

Polityka bezpieczeństwa

29.05.2026

Spis treści

1. Wstęp	2
1.1 Słowniczek	2
1.2 Polityka bezpieczeństwa i cel jej stosowania	2
1.3 Podstawowe zasady ochrony danych osobowych	3
2. Podmioty zaangażowane w ochronę danych osobowych i ich obowiązki	3
2.1 Administrator danych osobowych.....	3
2.2 Inspektor ochrony danych	4
2.3 Administrator systemów informatycznych	4
2.4 Osoby upoważnione do przetwarzania danych osobowych	5
2.5 Osoby przebywające w obszarze przetwarzania danych osobowych	5
3. Zasady przetwarzania danych osobowych	6
4. Przekazywanie danych osobowych w ramach współpracy z podmiotami zewnętrznymi	6
5. Środki stosowane w celu zapewnienia bezpieczeństwa danych osobowych	7
5.1 Rozwiązania organizacyjne	7
5.2 Zabezpieczenia fizyczne.....	8
5.3 Rozwiązania informatyczne	8
6. Naruszenia ochrony danych osobowych.....	8
7. Postanowienia końcowe.....	9
8. Załączniki	9

29.05.2026

(data wejścia w życie i podpis osoby reprezentującej najwyższe kierownictwo)

1. Wstęp

1.1 Słowniczek

Administrator danych osobowych / Administrator / ADO - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

W rozumieniu Polityki bezpieczeństwa Administratorem jest **Instytut Skrzynki** – Instytut Dokumentacji, Rozwoju i Promocji Dziedzictwa Kulturowego i Kulinarnego Powiatu Poznańskiego z siedzibą w Skrzynkach, przy pl. Parkowy 1, 62-060 Skrzynki.

inspektor ochrony danych / IOD - osoba wspierająca ADO w realizacji obowiązków, wynikających z przepisów o ochronie danych osobowych (w tym RODO i Ustawy).

obszar przetwarzania danych osobowych - teren, na którym ADO dokonuje przetwarzania danych osobowych w formie papierowej lub elektronicznej.

podmiot przetwarzający / procesor - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

Prezes Urzędu Ochrony Danych Osobowych / Prezes UODO - organ właściwy do spraw ochrony danych osobowych w Polsce; organ nadzorczy w rozumieniu RODO.

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)

Polityka bezpieczeństwa - ten dokument.

Ustawa - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

1.2 Polityka bezpieczeństwa i cel jej stosowania

1. Polityka bezpieczeństwa jest polityką ochrony danych w rozumieniu art. 24 ust. 2 RODO.
2. Polityka bezpieczeństwa została opracowana z uwzględnieniem:
 - 1) powszechnie obowiązujących przepisów prawa, związanych z ochroną danych osobowych i bezpieczeństwem informacji, w szczególności RODO,
 - 2) wytycznych Prezesa UODO i innych organów zaangażowanych w ochronę danych osobowych,
 - 3) dobrych praktyk, wytycznych lub standardów branży lub sektora, który reprezentuje ADO.
3. Polityka bezpieczeństwa służy zapewnieniu takiego poziomu bezpieczeństwa przetwarzanych przez ADO danych osobowych, który uchroni je przed:
 - 1) dostępem osób nieupoważnionych,
 - 2) nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Polityka bezpieczeństwa jest poddawana okresowym przeglądom. W razie potrzeby dokonuje się stosownych zmian jej treści, przy uwzględnieniu w szczególności:
 - 1) przepisów lub wytycznych, o których mowa w ust. 2 powyżej,
 - 2) aktualnego stanu wiedzy technicznej,
 - 3) możliwości logistycznych, kadrowych i finansowych ADO.
5. Integralną część Polityki bezpieczeństwa stanowią załączniki do niej, wskazane w rozdziale 8. Ponadto ADO może wprowadzać - lub dopuszczać do stosowania - dodatkowe wytyczne,

regulaminy i instrukcje, mające na celu realizację zasad ochrony danych osobowych i bezpieczeństwa informacji, opisanych w Polityce bezpieczeństwa.

6. Polityka bezpieczeństwa jest dokumentem wewnętrznym ADO. Jej treść nie może być udostępniana osobom lub podmiotom nieupoważnionym.

1.3 Podstawowe zasady ochrony danych osobowych

1. ADO zapewnia realizację następujących zasad wykorzystania danych osobowych:
 - 1) zgodność z prawem, rzetelność i przejrzystość,
 - 2) ograniczenie celu,
 - 3) minimalizacja danych,
 - 4) prawidłowość,
 - 5) ograniczenie przechowywania,
 - 6) integralność i poufność,- w rozumieniu RODO i innych przepisów prawa.
2. ADO wykazuje przestrzeganie zasad ochrony danych osobowych i bezpieczeństwa informacji w szczególności poprzez:
 - 1) Politykę bezpieczeństwa,
 - 2) dodatkowe wytyczne, regulaminy i instrukcje,
 - 3) papierowe lub elektroniczne wykazy, ewidencje, notatki służbowe lub korespondencję.

2. Podmioty zaangażowane w ochronę danych osobowych i ich obowiązki

2.1 Administrator danych osobowych

1. ADO decyduje o celach i środkach przetwarzanych danych osobowych.
2. ADO podejmuje działania, mające na celu zapewnienie:
 - 1) odpowiedniego poziomu bezpieczeństwa danych osobowych
 - 2) zgodności przetwarzania danych osobowych z zasadami, o których mowa w rozdziale 1.3 powyżej.
3. Działania ADO, o których mowa w ust. 2 powyżej, obejmują w szczególności:
 - 1) wdrażanie odpowiednich rozwiązań organizacyjnych, zabezpieczeń fizycznych i rozwiązań informatycznych (wskazanych w rozdziale 5 Polityki bezpieczeństwa i załącznikach do Polityki bezpieczeństwa),
 - 2) nadawanie upoważnień osobom, które w celach służbowych posiadają dostęp do danych osobowych,
 - 3) zapewnienie kontroli nad osobami przebywającymi w obszarze przetwarzania danych osobowych.
4. Jeżeli osoba, której dane dotyczą, wykaże ADO, że dane osobowe jej dotyczące są niekompletne, nieaktualne, nieprawdziwe, zebrane z naruszeniem prawa lub zbędne do realizacji celu, dla którego je zebrano - ADO jest zobowiązany do podjęcia niezbędnych kroków, mających na celu naprawę tego stanu rzeczy.
5. ADO prowadzi rejestr czynności przetwarzania, zgodnie z art. 30 ust. 1 RODO. **Wzór rejestru stanowi załącznik nr 9 do Polityki bezpieczeństwa.**
6. ADO dokonuje analizy ryzyka czynności przetwarzania danych osobowych (zgodnie z art. 32 ust. 2 RODO). Jeżeli w wyniku analizy zostanie ustalone, że czynność przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (lub gdy taki obowiązek wynika z przepisów prawa bądź wytycznych organu nadzorczego), ADO dokonuje

także oceny skutków (zgodnie z art. 35 ust. 1 RODO). **Analiza ryzyka i ocena skutków są dokonywane zgodnie z wytycznymi, stanowiącymi załącznik nr 1 do Polityki bezpieczeństwa.**

7. Jeżeli doszło do naruszenia ochrony danych osobowych, ADO niezwłocznie podejmuje odpowiednie kroki, mające na celu realizację obowiązków opisanych w art. 33-34 RODO. **Procedura postępowania z naruszeniami została opisana w rozdziale 6 Polityki bezpieczeństwa oraz w załączniku nr 3 do Polityki bezpieczeństwa.**
8. ADO wyznacza inspektora ochrony danych (IOD).

2.2 Inspektor ochrony danych

1. W dniu wejścia w życie dokumentu ADO nie wyznaczył IOD. W przypadku powołania przez ADO IOD do jego zadań należy wspieranie ADO i innych podmiotów zaangażowanych w ochronę danych osobowych, w szczególności poprzez:
 - 1) informowanie o obowiązkach związanych z ochroną danych osobowych i doradzanie w tej sprawie,
 - 2) monitorowanie przestrzegania przepisów oraz polityk ADO lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
 - 3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
 - 4) współpraca z organem nadzorczym,
 - 5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz, w stosownych przypadkach, prowadzenie konsultacji we wszelkich innych sprawach,
 - 6) wspieranie ADO w realizacji obowiązków wskazanych w Polityce bezpieczeństwa lub dodatkowych wytycznych, regulaminach lub instrukcjach.
2. W sytuacji wyznaczenia IOD dane kontaktowe IOD (imię, nazwisko, adres e-mail):
 - 1) są publikowane na stronie internetowej ADO lub - jeśli ADO nie posiada strony internetowej - w sposób ogólnie dostępny w miejscu prowadzenia działalności,
 - 2) są zgłaszane Prezesowi UODO w sposób opisany w art. 10 Ustawy,
3. W dokumencie, na mocy którego ADO powołuje IOD, osoba powołana do pełnienia tej funkcji jest wskazywana z imienia i nazwiska.
4. IOD podlega bezpośrednio najwyższemu kierownictwu ADO.
5. ADO może powołać zastępcę IOD w sposób wskazany w art. 11a Ustawy. Wprowadzone u ADO uregulowania, dotyczące IOD, stosuje się wówczas odpowiednio do zastępcy IOD.

2.3 Administrator systemów informatycznych

1. ADO może wyznaczyć na ASI osobę współpracującą z ADO lub powierzyć wykonywanie obowiązków ASI podmiotowi zewnętrznemu.
2. Do zadań ASI należy zapewnienie przestrzegania zasad ochrony danych osobowych lub bezpieczeństwa informacji, przetwarzanych za pomocą aplikacji, programów, systemów lub urządzeń wykorzystywanych przez ADO, w szczególności przez realizację zadań i działań wskazanych w **załączniku nr 11 do Polityki bezpieczeństwa.**
3. ASI podlega bezpośrednio najwyższemu kierownictwu ADO.
4. Jeżeli ADO nie wyznaczył ASI, za realizację obowiązków wskazanych w ust. 2 powyżej odpowiada ADO lub osoba wskazana przez ADO. Wprowadzone u ADO uregulowania, dotyczące ASI, stosuje się wówczas odpowiednio do ADO lub osoby wskazanej przez ADO.

2.4 Osoby upoważnione do przetwarzania danych osobowych

1. Do przetwarzania danych u ADO dopuszczone są jedynie osoby upoważnione przez ADO.
2. Upoważnienie jest nadawane zgodnie ze wzorem, stanowiącym **załącznik nr 13 do Polityki bezpieczeństwa** oraz procedurą, stanowiącą **załącznik nr 12 do Polityki bezpieczeństwa**. ADO może dopuścić - po konsultacji z IOD - nadanie upoważnienia w inny sposób, np. przez zawarcie treści upoważnienia w umowie będącej podstawą współpracy z daną osobą.
3. Po nadaniu upoważnienia do przetwarzania danych osobowych osoba upoważniona otrzymuje od ASI (lub osoby wskazanej przez ASI) dostęp do aplikacji, programów, systemów lub urządzeń niezbędnych do wykonywania jej obowiązków. W trakcie pracy osoba upoważniona jest zobowiązana do przestrzegania zaleceń związanych z pracą w systemach, na komputerach i innych urządzeniach, opisanych w **załączniku nr 7 do Polityki bezpieczeństwa**.
4. Osoba upoważniona do przetwarzania danych osobowych:
 - 1) jest zobowiązana do przestrzegania:
 - a) Polityki bezpieczeństwa,
 - b) innych obowiązujących u ADO wytycznych, regulaminów lub instrukcji dotyczących ochrony danych osobowych lub bezpieczeństwa informacji,
 - c) poleceń ADO, IOD lub ASI związanych z ochroną danych osobowych lub bezpieczeństwem informacji.
 - 2) jest zobowiązana do zachowania w tajemnicy zarówno danych osobowych, jak i sposobów ich zabezpieczenia,
 - 3) zgłaszania naruszeń lub podejrzeń naruszeń bezpieczeństwa danych osobowych, zgodnie z procedurą wskazaną w rozdziale 6 Polityki.
5. Działanie lub zaniechanie osoby upoważnionej, w wyniku którego doszło do naruszenia przestrzegania procedur lub poleceń, wskazanych w ust. 5 powyżej, może:
 - 1) mieć konsekwencje dyscyplinarne,
 - 2) zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych (w przypadku współpracy na podstawie Kodeksu pracy),
 - 3) zostać uznane za ważny powód uzasadniający wypowiedzenie lub rozwiązanie umowy będącej podstawą współpracy.
6. Po zakończeniu współpracy z ADO:
 - 1) upoważnienie do przetwarzania danych osobowych automatycznie wygasa,
 - 2) dostęp osoby upoważnionej do używanych przez nią aplikacji, programów, systemów lub urządzeń jest odbierany lub blokowany.

2.5 Osoby przebywające w obszarze przetwarzania danych osobowych

1. Osoby współpracujące z ADO, które w związku z realizacją swoich obowiązków przebywają na obszarze przetwarzania danych osobowych i których zakres obowiązków nie uzasadnia nadania upoważnienia do przetwarzania danych osobowych, podpisują oświadczenie o poufności, którego **wzór stanowi załącznik nr 4 do Polityki bezpieczeństwa**.
2. Osoby, o których mowa w ust. 1 powyżej, w przypadku wejścia w posiadanie danych osobowych lub informacji o ich zabezpieczeniach, są zobowiązane do zachowania tajemnicy w tym zakresie, zarówno w trakcie współpracy z ADO, jak i po jej zakończeniu.
3. Osoby, o których mowa w ust. 1 powyżej, w razie powzięcia informacji o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych, są zobowiązane do zawiadomienia o tym IOD lub bezpośredniego przełożonego.
4. Jeżeli osoby, o których mowa w ust. 1 powyżej, realizują swoje obowiązki w imieniu i na rzecz kontrahenta, którego łączy z ADO umowa o świadczenie usług, obowiązek wskazany w ust. 1 powyżej może być zastąpiony odpowiednim zobowiązaniem umownym.

3. Zasady przetwarzania danych osobowych

1. Przetwarzanie danych osobowych przez ADO jest dopuszczalne w razie istnienia przynajmniej jednej z podstaw, wskazanych w:
 - 1) art. 6 ust. 1 RODO - w zakresie danych osobowych zwykłych,
 - 2) art. 9 ust. 2 RODO - w zakresie szczególnych kategorii danych.
2. W zakresie przetwarzania danych w oparciu o podstawy wskazane w ust. 1 powyżej ADO wykorzystuje wzory zgód, oświadczeń itp. treści oraz procedur związanych z ich stosowaniem, przygotowane lub zatwierdzone do stosowania przez IOD.
3. W razie wątpliwości dotyczących podstaw prawnych dla przetwarzania danych osobowych ADO dokonuje konsultacji z IOD. Jeżeli:
 - 1) ADO nie dokonuje jeszcze przetwarzania danych, którego dotyczy wątpliwość - przetwarzanie danych może mieć miejsce dopiero po rozstrzygnięciu wątpliwości,
 - 2) ADO dokonuje już przetwarzania danych, którego dotyczy wątpliwość - do czasu rozstrzygnięcia wątpliwości ADO podejmuje kroki mające na celu wstrzymanie przetwarzania danych osobowych.
4. Wobec osób, których dane osobowe ADO przetwarza, realizowany jest - na zasadach określonych w art. 13-14 RODO - obowiązek informacyjny. W uzasadnionych sytuacjach, uzgodnionych z IOD, dopuszczalne jest warstwowe spełnianie obowiązku informacyjnego. ADO wykorzystuje w tym zakresie wzory obowiązków informacyjnych i procedur z nimi związanych, przygotowane lub zatwierdzone do stosowania przez IOD.
5. ADO przyjmuje wnioski związane z prawami osób, których dane dotyczą, określone w art. 15-22 RODO. Przy realizacji tych zadań ADO dba w szczególności o:
 - 1) potwierdzenie tożsamości i uprawnień wnioskodawców,
 - 2) przekazywanie informacji w sposób jasny, czytelny i zrozumiały,
 - 3) łatwość dostępu do danych,
 - 4) udzielanie odpowiedzi na wnioski w terminach wskazanych w art. 12 ust. 3 RODO.
6. **Procedura realizacji wniosków z art. 15-22 RODO stanowi załącznik nr 8 do Polityki bezpieczeństwa.**
7. ADO dokumentuje sposób realizacji praw osób, których dane dotyczą. Dokumentowanie może następować w szczególności przez gromadzenie korespondencji związanej z wnioskami lub inny, uzgodniony z IOD sposób.

4. Przekazywanie danych osobowych w ramach współpracy z podmiotami zewnętrznymi

1. W sytuacji, w której:
 - 1) ADO przekazuje dane osobowe podmiotowi zewnętrznemu, gdzie ADO decyduje o celach i środkach wykorzystania danych osobowych - ADO stosuje wytyczne z ust. 2 poniżej,
 - 2) podmiot zewnętrzny przekazuje dane osobowe ADO, gdzie podmiot zewnętrzny decyduje o celach i środkach wykorzystania danych osobowych - ADO stosuje wytyczne z ust. 3 poniżej,
 - 3) ADO przekazuje dane osobowe podmiotowi zewnętrznemu, gdzie każda ze stron realizuje własne cele wykorzystania danych osobowych - ADO stosuje wytyczne z ust. 4 poniżej,
 - 4) podmiot zewnętrzny przekazuje dane osobowe ADO, gdzie każda ze stron realizuje własne cele wykorzystania danych osobowych - ADO stosuje wytyczne z ust. 4 poniżej,

- 5) ADO wspólnie z podmiotem zewnętrznym lub podmiotami zewnętrznymi wspólnie decydują o celach wykorzystania danych osobowych - ADO stosuje wytyczne z ust. 5 poniżej.
2. W sytuacji, gdy ADO powierza przetwarzanie danych osobowych podmiotowi zewnętrznemu jako podmiotowi przetwarzającemu, stosuje się następujące wytyczne:
 - 1) przed rozpoczęciem współpracy ADO weryfikuje, czy podmiot zewnętrzny zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Weryfikacja może nastąpić w szczególności poprzez zobowiązanie podmiotu zewnętrznego do wypełnienia **ankiety, stanowiącej załącznik nr 5 do Polityki bezpieczeństwa**,
 - 2) powierzenie przetwarzania danych osobowych następuje w drodze podpisania umowy powierzenia, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do umowy głównej. **Wzór umowy powierzenia stanowi załącznik nr 6 do Polityki bezpieczeństwa** (w porozumieniu z IOD możliwe jest wykorzystanie innego wzoru umowy powierzenia, w szczególności przekazanego przez drugą stronę umowy).
3. W sytuacji, gdy podmiot zewnętrzny powierzenia przetwarzanie danych osobowych ADO jako podmiotowi przetwarzającemu, stosuje się następujące wytyczne:
 - 1) powierzenie przetwarzania danych osobowych następuje w drodze podpisania umowy powierzenia, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do umowy głównej. **Wzór umowy powierzenia stanowi załącznik nr 6 do Polityki bezpieczeństwa** (w porozumieniu z IOD możliwe jest wykorzystanie innego wzoru umowy powierzenia, w szczególności przekazanego przez drugą stronę umowy),
 - 2) ADO umieszcza informację o fakcie powierzenia przetwarzania w rejestrze kategorii czynności przetwarzania. **Wzór rejestru stanowi załącznik nr 10 do Polityki bezpieczeństwa**.
4. W sytuacji, w której ADO lub podmiot zewnętrzny udostępniają sobie dane osobowe, udostępnienie danych osobowych wymaga podpisania umowy udostępnienia, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do umowy głównej. Treść umowy oraz inne obowiązki ADO związane z udostępnieniem są wcześniej konsultowane przez ADO z IOD.
5. W sytuacji, gdy ADO staje się współadministratorem danych osobowych, zasady współadministrowania danych osobowych wymaga zawarcia umowy o współadministrowaniu, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do umowy głównej. Treść umowy oraz inne obowiązki ADO związane ze współadministrowaniem są wcześniej konsultowane przez ADO z IOD.

5. Środki stosowane w celu zapewnienia bezpieczeństwa danych osobowych

5.1 Rozwiązania organizacyjne

ADO stosuje w szczególności następujące środki organizacyjne:

- 1) wdrożenie i stosowanie Polityki bezpieczeństwa,
- 2) wdrożenie i stosowanie innych wytycznych, regulaminów i instrukcji, mających na celu realizację zasad ochrony danych osobowych i bezpieczeństwa informacji,
- 3) zobowiązanie osób zatrudnionych do zachowania w tajemnicy zarówno danych osobowych, jak i sposobów ich zabezpieczenia.

- 4) zapewnienie kontroli nad działaniem osób upoważnionych do przetwarzania danych osobowych i osób przebywających w obszarze przetwarzania danych osobowych,
- 5) zapewnienie kontroli nad działaniami osób postronnych, tymczasowo przebywających w obszarze przetwarzania danych osobowych.

5.2 Zabezpieczenia fizyczne

1. ADO stosuje w szczególności następujące zabezpieczenia fizyczne:
 - 1) możliwość zamykania pomieszczeń, w których przetwarzane są dane osobowe,
 - 2) zapewnienie osobom zatrudnionym dostępu do szafek, szuflad lub szaf zamykanych na klucz,
 - 3) dostęp do niszczarek dokumentów papierowych.
2. W przypadku niszczenia przez ADO większej liczby papierowych lub elektronicznych nośników potwierdzeniem dokonania zniszczenia zgodnie z procedurami bezpieczeństwa jest protokół, którego wzór stanowi **załącznik nr 14 do Polityki bezpieczeństwa**.
3. Bardziej szczegółowe informacje na temat stosowanych u ADO zabezpieczeń fizycznych znajdują się w **załączniku nr 15 do Polityki bezpieczeństwa**.

5.3 Rozwiązania informatyczne

1. ADO stosuje w szczególności następujące rozwiązania informatyczne:
 - 1) uwierzytelnianie osób pracujących w aplikacjach, programach lub systemach informatycznych (w szczególności z wykorzystaniem loginów i haseł),
 - 2) aplikacje, programy lub systemy chroniące przed złośliwym oprogramowaniem,
 - 3) środki gwarantujące ciągłą pracę systemów informatycznych,
 - 4) środki gwarantujące możliwość odtworzenia danych w razie wystąpienia zdarzenia niepożądanego,
2. Bardziej szczegółowe informacje na temat stosowanych u ADO rozwiązań informatycznych znajdują się w **załączniku nr 11 do Polityki bezpieczeństwa**.

6. Naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych jest odpowiedzialna za ich bezpieczeństwo.
2. Każda osoba współpracująca z ADO, podejrzewająca lub stwierdzająca naruszenie ochrony danych osobowych, zobowiązana jest do niezwłocznego zgłoszenia takiego naruszenia.
3. Przykładowa lista zdarzeń, mogących stanowić naruszenia ochrony danych osobowych wraz ze wskazaniem sposobu postępowania i osoby, której należy zgłosić zdarzenie, stanowi **załącznik nr 3 do Polityki bezpieczeństwa**.
4. Zgłoszenia podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych dokonuje się na formularzu, którego wzór stanowi **załącznik nr 2 do Polityki bezpieczeństwa**.
5. Zgłoszenie podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych jest weryfikowane w celu stwierdzenia, czy rzeczywiście doszło do naruszenia ochrony danych osobowych.
6. W razie stwierdzenia naruszenia ochrony danych osobowych ADO, we współpracy z IOD, ASI oraz - w razie potrzeby - innymi osobami:
 - 1) ocenia stan faktyczny i gromadzi informacje związane z naruszeniem,
 - 2) ustala konieczność zawiadomienia Prezesa UODO (zgodnie z np. 33 RODO) lub osób, których dotyczy naruszenie (zgodnie z np. 34 RODO),
 - 3) ustala działania, mające na celu zminimalizowanie ryzyka ponownego wystąpienia naruszenia w przyszłości,

7. Działania, o których mowa w ust. 6 p. 3 powyżej, mogą obejmować w szczególności:
 - 1) przeprowadzenie przeglądu i konserwacji sprzętu, oprogramowania lub baz danych,
 - 2) przeprowadzenie szkoleń,
 - 3) wyciągnięcie przewidzianych przepisami prawa konsekwencji względem osób odpowiedzialnych za zaistniałe naruszenia,
 - 4) zawiadomienie odpowiednich organów (np. policji), jeżeli do naruszenia doszło na skutek zachowania noszącego znamiona czynu sprzecznego z prawem.
8. ADO dokumentuje naruszenia poprzez gromadzenie wypełnionych formularzy, o których mowa w ust. 4 powyżej lub w inny, uzgodniony z IOD sposób.

7. Postanowienia końcowe

1. Polityka bezpieczeństwa obowiązuje od dnia jej wprowadzenia w sposób przyjęty u ADO. Wszelkie zmiany Polityki bezpieczeństwa obowiązują od dnia ich wprowadzenia w sposób przyjęty u ADO.
2. Z dniem wprowadzenia Polityki bezpieczeństwa traci ważność wcześniej obowiązująca u ADO dokumentacja ochrony danych osobowych.
3. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym przepisy o ochronie danych osobowych.

8. Załączniki

1. Analiza ryzyka i ocena skutków - wytyczne
2. Naruszenia - formularz zgłoszenia
3. Naruszenia - wytyczne
4. Oświadczenie o poufności
5. Powierzenie - ankieta dla podmiotu przetwarzającego
6. Powierzenie - wzór umowy
7. Praca w systemach, na komputerach i innych urządzeniach
8. Procedura realizacji wniosków z RODO
9. Rejestr czynności przetwarzania
10. Rejestr kategorii czynności przetwarzania
11. Rozwiązania informatyczne
12. Upoważnienie do przetwarzania danych osobowych - procedura
13. Upoważnienie do przetwarzania danych osobowych - wzór
14. Wzór protokołu likwidacji dokumentów, nośników lub sprzętu
15. Zabezpieczenia fizyczne