiązującymi przepisami prawa lub nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
2. Zebrane dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich są zbierane i przetwarzane.
3. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów, o których mowa w pkt. 2.1 1 lit. a, albo są zbędne do realizacji celu, dla którego zostały zebrane, osoba upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.
4. Po osiągnięciu celu przetwarzania dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację podmiotów danych, z zastrzeżeniem przepisów prawa określających okres przechowywania danych kategorii dokumentacji, informacji lub danych osobowych, w tym z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz przepisów wydanych na podstawie tej ustawy.

**osoby realizujące:**

* wszystkie osoby upoważnione.

## Uzyskanie zgody na przetwarzania danych osobowych

1. Zgoda na przetwarzanie danych osobowych (art. 4 ust. 11 i art. 7 RODO) jest jedną z podstaw prawnych przetwarzania danych osobowych. Przed rozpoczęciem zbierania zgody na przetwarzanie danych osobowych osoba upoważniona upewnia się, że:
   1. nie ma zastosowania inna przesłanka, wynikającą z art. 6, art. 9 lub art. 10 RODO uprawniająca do przetwarzania danych osobowych,
   2. zgoda zbierana jest w konkretnie oznaczonym celu przetwarzania, a zakres gromadzonych danych służy osiągnięciu tego celu,
   3. cel przetwarzania opisany jest w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem i będzie zrozumiały dla osoby, która udziela zgody na przetwarzanie danych osobowych,
   4. udzielenie zgody jest dobrowolne, a jej nieudzielenie nie powoduje żadnych negatywnych konsekwencji dla osoby udzielającej zgody (brak dobrowolności może wystąpić przy udzielaniu zgody na przetwarzanie danych osobowych przez pracownika; negatywną konsekwencją nie jest rezygnacja z usługi, a np. sytuacja w której nieudzielenie zgody na przetwarzanie danych osobowych dla jednego celu np. otrzymywania newslettera lub udostępnienie wizerunku uniemożliwi korzystanie z innych usług lub utrudni realizację praw w innym zakresie),
   5. osoba udzielająca zgody jest poinformowana o możliwości wycofania udzielonej zgody,
   6. dla wyrażenia zgody przewidziano formę wymagającą świadomego działania (np. złożenie podpisu, zaznaczenie pola tzw. checkbox, lub inną czynność wymagającą działania),
   7. przewidziano formę wycofania zgody, która nie jest trudniejsza (nie wymaga więcej działań) niż forma jej udzielenia,
   8. spełniony został obowiązek informacyjny zgodnie z pkt. 2.3. 1 niniejszej dokumentacji.
2. Udzielone zgody:
   1. w przypadku udzielania ich w formie papierowej gromadzone są one przez osobę upoważnioną lub przez osobę odpowiedzialną za realizację zadania, na potrzeby którego gromadzone były dane osobowe,
   2. w przypadku udzielania ich w formie elektronicznej za pośrednictwem systemu informatycznego, gromadzone są automatycznie w tym systemie. System musi zapewnić ewidencjonowanie zarówno udzielenia jak i wycofania zgody z uwzględnieniem daty tych czynności. Po wycofaniu zgody wszystkie dane osobowe w systemie należy usunąć i zaprzestać ich przetwarzania w celu dla jakiego zostały zgromadzone, za wyjątkiem danych potwierdzających udzielenie i wycofanie zgody.
3. Wzór zgody stanowi załącznik nr 2.1.1.

**osoby realizujące:**

* w zakresie zapewnienia prawidłowego gromadzenia zgód w formie tradycyjnej (papierowej) - osoba upoważniona,
* w zakresie zapewnienia prawidłowego gromadzenia zgód w formie elektronicznej – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Obowiązek informacyjny

1. W celu zapewnienia przejrzystości i rzetelności przetwarzania danych osobowych, w momencie zbierania danych osobowych od osób, których dane dotyczą (art. 13 RODO) w tym od swoich pracowników, ADO ma obowiązek podać osobie następujące informacje:
   1. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
   2. jeżeli powołał – dane kontaktowe Inspektora Ochrony Danych,
   3. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania zgodnie z art. 6, 9 lub 10 RODO,
   4. jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
   5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
   7. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   8. informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   9. jeżeli przetwarzanie odbywa się na podstawie zgody (art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   10. informację o prawie wniesienia skargi do organu nadzorczego,
   11. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
   12. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli planowane jest dalsze przetwarzanie danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem ADO informuje osobę, której dane dotyczą, o nowym celu oraz udziela jej wszelkich informacji wymienionych w pkt. 2.3. 1 lit. g – l.
3. ADO nie ma obowiązku podawać informacji, o których mowa w pkt. 2.3. 1 gdy podmiot danych, dysponuje już tymi informacjami i ADO jest w stanie ten fakt udowodnić.
4. W celu zapewnienia przejrzystości i rzetelności przetwarzania danych osobowych, w przypadku zbierania danych osobowych od osób innych niż osoby, których dane dotyczą (art. 14 RODO), ADO najpóźniej w ciągu miesiąca od zebrania danych lub przy pierwszym kontakcie z podmiotem danych podaje mu następujące informacje:
   1. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
   2. jeżeli powołał – dane kontaktowe Inspektora Ochrony Danych,
   3. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania zgodnie z art. 6, 9 lub 10 RODO,
   4. kategorie odnośnych danych osobowych,
   5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
   7. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   8. jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
   9. informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   10. jeżeli przetwarzanie odbywa się na podstawie zgody (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   11. informację o prawie wniesienia skargi do organu nadzorczego,
   12. źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych,
   13. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
5. Jeżeli planowane jest dalsze przetwarzanie danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem ADO informuje osobę, której dane dotyczą, o nowym celu oraz udziela jej wszelkich informacji wymienionych w pkt. 2.3. 4 lit. g – m.
6. ADO nie ma obowiązku podawać informacji, o których mowa w pkt. 2.3. 4 gdy:
   1. podmiot danych, dysponuje już tymi informacjami i ADO jest w stanie ten fakt udowodnić
   2. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku – w tym przypadku ADO zapewnia stosowne środki organizacyjne i techniczne dla zapewnienia bezpieczeństwa danych osobowych,
   3. pozyskiwanie lub ujawnianie jest uregulowane w obowiązujących ADO przepisach prawa,
   4. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w przepisach prawa, w tym ustawowym obowiązkiem zachowania tajemnicy.
7. Obowiązek informacyjny powinien być realizowany w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
8. ADO udostępnia na swojej stronie internetowej treść obowiązku informacyjnego dotyczącą osób, które nie są jego pracownikami.
9. Osoby upoważnione przekazują treść obowiązku informacyjnego w formie drukowanej w bezpośrednim kontakcie z podmiotem danych i pobierają stosowne oświadczenie o zapoznaniu się z treścią obowiązku informacyjnego.
10. Osoby upoważnione lub osoba wskazana przez ADO gromadzą złożone oświadczenia.
11. Obowiązek informacyjny może być umieszczany w treści regulaminów konkursów lub regulaminu biblioteki, z którymi zapoznawani są uczestnicy lub czytelnicy. Taki obowiązek informacyjny musi być wyraźnie zaznaczony w dokumencie.
12. ADO lub wskazana przez niego osoba przekazuje pracownikom ADO lub osobom wykonującym na jego rzecz zadania na podstawie umów cywilnoprawnych, obowiązek informacyjny w formie drukowanej i pobiera stosowne oświadczenie o zapoznaniu się z treścią obowiązku informacyjnego.
13. Jeżeli to możliwe treść obowiązku informacyjnego przekazywanego pracownikom umieszczana jest na portalu wewnętrznym ADO, do którego mają dostęp pracownicy lub – gdy nie jest to możliwe – udostępniana jest pracownikom w inny powszechnie przyjęty przez ADO sposób.
14. Wzór obowiązku informacyjnego stanowią załączniki nr 2.3.1 i 2.3.2.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie spełnienia obowiązku informacyjnego podczas kontaktu z podmiotem danych – osoba upoważniona,
* w zakresie spełnienia obowiązku informacyjnego podczas gromadzenia danych w systemach informatycznych – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

# Instrukcja wypełniania praw podmiotów danych

## Zasady ogólne

1. ADO ułatwia podmiotowi danych wykonanie następujących praw:
   1. prawa dostępu do danych,
   2. prawa do sprostowania danych,
   3. prawa do usunięcia danych,
   4. prawa do ograniczenia przetwarzania danych,
   5. obowiązku poinformowania podmiotu danych o sprostowaniu lub usunięciu danych lub ograniczenia ich przetwarzania,
   6. prawa do przenoszenia danych,
   7. prawa do sprzeciwu,
   8. prawa do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu,
   9. zawiadomieniu podmiotu danych o naruszeniu ochrony danych osobowych.
2. Ułatwienie polega na:
   1. terminowym udzielaniu informacji i odpowiedzi na żądania wykonania przysługujących praw,
   2. komunikowaniu się z podmiotem danych w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
3. ADO realizuje prawa osób kierujących żądanie w sytuacji gdy nie ma wątpliwości co do tożsamości tej osoby oraz, że osoba ta występuje z żądaniem dotyczącym przetwarzania należących do niej danych osobowych.
4. W przypadku gdy ADO nie przetwarza danych osobowych podmiotu kierującego żądanie, informuje o tym fakcie podmiot, nie później niż w terminie 30 dni od wpłynięcia żądania.
5. W sytuacji w której ADO, wykaże, że nie jest w stanie zidentyfikować osoby kierującej żądanie w miarę możliwości, prosi tą osobę o podanie dodatkowych informacji pozwalających na potwierdzenie jej tożsamości.
6. Jeżeli osoba kierująca żądanie nie udzieli informacji wymaganych dla jej identyfikacji ADO może odmówić wykonania praw wymienionych w pkt. 3.1.1.
7. Komunikacja z podmiotem danych w zakresie wykonania praw wymienionych w pkt. 3.1.1odbywa się w formie pisemnej lub elektronicznej zgodnie z żądaniem strony.
8. Na żądanie podmiotu danych komunikacja w zakresie wykonania praw wymienionych w pkt. 3.1.1 oraz spełnienia obowiązku informacyjnego może być prowadzona ustnie, jeżeli tożsamość osoby będzie skutecznie potwierdzona innymi sposobami.
9. Na żądania osób odpowiedź udzielana jest bez zbędnej zwłoki, jednak nie później niż w terminie jednego miesiąca od otrzymania żądania.
10. Ze względu na charakter żądania lub liczbę żądań, termin ich realizacji można przedłużyć o kolejne 2 miesiące. W terminie miesiąca od otrzymania żądania ADO informuje kierującego żądanie, o przedłużeniu terminu i jego przyczynach ADO.
11. Spełnienie obowiązku informacyjnego i praw wymienionych w pkt. 3.1.1 jest wolne od opłat.
12. Jeżeli żądania podmiotu danych są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na ustawiczny charakter, ADO ma prawo:
    1. pobrać opłatę za podjęcie działania,
    2. odmówić podjęcia działania.
13. Opłata za podjęcie działania zgodnego z żądaniem ustalana jest na podstawie administracyjnych kosztów udzielenia informacji, komunikacji lub podjęcia działań. Opłaty nie pobiera się za informowanie osób o naruszeniu danych osobowych.
14. O odmowie podjęcia działań ADO informuje osobę kierującą żądanie nie później niż w terminie miesiąca od otrzymania żądania.
15. ADO lub wskazana przez niego osoba prowadzi ewidencję realizacji praw podmiotów danych w formie papierowej lub elektronicznej.
16. Wzór ewidencji stanowi załącznik nr 3.1.1.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowej realizacji praw i wolności podmiotów danych – osoba upoważniona.

## Prawo dostępu do danych

1. Na żądanie podmiotu danych ADO ma obowiązek udzielić informacji czy przetwarza dane osobowe kierującego żądanie oraz, jeżeli zostało to ujęte w żądaniu, udzielić następujących informacji:
   1. jakie są cele przetwarzania,
   2. jakie dane osobowe są przetwarzane, z podaniem ich zakresu lub treści zgodnie z żądaniem podmiotu danych,
   3. informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych – jeżeli ma to miejsce, lub informację o nieprzekazywaniu danych,
   4. jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, należy wskazać zabezpieczenia, o których mowa w art. 46 RODO,
   5. jeżeli jest to możliwe planowany okres przechowywania danych osobowych, albo kryteria ustalania tego okresu,
   6. informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
   7. informacje o prawie wniesienia skargi do organu nadzorczego,
   8. jeżeli dane osobowe zostały zebrane od innych podmiotów niż podmiot danych – wszelkie dostępne informacje o ich źródle,
   9. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, wraz ze wskazaniem istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Żądanie dostępu do danych może być zrealizowane w formie drukowanej lub elektronicznej poprzez:
   1. odpowiedź pisemną,
   2. jeżeli podmiot danych tego zażądał, przekazanie kserokopii lub skanów dokumentów zawierających dane osobowe, z tym, że ze względu na podmiotowy charakter uprawnienia, przekazywane kopie dokumentów należy zanonimizować w zakresie wszelkich danych osobowych, które nie dotyczą kierującego żądanie (także dane zawarte w pieczątkach itp.). Za kolejne kopie, o które zwróci się osoba ADO może pobrać opłatę zgodnie z pkt. 3.1. 12.

**PODMIOTY REALIZUJĄCE ZADANIA PUBLICZNE**

1. Na podstawie art. 5 ust. 2 ustawy o ochronie danych osobowych, w przypadku, gdy realizacja prawa dostępu do danych 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.
2. Na podstawie art. 5 ust. 1 ustawy o ochronie danych osobowych, prawo dostępu do danych nie ma zastosowania w sytuacji, gdy ADO nie jest zobowiązany do spełnienia obowiązku informacyjnego zgodnie z pkt. 2.4. 1.
3. W przypadku wpłynięcia żądania do którego zastosowanie ma powyższy punkt, ADO niezwłocznie, nie później niż w ciągu miesiąca informuje podmiot o podstawie nieprzekazania żądanych informacji.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowej realizacji praw i wolności podmiotów danych – osoba upoważniona.

## Prawo do sprostowania danych

1. Na żądanie podmiotu danych ADO dokonuje sprostowania nieprawidłowych lub uzupełnienia brakujących ze względu na cel przetwarzania danych osobowych.
2. Na ADO ciąży obowiązek weryfikacji czy sprostowane lub uzupełniane dane są zgodne ze stanem faktycznym.
3. Do czasu sprostowania danych ADO ogranicza ich przetwarzanie w zakresie, którego prawidłowość jest kwestionowana zgodnie z zasadami określonymi w pkt. 3.5. 2.
4. O sprostowaniu lub uzupełnieniu danych ADO informuje osobę kierującą żądanie w terminie, o którym mowa w pkt. 3.1. i 9.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowej realizacji praw i wolności podmiotów danych – osoba upoważniona.

## Prawo do usunięcia danych

1. Na żądanie podmiotu danych ADO dokonuje usunięcia przetwarzanych danych osobowych w sytuacji, gdy:
   1. dane są zbędne ze względu na osiągnięcie celu przetwarzania dla jakiego zostały zgromadzone,
   2. podmiot danych cofnął zgodę na przetwarzanie danych osobowych i nie ma innej podstawy prawnej przetwarzania,
   3. dane osobowe były przetwarzane niezgodnie z prawem,
   4. konieczność usunięcia wynika z przepisów prawa,
   5. w ramach świadczenia usług społeczeństwa informacyjnego przetwarzane są dane osobowe dziecka, które ukończyło 16 lat lub, które nie ukończyło 16 roku życia, a zgodę na przetwarzanie wyraziła osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem,
   6. podmiot danych wniósł skuteczny sprzeciw dotyczący przetwarzania danych osobowych zgodnie z pkt. 3.8.
2. Prawo usunięcia danych nie ma zastosowania w szczególności, gdy przetwarzanie służy:
   1. do ustalenia, dochodzenia lub obrony roszczeń,
   2. spełnienia obowiązku prawnego lub realizacji zadań w interesie publicznym lub w ramach sprawowania władzy publicznej,
   3. zapewnieniu korzystania z prawa do wolności wypowiedzi i informacji,
   4. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz i, i art. 9 ust. 3 RODO,
3. Realizując prawo do usunięcia danych ADO dokonuje analizy czy prawo do usunięcia danych może zostać zrealizowane ze względu na ww. przesłanki. W tym czasie ogranicza się przetwarzanie danych osobowych, których dotyczy żądanie usunięcia zgodnie z pkt. 3.5. 2.
4. Realizując prawo do usunięcia danych ADO:
   1. niszczy lub anonimizuje dokumenty zawierające dane osobowe podlegające usunięciu,
   2. usuwa dane osobowe z systemu informatycznego lub uniemożliwia ich dalsze przetwarzanie.
5. Usuwając dane osobowe ADO musi zapewnić możliwość potwierdzenia zgody wyrażonej przez podmiot danych na przetwarzanie danych osobowych poprzez pozostawienie informacji niezbędnych do tego celu.
6. Jeżeli dane podlegające usunięciu zostały upublicznione, ADO, biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne w celu usunięcia tych danych z przestrzeni publicznej.
7. Jeżeli dane podlegające usunięciu zostały przez ADO przekazane innym podmiotom, ADO, biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne w celu poinformowania tych podmiotów o konieczności usunięcia danych osobowych, łącz do tych danych i ich kopii.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowej realizacji praw i wolności podmiotów danych – osoba upoważniona.

## Prawo do ograniczenia przetwarzania

1. Na żądanie podmiotu danych ADO ogranicza przetwarzanie danych osobowych tej osoby w sytuacji gdy:
   1. podmiot danych, kwestionuje prawidłowość dotyczących go danych osobowych – ograniczenie trwa do czasu sprostowania danych,
   2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą w skierowanym żądaniu, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania – ograniczenie przetwarzania trwa do czasu uchylenia żądania ograniczenia przetwarzania przez podmiot danych lub do czasu podjęcia czynności przez ADO lub podmiot danych pozwalające na ich dalsze, zgodne z prawem przetwarzanie. Po ewentualnym uchyleniu ograniczenia przetwarzania danych przez osobę kierującą żądanie, dane przetwarzane niezgodnie z prawem powinny zostać usunięte.
   3. dane osobowe są niezbędne osobie kierującej roszczenie do ustalenia, dochodzenia lub obrony roszczeń, a ADO osiągnął cel dla którego dane były przetwarzane – ograniczenie przetwarzania przez okres niezbędny do ustalenia, dochodzenia lub obrony roszczeń, lub do uchylenia ograniczenia przetwarzania przez osobę kierującą żądanie,
   4. osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania zgodnie z pkt. 3.8 – ograniczenie przetwarzania trwa do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. Dane osobowe, których ma dotyczyć ograniczenie nie mogą być przetwarzane w innych celach niż przechowywanie, łącznie z ograniczeniem dostępu do tych danych osób wykonujących zadania w imieniu ADO.
3. Pomimo ograniczenia przetwarzania ADO może przetwarzać nadal dane osobowe podmiotu kierującego żądanie w sytuacji, gdy:
   1. podmiot danych wyraził zgodę na przetwarzanie danych,
   2. przetwarzanie ma na celu ustalenie, dochodzenie lub obronę roszczeń ADO,
   3. przetwarzanie ma celu ochronę praw innej osoby fizycznej lub prawnej,
   4. przetwarzanie ma celu ważne względy interesu publicznego.
4. Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym fakcie osobę kierującą żądanie.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowej realizacji praw i wolności podmiotów danych – osoba upoważniona,
* w zakresie ograniczenia przetwarzania danych w systemach informatycznych – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Obowiązek poinformowania o sprostowaniu, usunięciu danych lub ograniczeniu ich przetwarzania

1. ADO ma obowiązek poinformować każdego odbiorcę, któremu ujawnił dane osobowe o:
   1. sprostowaniu danych osobowych,
   2. usunięciu danych osobowych,
   3. ograniczeniu przetwarzania, którego dokonał realizując: prawo do sprostowania danych, prawo do usunięcia danych oraz prawo do ograniczenia przetwarzania,
2. ADO może odstąpić od poinformowania odbiorców danych w sytuacji, gdy okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
3. ADO na żądanie podmiotu danych informuje go o odbiorcach, którym ujawnił dane osobowe.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowej realizacji praw i wolności podmiotów danych – osoba upoważniona,
* w zakresie ograniczenia przetwarzania danych w systemach informatycznych – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Prawo do przenoszenia danych

1. Prawo do przenoszenia danych osobowych ma zastosowanie wyłącznie w sytuacji, gdy przetwarzanie odbywa się w sposób zautomatyzowany z wykorzystaniem systemów informatycznych:
   1. na podstawie uzyskanej zgody, lub
   2. jest niezbędne w celu zawarcia i realizacji umowy.
2. Przeniesienie danych osobowych, zależnie od żądania podmiotu danych polega na:
   1. przekazaniu osobie, która wystąpiła z żądaniem, dotyczących jej danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (np. plik arkusza kalkulacyjnego, plik .xml, .json, .csv itp.),
   2. przekazaniu wskazanemu przez osobę, która wystąpiła z żądaniem, dotyczących jej danych osobowych administratorowi danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (np. plik arkusza kalkulacyjnego, plik .xml, .json, .csv itp.).
3. Zakres danych podlegających prawu przenoszenia obejmuje tylko dane dostarczone bezpośrednio przez podmiot danych.
4. ADO przed przekazaniem podmiotowi danych lub innemu administratorowi upewnia się, że przeniesienie nie naruszy praw i wolności osób trzecich (np. przesyłanie zdjęć grupowych, elektronicznych kopii dokumentów zawierających dane osobowe osób trzecich itp.).
5. 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.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowego przygotowania kopii dokumentów – osoba upoważniona,
* w zakresie przeniesienia danych (generowanie pliku lub transfer do innego ADO) – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Prawo do sprzeciwu przetwarzania danych osobowych

1. Prawo do sprzeciwu ma zastosowanie wyłącznie w sytuacji, gdy:
   1. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO,
   2. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.
2. Jeżeli podmiot danych sprzeciwi się przetwarzaniu jego danych osobowych w ww. celach ADO ma obowiązek zaprzestać ich przetwarzania, chyba, że wykaże istnienie:
   1. ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności podmiotu wnoszącego sprzeciw,
   2. podstaw do ustalenia, dochodzenia lub obrony roszczeń.
3. Jeżeli podmiot danych sprzeciwi się przetwarzaniu jego danych osobowych w celach marketingu bezpośredniego, ADO zaprzestaje przetwarzania danych osobowych w tym celu.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowej realizacji praw i wolności podmiotów danych, w tym prawidłowej oceny żądania – osoba upoważniona,
* w zakresie zapewnienia usunięcia danych z systemu informatycznego lub ograniczenia przetwarzania danych w systemach informatycznych – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu

1. Podmiot danych ma prawo by nie podlegać decyzjom opartym na zautomatyzowanym (z wykorzystaniem algorytmów i systemów komputerowych) podejmowaniu decyzji, w tym profilowaniu, które będą wywoływały skutki prawne.
2. W sytuacji, gdy ADO ma zamiar w sposób zautomatyzowany przetwarzać dane osobowe informuje o tym fakcie podmiot danych.
3. ADO może stosować zautomatyzowane podejmowanie decyzji w sytuacji, gdy:
   1. podmiot danych wyraził na to zgodę,
   2. jest to niezbędne do zawarcia lub wykonania umowy zawartej przez ADO z podmiotem danych,
   3. jest dozwolone przepisami prawa, którym podlega ADO.
4. Przetwarzanie danych szczególnych w zakresie podejmowania zautomatyzowanych decyzji, w tym profilowania, może mieć miejsce tylko w sytuacji, gdy:
   1. podmiot danych wyraził na to zgodę,
   2. przetwarzanie wykonywane jest w ważnym interesie publicznym na podstawie przepisów prawa.
5. Podmiot danych ma prawo odwołać się od decyzji podjętej w sposób zautomatyzowany, w tej sytuacji ADO zapewnia rozpatrzenie tej decyzji przez osobę upoważnioną.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie prawidłowego gromadzenia zgody na podejmowanie zautomatyzowanych decyzji – osoba upoważniona,
* w zakresie zapewnienia niepoddawania podmiotu danych zautomatyzowanym decyzjom bez aktualnej podstawy prawnej – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

# Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

## Uwzględnianie ochrony danych w fazie projektowania

1. ADO planując nowe zadania lub usługi (takie jak konkursy, spotkania, festyny i inne imprezy dostępne lokalnej społeczności oraz wykonując już funkcjonujące) zapewnia środki organizacyjne i techniczne służące bezpieczeństwu danych osobowych.
2. W fazie planowania nowych zadań lub usług ADO poddaje analizie:
   1. czy przetwarzanie danych osobowych będzie spełniało wymagania RODO, w szczególności czy zapewnione jest spełnienie podstawowych zasad przetwarzania danych osobowych, o których mowa w art. 5 RODO oraz w pkt. 2.1 niniejszego dokumentu,
   2. czy możliwa będzie realizacja praw i wolności podmiotów danych, którzy będą korzystali z nowego zadania lub usługi,
   3. czy ADO jest w stanie zapewnić odpowiednie środki organizacyjne i techniczne, w tym pseudonimizację i minimalizację, zapewniające bezpieczeństwo przetwarzanych danych w kontekście zidentyfikowanych ryzyk.
3. Uwzględnienie ochrony danych osobowych w fazie projektowania należy stosować także w sytuacji, gdy dokonywane są zakupy, produkcja lub wdrożenia systemów informatycznych służących lub mających wpływ na przetwarzanie danych osobowych.

**osoby realizujące:**

* w zakresie zapewnienia ochrony danych w fazie projektowania – ADO,
* w zakresie dokonywania zakupów dostaw i usług, informowania ADO o zamiarze podjęcia nowych zadań obejmujących przetwarzanie danych osobowych – osoba upoważniona w tym osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Domyślna ochrona danych

1. W celu zapewnienia domyślnej ochrony danych osobowych ADO wdraża odpowiednie środki techniczne i organizacyjne mające na celu minimalizację przetwarzania. Minimalizacja osiągana jest poprzez przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Obowiązek ten oznacza:
   1. minimalizację ilości danych osobowych,
   2. minimalizację zakresu danych osobowych,
   3. określenie niezbędnego czasu przetwarzania danych osobowych,
   4. określenie minimalnej grupy osób, które będą miały dostęp do tych danych,
   5. zapewnienie dostępności dodanych w niezbędnym zakresie.
2. ADO stosuje środki organizacyjne i techniczne mające na celu zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych.
3. Uwzględnienie domyślnej ochrony danych osobowych należy stosować także w sytuacji, gdy dokonywane są zakupy, produkcja lub wdrożenia systemów informatycznych służących lub mających wpływ na przetwarzanie danych osobowych.

**osoby realizujące:**

* w zakresie zapewnienia domyślnej ochrony danych – ADO,
* w zakresie dokonywania zakupów dostaw i usług, informowania ADO o zamiarze podjęcia nowych zadań obejmujących przetwarzanie danych osobowych – osoba upoważniona w tym osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

# Środki organizacyjne służące bezpieczeństwu danych osobowych

## Rejestry czynności i kategorii przetwarzania danych osobowych

1. ADO prowadzi rejestr czynności przetwarzania danych osobowych (dalej RCP), który stanowi jednocześnie inwentarz wszystkich czynności przetwarzania wykonywanych przez ADO.
2. W RCP umieszczone są wszystkie zadania i usługi, które realizuje ADO.
3. RCP jest na bieżąco aktualizowany w sytuacjach:
   1. wprowadzenia nowych usług,
   2. realizacji nowych zadań,
   3. zmiany przepisów mających wpływ na informacje zawarte w rejestrze.
4. ADO prowadzi rejestr kategorii przetwarzania danych osobowych (dalej RKP) dla czynności przetwarzania zostały mu powierzone na podstawie umów powierzenia przetwarzania.
5. Rejestry prowadzone są w formie **elektronicznej lub papierowej**.
6. Każda osoba upoważniona ma obowiązek poinformować osobę wyznaczoną do prowadzenia rejestru o sytuacji wymienionej w pkt. 5.1. 2.
7. Osoba prowadząca rejestr, raz do roku dokonuje szczegółowego przeglądu zawartych w nim danych.
8. Wzór RCP stanowi załącznik nr 5.1.1.
9. Wzór RKP stanowi załącznik nr 5.1.2.

**osoby realizujące:**

* w zakresie prowadzenia rejestrów – ADO,
* w zakresie informowania o nowych zadaniach, usługach lub zmianach przepisów – osoba upoważniona.

## Adekwatność, stosowność i ograniczenie czasowe przetwarzania danych osobowych

1. Osoby upoważnione realizując powierzone im zadania, zbierają i przetwarzają dane osobowe wyłącznie w ilości i zakresie:
   1. niezbędnym do osiągnięcia celu przetwarzania jakim jest realizowane zadanie,
   2. wynikającym z przepisów prawa, na podstawie których realizowane jest zadanie.
2. Osoby upoważnione realizując powierzone im zadania dbają, aby przetwarzać dane osobowe:
   1. nie dłużej niż jest to niezbędne dla celu przetwarzania,
   2. nie dłużej niż jest do dopuszczone obowiązującymi przepisami prawa określającymi czas przetwarzania danych osobowych, w tym z zastosowaniem zasad wynikających z instrukcji kancelaryjnej i obowiązku archiwizacji dokumentów.
3. Ograniczenie czasowe przetwarzania danych osobowych realizowane jest przez osoby upoważnione oraz przez ASI.

**osoby realizujące:**

* w zakresie nadzoru nad podejmowanym przetwarzaniem – ADO,
* w zakresie dbałości o spełnienie ww. wymagań – osoba upoważniona, osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Upoważnienia do przetwarzania danych osobowych i ich odbieranie

1. W celu zapewnienia ograniczenia dostępu do danych osobowych, przetwarzanych w formie tradycyjnej (drukowanej, pisemnej) i w formie elektronicznej, wyłącznie do osób realizujących zadania na polecenie ADO stosowane są upoważnienia do przetwarzania danych osobowych (dalej upoważnienia).
2. Upoważnienia nie mogą być wydawane w zakresie szerszym niż wynika to z zakresu powierzonych zadań.
3. Uprawnienia do systemów informatycznych nie mogą być nadawane w zakresie szerszym niż zakres upoważnienia.
4. Upoważnienie wydawane jest w momencie zlecenia realizacji zadania lub zadań wymagających przetwarzania danych osobowych niezależnie od formy tego zlecenia (umowa o pracę, umowa cywilnoprawna, powołanie lub inne umocowanie do działania w imieniu ADO).
5. Upoważnienia i uprawnienia nadawane są na okres czasu zgodny z umową lub innym instrumentem prawnym na podstawie którego zlecono realizację zadania.
6. Upoważnienia, wydaje ADO – Dyrektor jednostki.
7. Osoba odpowiedzialna za przygotowanie zakresu zlecanego do realizacji zadania lub zadań informuje ADO o konieczności wydania upoważnienia i przygotowuje jego projekt.
8. Wzór upoważnienia stanowi załącznik nr 5.3.1.
9. Upoważnienia wydawane są w formie pisemnej. Kopię upoważnienia przechowuje ADO.
10. ADO prowadzi na bieżąco, w formie elektronicznej, rejestr upoważnień.
11. Wzór rejestru upoważnień stanowi załącznik nr 5.3.2.
12. Wszystkie osoby w momencie otrzymania pierwszego upoważnienia lub w przypadku zmian obowiązujących przepisów składają stosowne oświadczenia o zachowaniu poufności.
13. Wzór oświadczenia stanowi załącznik nr 5.3.3.
14. Oświadczenia przechowywane są wraz z kopiami upoważnień.
15. Jeżeli osoba upoważniona ma wykorzystywać do przetwarzania danych osobowych systemy informatyczne (w tym pocztę elektroniczną) po wydaniu upoważnienia i odebrania oświadczenia, na polecenie ADO nadawane są niezbędne uprawnienia. Uprawnienia nadaje osoba odpowiedzialna za sprawne funkcjonowanie danego systemu (ASI).
16. Oświadczenia o zachowaniu poufności odbierane są także od osób, które nie realizują zadań wymagających przetwarzania danych osobowych, jednak mogą mieć do niech dostęp (np. osoby sprzątające lub dokonujące prac gospodarczych w obszarze przetwarzania w trakcie i po godzinach pracy ADO).
17. Osoba odpowiedzialna za nadawanie uprawnień w systemie informatycznym nadaje indywidualny login i hasło oraz poziom uprawnień w systemie, zgodnie z poleceniem ADO.
18. Osoba odpowiedzialna za nadawanie uprawnień w systemie informatycznym prowadzi rejestr uprawnień w systemie informatycznym (rejestr systemowy), a jeżeli to nie jest możliwe – poza systemem informatycznym w wersji elektronicznej. Rejestr prowadzony poza systemem informatycznym powinien być aktualny.
19. W sytuacji:
    1. wcześniejszego zakończenia obowiązywania umowy lub innej czynności prawnej, na podstawie której zlecono realizację zadań,
    2. zmiany zakresu zadań.

upoważnienia i uprawnienia muszą zostać odwołane lub zmodyfikowane przekazany analogicznie z opisaną wyżej procedurą.

**osoby realizujące:**

* w zakresie nadania upoważnienia i prowadzenia ewidencji upoważnień – ADO,
* w zakresie nadawania uprawnień w systemach informatycznych oraz zapewnienia aktualnej ewidencji uprawnień – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI lub osoba wyznaczona do nadawania uprawnień w systemach informatycznych.

## Obowiązki osób upoważnionych

1. Zbierając dane osobowe od osób, których dane dotyczą osoba upoważniona spełnia obowiązek informacyjny, zgodnie z zasadami określonymi w pkt. 2.3. 1 – 3.
2. W celu ograniczenia dostępu do danych osobowych osób nieuprawnionych wszystkie osoby przetwarzające dane osobowe na polecenie ADO:
   1. przetwarzają danew zakresie zadań powierzonych im do realizacji zgodnie z otrzymanymi upoważnieniami,
   2. dbają o spełnienie podstawowych zasad przetwarzania danych osobowych zawartych w Instrukcji gromadzenia i przetwarzania dokumentów (pkt.2) oraz Instrukcji wypełniania praw podmiotów danych (pkt. 3),
   3. dbają o zapewnienie poufności rozmów prowadzonych z czytelnikami, uczestnikami konkursów lub innymi osobami w ten sposób, żeby treść dotycząca danych osobowych nie mogła być usłyszana przez osoby nieuprawnione,
   4. nie dopuszczają do dostępu do danych osobowych i metod ich zabezpieczania przez osoby nieuprawnione w szczególności poprzez:
      * zakrywanie treści dokumentów w taki sposób, aby osoby obsługiwane nie mogły zapoznać się z ich treścią,
      * bieżącej pracy tylko z dokumentami niezbędnymi do wykonania aktualnego zadania oraz odkładania dokumentów do przeznaczonych do tego segregatorów, szaf lub szuflad po zakończeniu pracy (zasada czystego biurka),
      * uniemożliwienia odczytywania przez osoby nieuprawnione treści wyświetlanych na monitorze poprzez odpowiednie ustawienie monitora i zastosowanie wygaszacza ekranu
      * niszczenia dokumentów, ich projektów lub kopii w przeznaczonych do tego niszczarkach,
      * nie wynoszenie dokumentów zawierających dane osobowe poza siedzibę jednostki,
      * nieudostępnianie dokumentów zawierających dane osobowe osobom nieuprawnionym (również realizując obowiązek dostępu do informacji publicznej na podstawie ustawy o dostępie do informacji publicznej),
      * niepozostawianie bez nadzoru osób nieuprawnionych w pomieszczeniach gdzie przetwarzane są dane osobowe,
      * zamykanie pomieszczeń i niepozostawianie w drzwiach klucza, w sytuacji gdy w pomieszczeniu nie ma osoby upoważnionej.
   5. zapewniają bezpieczeństwo wykorzystywanych systemów informatycznych w szczególności poprzez:
      * zachowanie w poufności identyfikatorów i haseł dostępowych do systemów informatycznych, w tym nieudostępnianie tych elementów innym osobom upoważnionym i osobom nieuprawnionym, nieprzechowywanie zapisanych identyfikatorów i haseł w obszarze stanowiska pracy, niedopuszczenie do możliwości odczytania wprowadzanego do systemu hasła przez osoby nieuprawnione,
      * niewprowadzanie zmian w udostępnionych systemach informatycznych bez wiedzy osoby odpowiedzialnej za ich funkcjonowanie,
      * nieinstalowanie jakichkolwiek programów bez wiedzy osoby odpowiedzialnej za funkcjonowanie systemów informatycznych,
      * nieudzielania zdalnego dostępu do systemów informatycznych osobom nieuprawnionym,
      * korzystanie wyłącznie z programów udostępnionych przez ADO w celu realizacji zadań,
      * korzystanie wyłącznie z zaufanych serwisów internetowych służących realizacji realizowanych zadań,
      * niekorzystanie z portali społecznościowych, poczty elektronicznej i innych serwisów internetowych w celach prywatnych,
      * korzystanie wyłącznie z zaufanych nośników danych udostępnionych przez ADO,
      * dbanie o powierzony do użytkowania sprzęt informatyczny, w tym nieudostępnianie go osobom nieuprawnionym (także osobom znanym i członkom rodzin), niepozostawianie powierzonego sprzętu w miejscach dostępnych osobom nieuprawnionym,
      * stosowanie się do zaleceń osoby odpowiedzialnej za prawidłowe funkcjonowanie systemu informatycznego.

**osoby realizujące:**

* w zakresie nadzoru i monitoringu – ADO, IOD, bezpośredni przełożeni,
* w zakresie spełnienia ww. obowiązków – osoby upoważnione i ich przełożeni.

## Powierzanie przetwarzania danych osobowych

1. ADO w sytuacjach, w których powierza przetwarzanie danych osobowych innemu podmiotowi zawiera z nim stosowną umowę powierzenia.
2. Powierzenie następuje gdy podmiot trzeci będzie przetwarzał dane osobowe w imieniu ADO (np. umowy serwisowe sprzętu zawierającego dane osobowe, dostęp podmiotów zewnętrznych do baz danych ADO w ramach tzw. helpdesk, zlecanie realizacji zadań wymagających przetwarzania danych osobowych podmiotom zewnętrznym, niszczenie dokumentów).
3. Osoby odpowiedzialne za dokonywanie zakupu dostaw i usług w ramach których będą przetwarzane przez podmiot trzeci dane osobowe (w tym na podstawie regulacji wewnętrznych w zakresie zamówień i prawa zamówień publicznych), na etapie wyboru dostawcy zapewniają, że wybrany podmiot będzie zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by przetwarzanie spełniało wymogi RODO.
4. Dopuszczalne jest powierzenie przetwarzania danych osobowych na podstawie innych niż umowa powierzenia instrumentów prawnych (np. porozumienie, akt powołania komisji lub treść statutu w ramach którego tworzona jest jednostka wykonująca zadania w imieniu ADO). W tej sytuacji treść innego instrumentu prawnego musi zawierać co najmniej wszystkie elementy wymagane RODO lub zawierać treść zgodną ze wzorem umowy powierzenia.
5. Wzór umowy powierzenia stanowi załącznik nr 5.5.1.
6. ADO prowadzi w formie elektronicznej lub papierowej rejestr powierzeń przetwarzania danych osobowych.
7. Wzór rejestru powierzeń stanowi załącznik nr 5.5.2.

**osoby realizujące:**

* w zakresie nadzoru w ramach zawieranych umów – ADO, osoby uprawniona do zawierania umów w imieniu ADO,
* w zakresie zapewnienia bieżącego informowania o konieczności powierzenia przetwarzania danych osobowych – osoby upoważnione,
* w zakresie ujęcia treści powierzenia przetwarzania w umowach lub innych instrumentach prawnych – osoby odpowiedzialne za przygotowanie i sprawdzenie umów i innych instrumentów prawnych, w tym radcowie prawni.

## Udostępnianie danych osobowych

1. ADO udostępnia (ujawnia) dane osobowe, za które jest odpowiedzialny, tylko odbiorcom uprawnionym do ich otrzymania:
   1. na podstawie wyraźnej zgody podmiotu danych,
   2. na podstawie obowiązujących przepisów prawa.
2. Dane osobowe udostępniane są:
   1. na podstawie pisemnego wniosku od odbiorcy uprawnionego do otrzymywania danych osobowych na podstawie przepisów,
   2. na podstawie umowy z odbiorcą, w ramach której istnieje konieczność udostępnienia danych i zapewnione są środki ochrony praw i wolności podmiotów danych.
3. Odmawia się udostępnienia danych osobowych w przypadku, gdy spowodowałoby to naruszenie praw i wolności podmiotu danych lub osób trzecich i prawa te są nadrzędne w stosunku do uprawnień odbiorcy. W tym zakresie ADO podejmuje decyzję na podstawie przeprowadzonej analizy. ADO uzasadnia odmowę udostępnienia danych osobowych.
4. ADO zapewnia prowadzenie ewidencji udostępnianych danych osobowych obejmujących informację o odbiorcach, dacie i zakresie udostępnienia.
5. Ewidencja prowadzona jest w formie elektronicznej lub papierowej.
6. Wzór ewidencji stanowi załącznik nr 5.6.1.

**osoby realizujące:**

* w zakresie weryfikacji prawidłowości wniosku i propozycji odpowiedzi – osoba upoważniona, ADO,
* w zakresie udostępniania danych osobowych – ADO,
* w zakresie prowadzenia ewidencji – ADO.

# Środki techniczne służące bezpieczeństwu danych osobowych

## Niszczenie dokumentacji

1. ADO zapewnia osobom upoważnionym odpowiednie urządzenia służące niszczeniu dokumentów.
2. W sytuacji konieczności zniszczenia dużej ilości dokumentacji, czynność ta może zostać zlecona podmiotowi zewnętrznemu z zachowaniem zasad powierzania przetwarzania danych osobowych (pkt. 5.5.).
3. Niedopuszczalne jest wyrzucanie do kosza dokumentów zawierających dane osobowe.
4. Niedopuszczalne jest przekazywanie dokumentów zawierających dane osobowe osobom upoważnionym lub osobom trzecim w celu spalenia lub innej utylizacji.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie niszczenia dokumentów w niszczarkach – osoby upoważnione.

## Zabezpieczenie budynku i pomieszczeń oraz zasady postępowania z kluczami

1. ADO zapewnia możliwość zamykania i zabezpieczania obszarów przetwarzania w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych.
2. ADO wyznacza osoby odpowiedzialne za otworzenie i zamknięcie swojej siedziby oraz filii.
3. Wzór wyznaczenia osób odpowiedzialnych za otworzenie i zamknięcie budynków ADO stanowi zał. nr 6.2.1.
4. Jeżeli ma to zastosowanie, ADO wyznacza osoby które mają dostęp do kodów aktywujących i dezaktywujących system alarmowy na podstawie umowy zawartej z agencją ochrony mienia. Zawarta umowa zapewnia odrębne kody dla każdej z wyznaczonych osób.
5. Osoby wyznaczone odpowiedzialne są za:
   1. wykorzystywanie udostępnionych kluczy zgodnie z przeznaczeniem w godzinach wyznaczonych przez ADO,
   2. staranne zamknięcie wejścia do budynku,
   3. sprawdzenia czy nie doszło do próby włamania i niezwłoczne poinformowanie o takim zdarzeniu,
   4. aktywację i dezaktywację kodu do systemu alarmowego.
6. ADO wyznacza miejsce, w którym przechowywane są klucze do pomieszczeń i zapewnia ich należyte zabezpieczenie przed dostępem osób nieuprawnionych.
7. Niedopuszczalne jest posiadanie przez osoby inne niż wyznaczone zgodnie z pkt. 6.2. 2 kopii kluczy do budynku ADO i pomieszczeń w których przetwarzane są dane osobowe, poza osobami do tego wyznaczonymi.
8. Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania stanowisk pracy oraz wykonania czynności zabezpieczających, adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających w szczególności na:
   1. zabezpieczeniu dokumentacji,
   2. zabezpieczeniu pieczęci,
   3. zabezpieczeniu komputerów,
   4. zabezpieczeniu nośników informacji,
   5. wyłączeniu urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp,
   6. zamknięciu okien i drzwi,
   7. pozostawieniu kluczy od pomieszczeń biurowych w wyznaczonym pomieszczeniu/miejscu.
9. Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu osób upoważnionych, które ponoszą pełną odpowiedzialność za ich zabezpieczenie przed dostępem osób nieuprawnionych.

**osoby realizujące:**

* w zakresie nadzoru – ADO,
* w zakresie dbałości o udostępnione zasoby i uporządkowanie stanowiska pracy – osoby upoważnione
* w zakresie zachowania poufności w zakresie kodów dostępowych – osoby którym przydzielono kody,
* w zakresie dbałości o klucze do budynku – osoby wyznaczone do tego zadania.

## Monitoring wizyjny

1. ADO może prowadzić monitoring wizyjny terenu wokół swojej siedziby i budynków do niego należących w celu zapewnienia bezpieczeństwa osób przebywających na terenie ADO.
2. W celu zapewnienia przejrzystości i rzetelności przetwarzania danych osobowych umieszcza przy każdym wejściu do monitorowanego obszaru lub budynku tabliczkę informującą o tym fakcie. Tabliczka powinna zawierać co najmniej skrót do strony internetowej, na której spełniony jest obowiązek informacyjny opisany w pkt. 2.3. 1. Obowiązek informacyjny w zakresie monitoringu umieszczany jest także na tablicy ogłoszeń/informacyjnej ADO.
3. Przetwarzanie danych osobowych w systemie monitoringu wizyjnego podlega wszystkim zasadom opisanym w niniejszym dokumencie.

**osoby realizujące:**

* w zakresie spełnienia wymagań obowiązku informacyjnego – ADO
* za umieszczenie informacji na stronie www ADO – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Zasady korzystania z portali internetowych oraz poczty elektronicznej

1. Na służbowych komputerach, a także na innych urządzeniach dopuszczonych do pracy w sieci teleinformatycznej ADO, zabrania się korzystania ze stron internetowych do celów prywatnych, w tym do korzystania z portali społecznościowych i rozrywkowych.
2. ADO zapewnia dostęp do kont poczty elektronicznej w domenie, którą zarządza lub u dostawcy usług, który zapewnia możliwość zawarcie umowy powierzenia przetwarzania danych.
3. Niedopuszczalne jest rejestrowanie kont służących realizacji zadań w publicznie dostępnych domenach.
4. Niedopuszczalne jest wykorzystywanie do celów służbowych prywatnych kont poczty elektronicznej osób upoważnionych.
5. ADO zapewnia osobom upoważnionym możliwość oznaczania niechcianej poczty jako spam.
6. Osoba upoważniona odpowiedzialna jest za korzystanie z poczty elektronicznej, w tym każdorazowe weryfikowanie nadawcy i nieotwieranie załączników pochodzących z nieznanego źródła.
7. Przesyłanie drogą mailową pomiędzy osobami upoważnionymi lub przesyłanie odbiorcom danych, danych osobowych o wartości średniej lub wysokiej konieczne jest ich skompresowanie i zaszyfrowanie zaufanym oprogramowaniem i nadanie skompresowanemu plikowi bezpiecznego hasła. Hasło powinno zostać przekazane adresatowi innym środkiem komunikacji niż droga mailowa.

**osoby realizujące:**

* w zakresie zapewnienia niezbędnych zasobów – ADO,
* w zakresie realizacji obowiązków – osoby upoważnione,
* w zakresie utworzenia kont pocztowych – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Monitoring sieci i sprzętu prowadzony przez ADO

1. W przypadku prowadzenia monitoringu ruchu sieciowego oraz pracy na komputerach, ADO informuje o tym fakcie wszystkie osoby, których to dotyczy.
2. Prowadzenie monitoringu nie może naruszać tajemnicy korespondencji.
3. Korzystanie ze zgromadzonych danych dopuszczalne jest wyłącznie za zgodą ADO.

**osoby realizujące:**

* w zakresie zapewnienia niezbędnych zasobów – ADO,
* w zakresie zapewnienie tajemnicy korespondencji oraz nieudostępniania informacji z systemu monitorującego bez wyraźnego polecenia ADO – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Zabezpieczenia przenośnych nośników danych

W celu zabezpieczenia zasobów ADO o wartości średniej lub wysokiej, dozwolone jest używanie wyłącznie nośników danych udostępnionych przez ADO, które są zabezpieczone oprogramowaniem szyfrującym lub szyfrowaniem sprzętowym.

**osoby realizujące:**

* w zakresie zapewnienia niezbędnych zasobów – ADO,
* w zakresie instalacji oprogramowania szyfrującego – osoba odpowiedzialna za funkcjonowanie systemu informatycznego, ASI,
* w zakresie korzystania wyłącznie z udostępnionych przez ADO nośników danych – osoby upoważnione.

## Zarządzanie oprogramowaniem

1. ADO wyznacza osobę odpowiedzialną za instalację i aktualizację oprogramowania oraz osobę odpowiedzialną za zapewnienie sprawnego funkcjonowania systemu informatycznego (ASI).
2. Do zadań ASI może należeć:
   1. monitorowanie oraz zapewnianie ciągłości działania systemów informatycznych,
   2. utrzymywanie, konfigurowanie i monitorowanie wydajności systemów informatycznych,
   3. instalacja i konfiguracja sprzętu i aplikacji,
   4. administracja, w tym aktualizacja, oprogramowania systemowego w celu zachowania bezpieczeństwa i integralności systemów informatycznych oraz zabezpieczenia danych, a w szczególności danych osobowych przed bezprawnym dostępem osób trzecich,
   5. konserwacja oprogramowania i systemów informatycznych,
   6. współpraca z licencjodawcami i innymi dostawcami oprogramowania,
   7. zarządzanie kopiami zapasowymi, w tym danych osobowych zgodnie z otrzymanym upoważnieniem,
   8. dbanie o aktualność oprogramowania antywirusowego.
3. W przypadku wyznaczenia osoby odpowiedzialnej za ww. czynności **niebędącej** pracownikiem ADO należy zapewnić spełnienie zasad powierzania przetwarzania danych osobowych określonych w pkt. 5.5.
4. Powierzenie zadań związanych z instalacją i aktualizacją oprogramowania oraz zapewnieniem sprawnego funkcjonowania systemu informatycznego odbywa się poprzez dokonanie odpowiedniego zapisu w zakresie czynności pracownika ADO lub zapisu w zawartej umowie cywilnoprawnej.
5. Do użytkowania może być dopuszczone tylko oprogramowanie, które posiada licencję lub dokument równoważny upoważniający do zainstalowania i użytkowania.
6. Osoba odpowiedzialna za zapewnienie sprawnego działania systemów informatycznych prowadzi ewidencję wykorzystywanego u ADO oprogramowania.
7. Ewidencja prowadzona jest w formie elektronicznej lub papierowej. Dopuszczalne jest prowadzenie ewidencji oprogramowania poprzez wykorzystanie zaufanego oprogramowania audytowego.
8. Wzór ewidencji oprogramowania stanowi załącznik nr 6.7.1.
9. Zabrania się instalowania i/lub użytkowania oprogramowania:
   1. naruszającego prawa autorskie,
   2. naruszającego warunki licencji,
   3. do celów prywatnych.
10. Osoby upoważnione mogą korzystać wyłącznie z kont z uprawnieniami użytkownika.
11. ASI korzysta z konta o uprawnieniach administracyjnych tylko w sytuacji wykonywania zadań związanych z instalacją i aktualizacją oprogramowania oraz zapewnieniem sprawnego funkcjonowania systemu informatycznego. W przypadku wykonywania innych zadań zobowiązany jest korzystać z konta o uprawnieniach użytkownika.
12. Dopuszczalne jest stosowanie zdalnego dostępu do komputerów będących w zasobach ADO w ramach pomocy technicznej pod warunkiem zapewnienia szyfrowanego połączenia i innych mechanizmów zapewniających nienaruszalność praw i wolności podmiotów danych oraz zawarcia zapisów o szczegółowej realizacji tego wymogu w umowie powierzenia przetwarzania danych osobowych.

**osoby realizujące:**

* w zakresie zapewnienia niezbędnych zasobów – ADO,
* w zakresie zapewnienia zgodnej z wymaganiami niniejszej dokumentacji pracy i konfiguracji systemów informatycznych, w tym zgłaszania ADO niezbędnych potrzeb – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

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

1. Podstawową metodą uwierzytelniania użytkowników w systemie informatycznym są identyfikator użytkownika i hasło.
2. Identyfikator użytkownika nadawany jest przez administratora systemu (ASI) zgodnie z wymogami systemu.
3. Hasło początkowe nadaje użytkownikowi ASI, a następnie przekazuje je użytkownikowi po zweryfikowaniu tożsamości osoby. Niedopuszczalne jest w szczególności:
   1. przekazywanie hasła za pośrednictwem osób trzecich,
   2. przekazywanie hasła telefonicznie lub za pomocą poczty elektronicznej.
4. Niezależnie od wartości zasobu danych osobowych przetwarzanych w danym systemie stosowane hasła powinny zawierać co najmniej 8 znaków, w tym duże i małe litery, znaki interpunkcyjne, cyfry i znaki specjalne. Hasła powinny być łatwe do zapamiętania, jednakże nie powinny być oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby lub osób bliskich (np. imiona, numery telefonów, daty urodzenia itp.).
5. Osoba upoważniona jest zobowiązana do zachowania haseł w poufności i nieudostępniania ich nikomu.

**osoby realizujące:**

* w zakresie zapewnienia zgodnej z wymaganiami niniejszego punktu pracy i konfiguracji systemów informatycznych – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI,
* w zakresie stosowania haseł zapewnienia zgodnych z ww. wymaganiami – osoby upoważnione (użytkownicy systemu informatycznego).

# Bezpieczeństwo

## Analiza ryzyka

1. ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.
2. ADO przeprowadza i dokumentuje analizę stosowanych środków bezpieczeństwa danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i skutkach dla dostępności integralności i poufności danych.
3. W ramach analizy ryzyka ADO identyfikuje i ocenia stosowane mechanizmy kontroli ryzyka, dla poszczególnych zagrożeń, a w przypadku stwierdzenia takiej potrzeby planuje i wdraża uwzględniając koszty i aktualny stan wiedzy nowe metody kontroli ryzyka zapewniające zadowalający poziom bezpieczeństwa.
4. Analiza ryzyka przeprowadzana jest nie rzadziej niż raz na rok.
5. Analizy ryzyka prowadzona jest z udziałem:
   1. ADO,
   2. osoby odpowiedzialnej za funkcjonowanie danego systemu informatycznego, ASI,
6. Metodologia stosowanej analizy ryzyka stanowi załącznik nr 7.1.1.

**osoby realizujące:**

* w zakresie planowania analizy ryzyka i wskazania osób biorących udział w tym procesie – ADO,
* w zakresie przeprowadzenia analizy ryzyka – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI, IOD, inne osoby wyznaczone przez ADO.

## Ocena skutków dla ochrony danych

1. Przed rozpoczęciem przetwarzania danych osobowych, który ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO dokonuje oceny skutków planowanych czynności przetwarzania dla ochrony danych.
2. Ocena skutków dla ochrony danych, jest wymagana w szczególności w przypadku:
   1. 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,
   2. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa,
   3. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
3. Dokonując oceny skutków dla ochrony danych ADO konsultuje się z IOD.
4. Ocena skutków przetwarzania dla ochrony danych zawiera co najmniej:
   1. opis planowanych operacji przetwarzania,
   2. opis celów przetwarzania, w tym prawnie uzasadnionych interesów realizowanych przez administratora jeżeli stanowią podstawę przetwarzania,
   3. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
   4. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
   5. planowane środki organizacyjne i techniczne mające na celu minimalizację zidentyfikowanych ryzyk, w tym metody kontroli ryzyka (zabezpieczenia) środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i możliwość wypełnienia praw i prawnie uzasadnionych interesów podmiotów danych.
5. ocena ryzyka nie jest przeprowadzana dla zadań, których wykonanie jest obowiązkiem ADO wynikającym z przepisów prawa.

**osoby realizujące:**

* w zakresie weryfikacji konieczności przeprowadzenia oceny skutków dla ochrony danych i wskazania osób biorących udział w tym procesie – ADO, IOD,
* w zakresie przeprowadzenia oceny skutków dla ochrony danych – ADO, inne osoby wyznaczone przez ADO.

# Incydenty bezpieczeństwa ochrony danych osobowych

## Naruszenia

1. Do typowych naruszeń zagrażających ochronie danych osobowych należą:
   1. zdarzenia losowe zewnętrzne (np. utrata zasilania, utrata łączności, zalanie, pożar),
   2. zdarzenia losowe wewnętrzne (np. awarie serwera, urządzeń sieciowych, komputerów, dysków, oprogramowania, pomyłki użytkowników, utrata danych),
   3. zdarzenia zewnętrzne umyślne (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub informacji, kradzież lub zagubienie sprzętu, ujawnienie danych osobom nieuprawnionym, świadome zniszczenie dokumentów/danych dokonane przez osoby nierealizujące zadań na rzecz ADO lub działanie wirusów i innego szkodliwego oprogramowania),
   4. zdarzenia wewnętrzne umyślne (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub informacji, kradzież lub zagubienie sprzętu, ujawnienie danych osobom nieuprawnionym, świadome zniszczenie dokumentów/danych, dokonane przez osoby realizujące zadania na rzecz ADO lub działanie wirusów i innego szkodliwego oprogramowania, niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów zawierających dane),
   5. nieprzestrzeganie przez pracowników zasad ochrony danych (np. niestosowanie ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, stosowanie kluczy do pomieszczeń służbowych innych niż wydane przez ADO),
   6. zdarzenia nieumyślne będące skutkiem nieszczęśliwych wypadków.
2. Naruszenia mogą występować pojedynczo, na jednym stanowisku lub na wielu stanowiskach jednocześnie.

## Postępowanie w przypadku zaistnienia naruszenia

1. W sytuacji podejrzenia zaistnienia naruszenia każdy pracownik:
   1. w pierwszej kolejności powinien zadbać o własne bezpieczeństwo,
   2. w miarę swoich możliwości powinien zminimalizować skutki naruszenia, w tym celu może także poprosić o pomoc współpracowników, bezpośrednich przełożonych, ASI, IOD lub osoby odpowiedzialne za ochronę budynku,
   3. informuje bezpośredniego przełożonego lub ADO.
2. ADO podejmuje wszelkie możliwe działania mające na celu minimalizację skutków naruszeń.
3. ADO, zależnie od charakteru zdarzenia, wskazuje osoby, które zajmą się obsługą naruszenia, identyfikacją jego przyczyn i skutków dla ochrony danych.

**osoby realizujące:**

* w zakresie zgłaszania podejrzeń incydentów i minimalizacji skutków – osoby upoważnione, osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI,
* w zakresie obsługi zdarzenia i minimalizacji skutków – osoby wskazane przez ADO,
* w zakresie wskazania osoby prowadzącej postępowanie – ADO.

## Postępowanie wyjaśniające

1. Postępowanie wyjaśniające prowadzi osoba lub osoby wskazane przez ADO.
2. Osoba prowadząca postępowanie:
   1. ustala charakter i lokalizację zaistnienia naruszenia,
   2. ustala rodzaj naruszenia, w tym ilość i zakres danych osobowych, które zostały zagrożone w wyniku naruszenia,
   3. ustala okoliczności towarzyszące naruszeniu,
   4. wskazuje podjęte lub konieczne do podjęcia działania w celu minimalizacji skutków naruszenia,
   5. ustala przyczyny wystąpienia naruszenia i dokonuje ich oceny,
   6. proponuje środki naprawcze w celu odwrócenia skutków naruszenia i zapobieżenia jego ponownemu wystąpieniu.
3. wszystkie osoby upoważnione udzielają niezbędnych informacji, przygotowują oświadczenia i zabezpieczają niezbędne dokumenty na żądanie osoby prowadzącej postępowanie wyjaśniające.
4. Z prowadzonego postępowania sporządzany jest raport.
5. Wzór raportu stanowi załącznik nr 8.3.1.
6. ADO podejmuje decyzje o stosowanych środkach naprawczych.

**osoby realizujące:**

* w zakresie prowadzenia postępowania – osoba wskazana przez ADO,
* w zakresie pomocy osobie prowadzącej postępowanie wyjaśniające – osoby upoważnione, osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI,
* w zakresie zatwierdzenia raportu z postępowania wyjaśniającego i decyzji o środkach naprawczych – ADO.

## Ewidencjonowanie incydentów i informowanie organu nadzorczego i podmiotu danych

1. W sytuacji gdy naruszenie powoduje małe prawdopodobieństwo naruszenia praw i wolności podmiotów danych – odnotowywany jest w rejestrze incydentów.
2. Wzór rejestru incydentów stanowi załącznik nr 8.4.1.
3. W sytuacji gdy naruszenie powoduje większe niż małe prawdopodobieństwo naruszenia praw i wolności podmiotów danych, ADO informuje organ nadzorczy nie później niż 72 godziny od stwierdzenia naruszenia. W tym celu ADO przygotowuje zgłoszenie i przesyła je organowi nadzorczemu w formie elektronicznej.
4. W zakresie, w jakim nie da się udzielić organowi nadzorczemu pełnej informacji w terminie wskazanym powyżej, można je udzielać sukcesywnie bez zbędnej zwłoki.
5. Wzór zgłoszenia stanowi załącznik nr. 8.4.2.
6. W sytuacji gdy naruszenie powoduje wysokie prawdopodobieństwo naruszenia praw i wolności podmiotów danych, ADO informuje podmioty danych bez zbędnej zwłoki.
7. Zawiadomienie sporządzone jest jasnym i prostym językiem, opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej:
   1. dane kontaktowe IOD,
   2. opis możliwych konsekwencji naruszenia ochrony danych osobowych,
   3. opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych,
   4. opis środków zastosowanych w celu zminimalizowania jego ewentualnych negatywnych skutków – jeżeli ma to zastosowanie.
8. ADO może odstąpić od poinformowania podmiotów danych o naruszeniu w sytuacji gdy:
   1. naruszenie dotyczyło danych osobowych, które zostały zanonimizowane, zaszyfrowane lub zabezpieczone środkami technicznymi i organizacyjnymi uniemożliwiającymi odczyt tych danych przez osoby nieuprawnione,
   2. ADO zastosował po zaistnieniu naruszenia środki eliminujące wysokie ryzyko naruszenia praw lub wolności podmiotu danych,
   3. wymagałoby ono niewspółmiernie dużego wysiłku – w takim przypadku ADO wydaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

**osoby realizujące:**

* w zakresie prowadzenia rejestru incydentów – ADO,
* w zakresie uzupełniania informacji w rejestrze incydentów – osoba prowadząca postępowanie,
* w zakresie przygotowania treści zgłoszenia – osoba prowadząca postępowanie,
* w zakresie dokonania zgłoszenia do organu nadzorczego – ADO,
* w zakresie podjęcia decyzji o odstąpieniu od zgłoszenia naruszenia organowi nadzorczemu lub o nieinformowaniu podmiotów danych – ADO,
* w zakresie informowania podmiotów danych o incydencie – osoby wskazane przez ADO.

# Inspektor Ochrony Danych

## Wybór i wyznaczenie IOD

1. ADO podejmuje decyzję o wyznaczeniu IOD na podstawie oceny jego fachowej wiedzy i znajomości praktyk z zakresu ochrony danych osobowych oraz umiejętności wypełniania zadań.
2. ADO obowiązkowo wyznacza IOD gdy:
   1. jest podmiotem publicznym w rozumieniu art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
   2. jest instytutem badawczym w rozumieniu ustawy o instytutach badawczych,
   3. jego główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
   4. jego główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących lub naruszeń prawa.
3. Wzór wyznaczenia IOD stanowi załącznik nr 9.1.1.
4. W przypadku wyznaczenia IOD, ADO zgłasza ten fakt organowi nadzorczemu w terminie 14 dni od dnia jego wyznaczenia.
5. Zgłoszenie organowi nadzorczemu sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.
6. Wzór zgłoszenia stanowi zał. nr 9.1.2.
7. ADO umieszcza na swojej stronie internetowej następujące dane IOD:
   1. imię i nazwisko,
   2. adres poczty elektronicznej przydzielonej IOD.
8. Adres poczty elektronicznej powinien być przydzielony w domenie internetowej jednostki. ADO powinien przydzielić IOD oddzielne, służbowe konto poczty elektronicznej.
9. ADO w terminie 14 dni zawiadamia w sposób opisany w pkt. 9.1. 5 organ nadzorczy o:
   1. odwołaniu IOD,
   2. zmianie danych kontaktowych IOD,
   3. zmianie swoich danych teleadresowych.

**osoby realizujące:**

* w zakresie wyznaczenia i wyboru IOD – ADO,
* w zakresie przygotowania zgłoszenia wyznaczenia IOD lub zmian w tym zakresie – osoba wyznaczona przez ADO,
* w zakresie stworzenia konta poczty elektronicznej oraz umieszczenia informacji o IOD na stronie ADO – osoba odpowiedzialna za funkcjonowanie danego systemu informatycznego, ASI.

## Pozycja IOD

1. ADO zapewnia niezależność IOD poprzez:
   1. zapewnienie organizacyjnej podległości bezpośrednio najwyższemu kierownictwu ADO lub bezpośrednio ADO,
   2. unikanie wydawania poleceń dotyczących sposobu realizacji zadań IOD – ograniczenie to obowiązuje zarówno ADO jak i osoby przez niego upoważnione,
   3. zakaz karania w żadnej formie (pośredniej lub bezpośredniej) lub odwoływania IOD za wykonywane czynności związane z ochroną danych osobowych,
   4. taką organizację pracy i zlecanie IOD innych zadań, które nie powodują konfliktu interesów.
2. ADO informuje IOD o wszystkich sprawach związanych z ochroną danych osobowych i stosuje się do jego zaleceń w tym zakresie.
3. ADO zapewnia wszelkie niezbędne zasoby IOD, które umożliwią mu wykonywanie zadań, w tym poprzez:
   1. wspieranie IOD w realizacji zadań przez kadrę kierowniczą,
   2. zapewnienie dostępu do zasobów ADO umożliwiających realizację zadań,
   3. umożliwienie dostępu do wszystkich działów i stanowisk pracy ADO w celu wykonywania zadań związanych z ochroną danych osobowych,
   4. zapewnienie szkoleń lub środków finansowych na szkolenie IOD,
   5. jeżeli to niezbędne – powołanie zespołu wspierającego działania IOD.
4. ADO konsultuje z IOD:
   1. konieczność przeprowadzenia oceny skutków dla ochrony danych oraz ewentualną konieczność zlecenia tej oceny podmiotowi zewnętrznemu,
   2. dobór metodologii przeprowadzenia oceny skutków dla ochrony danych,
   3. prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z wymogami ochrony danych
   4. stosowane zabezpieczenia, w tym środki techniczne i organizacyjne stosowanych do łagodzenia wszelkich zagrożeń praw i interesów podmiotów danych.
5. ADO osobowych podejmuje wszelkie ostateczne decyzje w zakresie ochrony danych osobowych.

**osoby realizujące:**

* w zakresie zapewnienia niezależności, wsparcia i niezbędnych zasobów IOD – ADO,
* w zakresie bieżącego kontaktu z IOD w sytuacjach związanych z ochroną danych osobowych – osoby upoważnione.

## Zadania Inspektora Ochrony Danych

1. IOD monitoruje działania ADO i wspiera go w przestrzeganiu przepisów prawa w zakresie ochrony danych osobowych i wspomaga w podejmowaniu decyzji w tym zakresie. W tym celu IOD:
   1. zbiera informacje w celu identyfikacji czynności przetwarzania,
   2. analizuje i sprawdza zgodność tego przetwarzania,
   3. informuje, doradza i rekomenduje określone działania.
2. IOD współpracuje z organem nadzorczym i stanowi punkt kontaktowy dla tego organu w szczególności, w zakresie:
   1. związanym z przetwarzaniem danych osobowych,
   2. uprzednich konsultacji jeżeli jest to wymagane przepisami,
   3. wszelkich innych spraw, jeżeli jest to wymagane przepisami.
3. IOD wykonuje swoje zadania z uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
4. IOD wspiera i doradza ADO w zakresie prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania.
5. IOD może wykonywać inne czynności niezwiązane z ochroną danych osobowych jeżeli nie będą one powodowały konfliktu interesów z podstawową działalnością IOD.
6. IOD prowadzi w formie elektronicznej rejestr podjętych czynności, w którym ewidencjonuje wszystkie podjęte działania związane z ochroną danych osobowych. Rejestr, na koniec każdego roku lub na żądanie, przekazywany jest ADO.
7. Wzór rejestru podjętych czynności stanowi załącznik nr 9.3.1.