# **ROZDZIAŁ I SŁOWNIK POJĘĆ**

Użyte w niniejszej Polityce terminy oznaczają:

**Administrator Danych Osobowych** – rozumie się przez to Akademię Sztuk Pięknych   
im. E. Gepperta we Wrocławiu.

**ASP** – rozumie się przez to Akademię Sztuk Pięknych im. E. Gepperta we Wrocławiu.

**Lokalny Administrator Danych Osobowych** – rozumie się przez to osoby wyznaczone przez Administratora Danych Osobowych, odpowiedzialne w ramach podległej sobie struktury za stosowanie zabezpieczeń i prowadzenie dokumentacji uproszczonej w zakresie ochrony danych osobowych. Są nimi kierownicy jednostek organizacyjnych ASP.

**Dane osobowe** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest osoba fizyczna, której tożsamość można bezpośrednio lub pośrednio ustalić, 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.

**IOD** – rozumie się przez to Inspektora Ochrony Danych.

**Naruszenie ochrony danych** – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

**Polityka** – rozumie się przez to Politykę Ochrony Danych Osobowych.

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

**Pracownik** – rozumie się przez to osobę zatrudnioną w ASP na podstawie umowy o pracę, umowy cywilnoprawnej, a także osobę wykonującą pracę na podstawie innych umów.

**RODO** – rozumie się przez to 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. (Dziennik Urzędowy Unii Europejskiej L 119 4 maja 2016 r.).

**Szczególne kategorie danych osobowych** – rozumie się przez to dane określone w art. 9 RODO, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne oraz dane dotyczące zdrowia, seksualności lub orientacji.

**Ustawa** – rozumie się przez to ustawę o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781 t.j.).

**Zgoda** – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych w formie papierowej lub elektronicznej.

**POLITYKA OCHRONY DANYCH OSOBOWYCH**

**DEKLARACJA I ZAKRES STOSOWANIA**

1. Niniejsza Polityka Ochrony Danych Osobowych (dalej jako: Polityka) została opracowana w celu wdrożenia w Akademii Sztuk Pięknych im. E. Gepperta we Wrocławiu zasad ochrony i nadzoru przestrzegania danych osobowych zgodnie z Rozporządzeniem 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), Dziennik Urzędowy Unii Europejskiej L 119 4 maja 2016 r. oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

2. Zadaniem Polityki jest zagwarantowanie zgodności działania Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania, współadministrowania i przetwarzania danych osobowych.

3. Polityka określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych w ASP w postaci papierowej oraz zawartych w systemach informatycznych. Są one oparte   
o podejście procesowe, stąd też wynikają z nich konkretne terminy związane z utrzymaniem efektywnego systemu ochrony danych osobowych.

4. Każdy pracownik zobowiązany jest przed rozpoczęciem obowiązków służbowych zapoznać się z treścią niniejszej Polityki i zobowiązany jest przestrzegać procedur i zasad z niej wynikających.

5. Polityka obowiązuje wszystkich pracowników oraz innych osób, które z upoważnienia Administratora Danych Osobowych uzyskały dostęp do danych osobowych kontrahentów, a także podmioty współpracujące, mające kontakt z danymi osobowymi podlegającymi ochronie.

**W SPRAWACH NIEUREGULOWANYCH NINIEJSZĄ POLITYKĄ, ZWŁASZCZA W ZAKRESIE BEZPIECZEŃSTWA TECHNICZNEGO ZASTOSOWANIE ZNAJDĄ UREGULOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

|  |
| --- |
| **Data ostatniej aktualizacji: 23.11.2023 r.** |

**WSTĘP I ZASADY PRZETWARZANIA DANYCH OSOBOWYCH**

**1. Przetwarzanie danych osobowych.**

ASP jako Administrator Danych Osobowych zapewnia, że każda osoba, która ma dostęp do danych osobowych działa na polecenie administratora lub podmiotu przetwarzającego   
i przetwarza dane osobowe zgodnie z niniejszą Polityką, instrukcjami i zarządzeniami dotyczącymi przetwarzania danych osobowych wydanymi przez Administratora oraz na podstawie upoważnienia do przetwarzania danych osobowych.

**2. Lokalni Administratorzy Danych Osobowych.**

ASP wyznaczyła Lokalnych Administratorów Danych Osobowych, którzy są odpowiedzialni   
w ramach podległej sobie struktury za stosowanie zabezpieczeń i prowadzenie dokumentacji uproszczonej w zakresie ochrony danych osobowych. Należą do nich kierownicy jednostek organizacyjnych. Do zakresu ich zadań należy:

* nadawanie i odwoływanie upoważnień do przetwarzania danych osobowych - załącznik nr 6 do niniejszej Polityki,
* prowadzenie ewidencji osób upoważnionych – załącznik nr 5 do niniejszej Polityki,
* delegowanie osób przetwarzających dane osobowe na szkolenia prowadzone przez Inspektora Ochrony Danych,
* współpraca z Administratorem Danych Osobowych w obszarze zgłaszania naruszeń zasad ochrony danych osobowych i ich obsługi.

**3. Przetwarzanie danych osobowych powierzonych.**

ASP jako podmiot przetwarzający, przetwarza dane osobowe tylko na podstawie umów powierzenia lub innych instrumentów prawnych, których zakres reguluje art. 28 ust. 3 RODO. Wzór takiej umowy stanowi załącznik nr 1 do Procedury powierzenia przetwarzania danych osobowych stanowiącej załącznik nr 13 do niniejszej Polityki.

**4. Zasada zgodności z prawem, rzetelności i przejrzystości.**

ASP zapewnia, że dane osobowe przetwarzane są zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą zgodnie z zasadą, o której mowa w art. 5 ust. 1. a) RODO tj. „Dane osobowe muszą być: przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”)”.

ASP realizuje tę zasadę między innymi poprzez:

* przekazywanie informacji kierowanych do osoby, której dane dotyczą, w sposób zwięzły, dostępny i zrozumiały, jasnym i prostym językiem,
* stosowanie obowiązku informacyjnego wobec osoby, której dane dotyczą,
* możliwość dostępu do danych,
* możliwość wniesienia wniosku przez osobę, której dane dotyczą o sprostowanie, ograniczenie przetwarzania i usunięcia danych osobowych.

**5. Zasada ograniczenia celu przetwarzania**

ASP zapewnia, że dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach.

ASP realizuje tę zasadę między innymi poprzez:

* zbieranie danych na podstawie przepisów prawa rangi ustawy lub przewidzianych prawem Unii Europejskiej i tylko do określonych celów,
* stosowanie obowiązku informacyjnego wobec osoby, której dane dotyczą.

**6. Zasada minimalizacji danych**

ASP zapewnia, że przetwarzane dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane zgodnie z zasadą, o której mowa w art. 5 ust. 1. c) RODO tj. „Dane osobowe muszą być: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”)”.

ASP realizuje tę zasadę między innymi poprzez:

* zbieranie danych na podstawie przepisów prawa rangi ustawy lub przewidzianych prawem Unii i tylko do określonych celów,
* stosowanie obowiązku informacyjnego wobec osoby, której dane dotyczą.

**7. Zasada prawidłowości**

ASP zapewnia, że dane osobowe są prawidłowe i w razie potrzeby uaktualniane zgodnie   
z zasadą, o której mowa w art. 5 ust. 1. d) RODO tj. „Dane osobowe muszą być: prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”)”.

ASP realizuje tę zasadę między innymi poprzez:

* możliwość dostępu do danych i wniesienia wniosku o sprostowanie danych osobowych, przez osobę, której dane dotyczą,
* monitorowanie przetwarzanych danych.

**8. Zasada ograniczenia przechowywania**

ASP zapewnia, że dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane zgodnie z zasadą, o której mowa w art. 5 ust. 1. e) RODO, tj. „Dane osobowe muszą być: przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 zabezpieczenia   
i wyjątki mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”)”, chyba że inne przepisy prawa stanowią inaczej.

ASP realizuje tę zasadę między innymi poprzez:

* ustalenie terminu przetwarzania danych,
* określenie sposobu usunięcia danych,
* możliwość wniesienia wniosku przez osobę, której dane dotyczą o sprostowanie, ograniczenie przetwarzania i usunięcia danych osobowych.

**9. Zasada integralności i poufności**

ASP zapewnia, że dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych zgodnie z zasadą, o której mowa w art. 5 ust. 1 lit f RODO tj.: „Dane osobowe muszą być: przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”)”, a realizuje tę zasadę między innymi poprzez wdrożenie środków fizycznych, organizacyjnych i technicznych, które gwarantują bezpieczeństwo fizyczne i informatyczne przetwarzanych danych. Zasada integralności   
i poufności jest realizowana poprzez rozdział IX Środki Bezpieczeństwa i Obowiązki Pracowników oraz rozdział X Zarządzanie Bezpieczeństwem Pracy Zdalnej i Mobilnym Przetwarzaniem Danych Osobowych.

**10. Zasada rozliczalności**

ASP zapewnia, że przestrzega realizację wszystkich wymienionych powyższych zasad zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO tj. „Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”)”. ASP realizuje tę zasadę między innymi poprzez wdrożenie wewnętrznych procedur i zasad, zapewniając odpowiedni nadzór w zakresie ich realizacji   
i przestrzegania przez Inspektora Ochrony Danych.

**11. Zasada retencji danych osobowych**

Zasada retencji danych określa zasady postępowania w zakresie ustalania czasu przetwarzania danych osobowych w ASP.

Ma ona zapewnić realizację wymogów art. 5 ust. 1 lit. e RODO. Zgodnie z wymogami, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Kryteria ustalania okresu retencji danych mogą być określane na podstawie następujących kryteriów:

- do czasu zakończenia realizacji umowy i związanych z tym roszczeń;

- do czasu wycofania zgody lub zgłoszenia sprzeciwu wobec dalszego przetwarzania danych;

- przez okres wymagany przepisami prawa;

- do czasu zrealizowania celu przetwarzania danych.

Zasada retencji danych osobowych ma zastosowanie do wszystkich pracowników ASP oraz osób świadczących usługi na podstawie umowy cywilnoprawnej, a także osób wykonujących pracę na podstawie innych umów.

**12. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych**

ASP przekazuje dane osobowe do państw na podstawie umów powierzenia przetwarzania danych osobowych. W umowach powierzenia przetwarzania danych osobowych wskazuje się podmioty, którym przekazuje się (powierza do dalszego przetwarzania) dane osobowe   
z jednoczesnym wskazaniem, że ma miejsce przekazanie danych do państwa trzeciego.

**13. Profilowanie danych**

ASP nie podejmuje żadnych decyzji, które opierają się na zautomatyzowanym przetwarzaniu, w tym profilowaniu w indywidualnych przypadkach, o których mowa w art. 22 RODO.

**14. Zarządzanie aktywami**

Celem zapewnienia skutecznej ochrony ASP identyfikuje aktywa i definiuje właściwą odpowiedzialność w dziedzinie ich ochrony. Dla przetwarzanych zbiorów danych własnych administrator prowadzi rejestr czynności przetwarzania danych. Dla przetwarzanych zbiorów danych powierzonych do przetwarzania Administrator Danych Osobowych prowadzi rejestr kategorii przetwarzanych danych osobowych w zakresie danych sobie powierzonych.

**15. Udostępnienie danych osobowych i powierzenie przetwarzania**

Niniejsza procedura przewiduje, że ASP może powierzać do dalszego przetwarzania dane osobowe na podstawie umowy lub innego instrumentu prawnego, który podlega prawu Unii lub prawu krajowemu. Szczegółowy zakres powierzenia przetwarzania określa załącznik nr 13 - Procedura powierzenia przetwarzania danych osobowych.

**16. Ochrona przetwarzanych danych osobowych**

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności o różnym prawdopodobieństwie i wadze dotyczących osób fizycznych ASP wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem, w szczególności w celu zapewnienia realizacji zasady poufności i integralności. Zasada ochrony danych osobowych jest realizowana poprzez rozdział IX Środki Bezpieczeństwa i Obowiązki Pracowników oraz rozdział X Zarządzanie Bezpieczeństwem Pracy Zdalnej i Mobilnym Przetwarzaniem Danych Osobowych.

**17. Naruszenie ochrony danych osobowych**

Niniejsza Polityka definiuje katalog przykładowych sytuacji, które mogą prowadzić do naruszenia ochrony danych osobowych, jak również przykłady zdarzeń stanowiących naruszenie ochrony danych. Polityka wprowadza instrukcję postępowania z naruszeniami stanowiącymi naruszenie ochrony danych osobowych, która szczegółowo opisana jest   
w rozdziale nr XI. Polityka określa także zasady dotyczące powiadomienia o naruszeniu ochrony danych osobowych organu nadzorczego oraz osób, których dane dotyczą.

**18. Inspektor Ochrony Danych (IOD)**

Celem nadzorowania realizacji wdrożonych przez politykę postanowień oraz zapewnienia praw osób fizycznych do ochrony danych osobowych oraz kierując się dbałością o dobre praktyki w obszarze ochrony danych osobowych, ASP jako Administrator powołał Inspektora Ochrony Danych oraz zastępcę Inspektora Ochrony Danych.

**Spis treści**

[**ROZDZIAŁ I** SŁOWNIK POJĘĆ 1](#_Toc133322694)

[**ROZDZIAŁ II** OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH 11](#_Toc133322695)

[**ROZDZIAŁ III** PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ 12](#_Toc133322696)

[**ROZDZIAŁ IV** PRZETWARZANIE SZCZEGÓLNEJ KATEGORII DANYCH OSOBOWYCH 14](#_Toc133322697)

[**ROZDZIAŁ V** OBOWIĄZEK INFORMACYJNY 16](#_Toc133322698)

[**ROZDZIAŁ VI** REJESTR CZYNNOŚCI PRZETWARZANIA I REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA 17](#_Toc133322699)

[**ROZDZIAŁ VII** NADAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH 18](#_Toc133322700)

[**ROZDZIAŁ VIII** WSPÓŁADMINISTROWANIE I POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH 19](#_Toc133322701)

[**ROZDZIAŁ IX** ŚRODKI BEZPIECZEŃSTWA I OBOWIĄZKI PRACOWNIKÓW 21](#_Toc133322702)

[**ROZDZIAŁ X** ZARZĄDZANIE BEZPIECZEŃSTWEM PRACY ZDALNEJ I MOBILNYM PRZETWARZANIEM DANYCH OSOBOWYCH 23](#_Toc133322703)

[**ROZDZIAŁ XI** PROCEDURA NARUSZENIA OCHRONY DANYCH OSOBOWYCH 24](#_Toc133322704)

[**ROZDZIAŁ XII** SZACOWANIE I ANALIZA RYZYKA 26](#_Toc133322705)

[**ROZDZIAŁ XIII** SZKOLENIA 27](#_Toc133322706)

[**ROZDZIAŁ XIV** AUDYT OCHRONY DANYCH OSOBOWYCH 28](#_Toc133322707)

[**ROZDZIAŁ XV** INSPEKTOR OCHRONY DANYCH 29](#_Toc133322708)

[**ROZDZIAŁ XVI** AKTUALIZACJA POLITYKI 31](#_Toc133322709)

[**ROZDZIAŁ XVII** POSTANOWIENIA KOŃCOWE 32](#_Toc133322710)

[**WYKAZ ZAŁĄCZNIKÓW** DO POLITYKI OCHRONY DANYCH OSOBOWYCH 33](#_Toc133322711)

# **ROZDZIAŁ II OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH**

1. Siedzibą Administratora Danych Osobowych jest pl. Polski 3/4 we Wrocławiu.
2. Celem skutecznej ochrony przetwarzanych danych osobowych Administrator Danych Osobowych inwentaryzuje posiadane aktywa:
   * zbiory danych osobowych,
   * sprzęt techniczny – informatyczny, który w sposób bezpośredni lub pośredni bierze udział w procesie przetwarzania danych osobowych,
   * programy, narzędzia programowe i procedury zastosowane w celu przetwarzania danych osobowych.
3. Obszarami przetwarzania danych osobowych są wszystkie pomieszczenia biurowe, archiwa i serwerownia pozostające w dyspozycji ASP.
4. Do pomieszczeń przetwarzania danych osobowych mają dostęp tylko osoby upoważnione.
5. Karty wejść (klucze) do pomieszczeń posiadają wyłącznie osoby upoważnione.

# **ROZDZIAŁ III PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ**

1. W zależności od przesłanek przetwarzania danych osobowych, osobie, której dane dotyczą przysługują wskazane poniżej prawa:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Przysługujące prawo** | **art. 6  ust. 1a** | **art. 6  ust. 1b** | **art. 6  ust. 1c** | **art. 6  ust.**  **1d** | **art. 6  ust.**  **1e** | **art. 6  ust.**  **1f** |
| **Prawo dostępu do treści swoich danych**  **(Art. 15)** | **X** | **X** | **X** | **X** | **X** | **Nie dotyczy** |
| **Prawo do sprostowania lub uzupełnienia danych  (Art. 16)** | **X** | **X** | **X** | **X** | **X** | **Nie dotyczy** |
| **Prawo do usunięcia danych („prawo do bycia zapomnianym”)  (Art. 17) (dotyczy danych przetwarzanych na podstawie zgody i dane będą mogły być usunięte po zakończeniu okresu archiwizacji)** | **X** |  |  |  |  | **Nie dotyczy** |
| **Prawo do ograniczenia przetwarzania  (Art. 18)  (pod warunkiem, że osoba której dane dotyczą wykaże jedną**  **z podstaw prawnych w art. 18 ust. 1 a-d )** | **X** | **X** | **X** | **X** | **X** | **Nie dotyczy** |
| **Prawo do przenoszenia danych  (Art. 20)**  **(lub art. 9 ust. 2 lit. a oraz przetwarzanie odbywa się w sposób zautomatyzowany)** | **X** | **X** |  |  |  | **Nie dotyczy** |
| **Prawo do sprzeciwu wobec przetwarzania**  **(nie dotyczy to przypadków, w których ASP posiada uprawnienie do przetwarzania danych na podstawie przepisów prawa).  (Art. 21)** |  |  |  | **X** | **X** | **Nie dotyczy** |

* art. 6 ust 1 lit. a - osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
* art. 6 ust 1 lit. b - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
* art. 6 ust 1 lit. c - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
* art. 6 ust 1 lit. d - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub osoby fizycznej;
* art. 6 ust 1 lit. e - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
* art. 6 ust 1 lit. f - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (przepis ten nie ma zastosowania w do przetwarzani, którego dokonują organy publiczne w ramach realizacji swoich zadań).

2. W przypadku wyrażenia chęci, w formie mailowej lub telefonicznej przez podmiot danych ze skorzystania z praw wynikających z RODO (art. 15-21) Inspektor Ochrony Danych podejmuje decyzje w zakresie realizacji ww. praw. Prowadzi on także rejestr osób, które wyraziły chęć skorzystania z praw wynikających z unijnego rozporządzenia, który stanowi załącznik nr 2 do niniejszej Polityki – **Rejestr praw osób, które wyraziły chęć skorzystania z praw podmiotów danych.**

**Załącznik nr 11 – Procedura realizacji praw osób trzecich**

# **ROZDZIAŁ IV PRZETWARZANIE SZCZEGÓLNEJ KATEGORII DANYCH OSOBOWYCH**

1. ASP przetwarza dane szczególnej kategorii w formie orzeczeń o stopniu niepełnosprawności czy w ramach Zakładowego Funduszu Świadczeń Socjalnych.

2. Dane są przetwarzane zgodnie z art. 9 RODO, który zezwala na przetwarzanie danych szczególnych kategorii, kiedy:

* osoba, której dane dotyczą, wyraziła w sposób wyraźny zgodę na przetwarzanie danych osobowych (chyba, że przepis prawa stanowi, iż osoba, której dane osobowe dotyczą nie może uchylić zakazu);
* przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora danych osobowych lub osobę, której dane dotyczą,   
  w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone przepisami prawa;
* przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
* przetwarzanie dotyczy danych osobowych w sposób oczywisty upubliczniony przez osobę, której dane dotyczą;
* przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
* przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie przepisów prawa;
* przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego na podstawie przepisów prawa lub zgodnie z umową z pracownikiem służby zdrowia zgodnie z prawem;
* przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, na podstawie przepisów prawa;
* przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie przepisów prawa.

# **ROZDZIAŁ V** **OBOWIĄZEK INFORMACYJNY**

1. Administrator Danych Osobowych spełnia obowiązki informacyjne wobec osób, których dane dotyczą.
2. Administrator informuje osobę o przetwarzaniu jej danych osobowych przy pozyskiwaniu danych od tej osoby.
3. Jeżeli dane osobowe są zbierane od osoby, której dane dotyczą, Administrator podaje jej następujące informacje:
   1. swoją tożsamość i dane kontaktowe,
   2. dane kontaktowe IOD,
   3. cel przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
   4. informacje a odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   5. informacje o zamiarze przekazania danych osobowych do państwa trzeciego — jeżeli będzie to miało zastosowanie,
   6. okres, przez który dane osobowe będą przechowywane lub kryteria ustalania tego okresu,
   7. informacje o prawie żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawie wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   8. informacje o prawie do cofnięcia zgody na przetwarzanie danych osobowych w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   9. informacje o prawie wniesienia skargi do organu nadzorczego,
   10. informacje o podstawie zbierania danych osobowych oraz o konsekwencjach ich niepodania.
4. Procedura tworzenia, weryfikacja i sposobu przekazywania obowiązków informacyjnych została opisana w procedurze „Formularze zgód dotyczących przetwarzania danych osobowych wraz z klauzulami informacyjnymi”, która stanowi załącznik nr 10 do niniejszej Polityki.

# **ROZDZIAŁ VI REJESTR CZYNNOŚCI PRZETWARZANIA I REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA**

1. Administrator Danych Osobowych prowadzi rejestr czynności przetwarzania (zwany dalej: rejestrem) oraz rejestr kategorii czynności przetwarzania (zwany dalej: rejestrem kategorii).
2. Osobą odpowiedzialną za nadzór nad prowadzeniem rejestrów jest Inspektor Ochrony Danych.
3. Rejestry stanowią formę dokumentowania czynności przetwarzania danych, w którym inwentaryzuje dane osobowe oraz monitoruje sposób przetwarzania danych osobowych.
4. W rejestrach zawarte są informacje zgodnie z art. 30 ust. 1 i 2 RODO.
5. Rejestry prowadzone są w formie elektronicznej.
6. Administrator dołożył należytej staranności w celu zidentyfikowania wszelkich procesów przetwarzania danych osobowych zachodzących w ramach jego struktury, wyodrębniając jednocześnie cele przetwarzania.
7. Rejestry podlegają bieżącej aktualizacji, w szczególności pod kątem weryfikacji podstaw prawnych przetwarzania danych osobowych. **Odbywa się ona nie rzadziej niż raz   
   w roku (tj. do 30 kwietnia każdego roku) i zakończona jest notatką dla Administratora Danych Osobowych.**

# **ROZDZIAŁ VII NADAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH**

1. Lokalni administratorzy danych nadają upoważnienia do przetwarzania danych osobowych.
2. Wzór upoważnienia wraz z oświadczeniem o zachowaniu poufności i zapoznaniu się z Polityką Ochrony Danych Osobowych stanowi załącznik nr 6 do niniejszej Polityki.
3. Każde upoważnienie do przetwarzania danych osobowych jest rejestrowane. Rejestr stanowiący załącznik nr 4 do Polityki - **Rejestr osób upoważnionych do przetwarzania danych osobowych** jest prowadzony przez Biuro Kanclerza.
4. **Rejestr osób upoważnionych do przetwarzania danych osobowych w ASP podlega cyklicznym przeglądom (nie rzadziej jednak niż raz w roku do 30 września każdego roku)**. Z przeglądu sporządzona jest notatka dla Administratora Danych Osobowych   
   o przeprowadzeniu tej czynności.

# 

# **ROZDZIAŁ VIII WSPÓŁADMINISTROWANIE I POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH**

1. ASP współadministruje oraz powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu tylko na podstawie umowy lub na podstawie innego instrumentu prawnego, który podlega prawu Unii Europejskiej lub prawu krajowemu.
2. ASP korzysta wyłącznie z usług takich podmiotów współadministrujących   
   i przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą. Odbywa się to poprzez zapisy wynikające z przystąpienia do umowy powierzenia danych lub umowy współadministrowania.
3. Współadministrowanie i powierzenie określają:
   * przedmiot i czas trwania przetwarzania,
   * charakter i cele przetwarzania,
   * kategorie osób, których dane dotyczą,
   * rodzaj danych osobowych,
   * obowiązki i prawa administratora/współadministratora.
4. Umowa zapewnia kontrolę nad danymi osobowymi (zarówno w formie współadministrowania jak i powierzenia danych), poprzez:
   * zawarcie klauzuli, że współadministrator i podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora, a przynajmniej bez poinformowania Administratora   
     o dalszym powierzeniu,
   * wyraźne określenie, że po zakończeniu świadczenia usług związanych z przetwarzaniem, przetwarzający zwraca wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo stanowi inaczej (dotyczy wyłącznie umowy powierzenia),
   * zapewnienie przez podmiot przetwarzający, że osoby upoważnione do przetwarzania danych osobowych zobowiązane się do zachowania tajemnicy lub że podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
   * zawarcie klauzuli, że administrator ma prawo do kontroli sposobu przetwarzania przetwarzanych danych w siedzibie przetwarzającego poprzez umożliwienie administratorowi lub audytorowi/IOD upoważnionemu przez administratora na przeprowadzanie audytów, w tym inspekcji,
   * zawarcie klauzuli, że współadministrator i przetwarzający musi wdrożyć środki techniczne i organizacyjne odpowiednie do ryzyk przetwarzania – tak by to przetwarzanie odpowiadało wymogom rozporządzenia.
5. Umowa zawiera klauzule zobowiązujące współadministratora i podmiot przetwarzający:
   * do zgłaszania naruszeń ochrony danych do organu nadzorczego i do administratora oraz informuje o wszystkich kontrolach organu nadzorczego i jego wynikach,
   * pomaga administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
6. Umowy współadministrowania oraz powierzenia danych przechowywane są wraz z umowami zasadniczymi. Dodatkowo Inspektor Ochrony Danych prowadzi **Rejestr umów powierzenia przetwarzania danych osobowych, który stanowi załącznik nr 3 do niniejszej Polityki**.

Załącznik nr 14 Procedura współadministrowania a udostępniania danych osobowych

# **ROZDZIAŁ IX ŚRODKI BEZPIECZEŃSTWA I OBOWIĄZKI PRACOWNIKÓW**

1. W ASP wdrożono następujące środki bezpieczeństwa oraz obowiązki pracowników wynikających z tego zakresu:

* wyznaczono Inspektora Ochrony Danych,
* wyznaczono Administratora Systemów Informatycznych,
* wprowadzono procedury regulujące procesy przetwarzania danych,
* wprowadzono prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem ewidencji stanowiącym załącznik nr 4 do niniejszej Polityki,
* do przetwarzania danych osobowych są dopuszczane tylko osoby upoważnione zgodnie ze wzorem upoważnienia stanowiącym załącznik nr 6 do niniejszej Polityki,

- przeprowadzanie okresowych przeglądów sieci informatycznej, w tym przeprowadzanie cyklicznych testów odtwarzania serwera z kopii zapasowej,

- dostęp do systemu informatycznego następuje z użyciem identyfikatora i hasła,

- zastosowano mechanizmy rozliczalności działań poszczególnych użytkowników,

- zastosowano oprogramowanie antywirusowe, w tym systematyczne instalowanie wymaganych przez producentów oprogramowania aktualizacji związanych   
z bezpieczeństwem,

- zastosowano zaporę ogniową (firewall) ze zdefiniowanymi listami dostępów,

- szczegółowe zabezpieczenia fizyczne zostały opisane w dokumentacji prowadzonej przez Specjalistę ds. obronnych. Dokumentacja może być udostępniona tylko osobom upoważnionym przez Kanclerza ASP,

* obowiązkowe szkolenia pracowników ASP, odbywające się w miarę uzasadnionych potrzeb, w zakresie ochrony danych osobowych.

1. W celu zapewnienia rozliczalności dostępu do danych:
   1. z dniem rozwiązania stosunku pracy z użytkownikiem:
      * ASI zamyka konto użytkownika w systemie informatycznym oraz zabezpiecza dostęp do danych hasłem; dane z konta użytkownika, z którym rozwiązano stosunek pracy, są archiwizowane lub usuwane – zgodnie z decyzją kierownika jednostki organizacyjnej, w której zatrudniony był użytkownik,
      * IOD lub osoba zastępująca wpisuje w ewidencji osób upoważnionych do przetwarzania danych osobowych datę wygaśnięcia upoważnienia do przetwarzania danych osobowych,
   2. w karcie obiegowej pracownika, z którym rozwiązano stosunek pracy:
      * ASI potwierdza zamknięcie konta pracownika w systemie informatycznym,
      * IOD lub osoba zastępująca potwierdza wpisanie do ewidencji osób upoważnionych daty wygaśnięcia upoważnienia.

# **ROZDZIAŁ X ZARZĄDZANIE BEZPIECZEŃSTWEM PRACY ZDALNEJ I MOBILNYM PRZETWARZANIEM DANYCH OSOBOWYCH**

1. Przy korzystaniu z urządzeń mobilnych użytkownik otrzymujący komputer przenośny podpisuje oświadczenie, w którym zobowiązuje się do przestrzegania zaleceń związanych   
z ochroną laptopa:

* 1. laptop powinien być transportowany pod kontrolą użytkownika lub innej upoważnionej osoby,
  2. laptop nie powinien być pozostawiany w sposób narażający go na kradzież,
  3. dyski na komputerach przenośnych powinny być szyfrowane,
  4. nie zezwala się na pracę nad danymi osobowymi w miejscach publicznych,
  5. co najmniej raz w miesiącu komputer przenośny powinien być podłączony do lokalnej sieci ASP w celu aktualizacji oprogramowania oraz polityki bezpieczeństwa.

1. Zabrania się kopiowania i przechowywania danych stanowiących własność ASP na smartfonach.
2. Zabrania się korzystania z prywatnych laptopów i innych urządzeń przenośnych do kopiowania i przetwarzania danych należących do ASP bez zgody bezpośredniego przełożonego.
3. Zobowiązuje się przy korzystaniu z urządzeń mobilnych do korzystania z wyłącznie szyfrowanych połączeń do sieci Internet. Szczegółowe zasady w tym zakresie określa **załącznik nr 1 – Instrukcja ochrony danych osobowych w trakcie pracy zdalnej.**

# **ROZDZIAŁ XI PROCEDURA NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

1. W przypadku stwierdzenia faktu nieuprawnionego przetwarzania ujawnienia lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych każdy pracownik zgłasza Inspektorowi Ochrony Danych w trybie natychmiastowym każdy przypadek naruszenia bezpieczeństwa ochrony danych osobowych przez dedykowany adres mailowy **iod@asp.wroc.pl**. W przypadku nieobecności IOD, pracownik zobowiązany jest zgłosić naruszenie swojemu bezpośredniemu przełożonemu, który przekazuje tę bezpośredniej reprezentacji Administratora Danych Osobowych. Szczegółowe postępowanie w zakresie naruszeń danych osobowych określa **załącznik nr 12** - **Procedura notyfikacji naruszeń danych osobowych.**
2. Do zdarzeń mogących prowadzić do naruszenia zasad ochrony danych osobowych zalicza się m.in.:
   1. kradzież plików lub dokumentacji z danymi osobowymi w każdej formie,
   2. nieumyślną lub celową modyfikację danych, zarówno w formie elektronicznej i papierowej,
   3. utratę danych,
   4. włamania do systemu informatycznego w formie ataków phishingowych czy ransomware,
   5. nieplanowane awarie sprzętu lub uszkodzenie oprogramowania,
   6. utratę zasilania powodującą przerwę w pracy systemów,
   7. kradzież sprzętu lub nośników z ważnymi danymi,
   8. nieprzestrzeganie postanowień Polityki,
   9. inne skutkujące utratą danych osobowych bądź wejściem w ich posiadanie osób nieuprawnionych, zjawiska takie jak: naturalne katastrofy, przechwycenie transmisji danych, odczyt z monitora komputera przez osoby nieuprawnione, zauważenie śladów usiłowania lub dokonania włamania do pomieszczenia lub szafy z danymi, zauważenie elektronicznych śladów próby włamania do systemu informatycznego.
3. Inspektor Ochrony Danych dokonuje analizy naruszenia we współpracy z Administratorem Danych Osobowych. W przypadku wysokiego prawdopodobieństwa naruszenia ochrony danych osobowych jest ono zgłaszane do Prezesa Urzędu Ochrony Danych Osobowych w terminie do 72 godzin od wystąpienia naruszenia. Analiza powinna być przeprowadzona zgodnie z **załącznikiem nr 15 –** **Kartą naruszenia**.
4. W ASP jest prowadzony zgodnie z załącznikiem nr 16 do niniejszej Polityki – **Rejestr naruszeń z zakresu ochrony danych osobowych**, który prowadzi i aktualizuje Inspektor Ochrony Danych. Dodatkowo raz w roku dokonywany jest jego przegląd w celu wyciągnięcia wniosków w ramach funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji.

Załącznik nr 12 Procedura notyfikacji naruszeń danych osobowych

# 

# **ROZDZIAŁ XII SZACOWANIE I ANALIZA RYZYKA**

1. Administrator Danych Osobowych przeprowadza cyklicznie **nie rzadziej jednak niż raz w roku (do 30 czerwca każdego roku)** szacowanie i analizę ryzyka w obszarze ochrony danych osobowych w konsultacji z Inspektorem Ochrony Danych. Efektem końcowym takiej analizy jest dokument analizy ryzyka, wynikający z procedury oceny skutków dla ochrony danych osobowych.
2. W przypadku, kiedy nowa operacja na danych osobowych wiąże się z dużym prawdopodobieństwem wysokiego ryzyka naruszenia praw i wolności osób fizycznych Administrator we współpracy z IOD przeprowadza ocenę skutków dla ochrony danych zgodnie z art. 35 RODO.

# **ROZDZIAŁ XIII SZKOLENIA**

1. Administrator Danych Osobowych zapewnia szkolenia dla nowych pracowników oraz osób mających dostęp do danych osobowych, szkolenia okresowe, szkolenia po incydencie lub zagrożeniu wystąpieniem incydentu w zakresie danych osobowych.
2. Podnoszenie poziomu wiedzy wykonuje się poprzez szkolenia pracowników **co najmniej raz w roku (do 30 października)** lub każdorazowo przy zmianie niniejszej Polityki, lub przepisów prawa w zakresie ochrony danych osobowych.
3. Każdy nowo zatrudniony pracownik w ASP ma obowiązek zapoznać się z Polityką Ochrony Danych Osobowych przed rozpoczęciem stosunku pracy.
4. Szkolenie dla nowo zatrudnionych pracowników odbywa się w terminie 30 dni od podpisania umowy o pracę. Zakres szkolenia jest określany przez osobę szkolącą – Inspektora Ochrony Danych, jednakże powinien on zawierać takie zagadnienia jak: obowiązki administratora danych osobowych, odpowiedzialność pracownika, rola Inspektora Ochrony Danych, aktualne zagrożenia z zakresu ochrony danych osobowych, czy dobre praktyki związane z przetwarzaniem danych osobowych.
5. Inspektor Ochrony Danych działając w celu podnoszenia świadomości pracowników w obszarze cyberbezpieczeństwa przesyła do wszystkich pracowników raz na kwartał broszurę informacyjną na temat aktualnych zagrożeń w Internecie.
6. Inspektor Ochrony Danych przeprowadza cyklicznie (nie rzadziej niż raz w roku) szkolenia dla personelu przetwarzającego dane osobowe. Zakres szkolenia obejmuje takie zagadnienia jak: obowiązki Administratora Danych Osobowych, odpowiedzialność pracownika, rola Inspektora Ochrony Danych, aktualne zagrożenia z zakresu ochrony danych osobowych czy dobre praktyki związane z przetwarzaniem danych osobowych.

# **ROZDZIAŁ XIV AUDYT OCHRONY DANYCH OSOBOWYCH**

1. Administrator Danych Osobowych zapewnia audyt ochrony danych osobowych **nie rzadziej niż raz w roku (tj. do 30 czerwca każdego roku)**, który powinien zostać zakończony protokołem bądź sprawozdaniem z przeprowadzonego audytu.
2. Audyt może być przeprowadzany wewnętrznie - przez Inspektora Ochrony Danych lub zlecony firmie zewnętrznej. Protokół bądź sprawozdanie z przeprowadzonego audytu zostaje przekazane każdorazowo Administratora Danych Osobowych.
3. Audyt może być przeprowadzany również na podstawie rocznego planu, a także w sytuacji ryzyka wystąpienia naruszenia ochrony danych osobowych.

# **ROZDZIAŁ XV INSPEKTOR OCHRONY DANYCH**

1. Rektor ASP wyznaczył do pełnienie funkcji Inspektora Ochrony Danych – Pana Eryka Brodnickiego (zarządzenie Rektora nr I/25/2023 z dnia 17 marca 2023 r.).
2. Wybór Inspektora Ochrony Danych odbył się na podstawie art. 37 ust. 5 RODO, który określa, że Inspektor Ochrony Danych został wyznaczony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz wypełnienia zadań, o których mowa w art. 39 RODO.
3. Do zadań Inspektora Ochrony Danych należy w szczególności:

* informowanie administratora podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich mocą rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
* monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora 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,
* udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
* współpraca z organem nadzorczym,
* 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,
* sprawowanie nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych osobowych,
* przegląd i opiniowanie dokumentacji dotyczącej ochrony danych osobowych

1. Kontakt z Inspektorem Ochrony Danych jest możliwy poprzez adres mailowy: [**iod@asp.wroc.pl**](mailto:iod@asp.wroc.pl)
2. W celu zapewnienia ciągłości działania pracy Inspektora Ochrony Danych w ASP został wyznaczony Zastępca Inspektora Ochrony Danych, z którym można się skontaktować poprzez adres mailowy: [iod@asp.wroc.pl](mailto:iod@asp.wroc.pl)

# **ROZDZIAŁ XVI AKTUALIZACJA POLITYKI**

1. Administrator Danych Osobowych lub zespół osób do tego wyznaczonych przeprowadza cyklicznie **nie rzadziej jednak niż raz w roku (do 30 września każdego roku)** przegląd Polityki Ochrony Danych Osobowych.

2. Potwierdzeniem przeglądu Polityki Ochrony Danych Osobowych jest raport dla Administratora Danych Osobowych stanowiący załącznik nr 7 do Polityki Ochrony Danych Osobowych – **Raport z przeglądu Polityki Ochrony Danych Osobowych**.

3. Zasady aktualizacji uregulowań wewnętrznych w zakresie ochrony danych osobowych określa załącznik nr 5 do niniejszej Polityki.

# **ROZDZIAŁ XVII POSTANOWIENIA KOŃCOWE**

W Polityce Bezpieczeństwa Informacji oraz w pozostałych dokumentach SZBI określono zasady:

* + dostępu do urządzeń w systemie informatycznym,
  + dostępu do zasobów informatycznych,
  + pracy w systemach informatycznych,
  + organizacji systemu informatycznego,
  + nadawania i odbierania uprawnień do pracy w systemach informatycznych,
  + polityki haseł i postępowania z hasłami dostępu do poczty elektronicznej i Internetu.

# 

# **WYKAZ ZAŁĄCZNIKÓW DO POLITYKI OCHRONY DANYCH OSOBOWYCH**

**Załącznik nr 1** – Instrukcja ochrony danych osobowych w trakcie pracy zdalnej

**Załącznik nr 2** – Rejestr praw osób, które wyraziły chęć skorzystania z praw podmiotów danych

**Załącznik nr 3** – Rejestr umów powierzenia przetwarzania danych osobowych

**Załącznik nr 4** – Rejestr osób upoważnionych do przetwarzania danych osobowych

**Załącznik nr 5** – Zasady aktualizacji uregulowań wewnętrznych w zakresie ochrony danych osobowych

**Załącznik nr 6** – Upoważnienie do przetwarzania danych osobowych

**Załącznik nr 7** – Raport z przeglądu Polityki Ochrony Danych Osobowych

**Załącznik nr 8** – Ogólny opis technicznych i organizacyjnych śr. bezpieczeństwa danych os.

**Załącznik nr 9** – Wycofanie upoważnienia do przetwarzania danych osobowych

**Załącznik nr 10** – Formularze zgód dotyczących przetwarzania danych osobowych wraz   
z klauzulami informacyjnymi

**Załącznik nr 11** – Procedura realizacji praw osób trzecich

**Załącznik nr 12** – Procedura notyfikacji naruszeń danych osobowych

**Załącznik nr 13** – Procedura powierzenia przetwarzania danych osobowych

**Załącznik nr 14** – Procedura współadministrowania a udostępniania danychosobowych

**Załącznik nr 15** – Karta naruszenia

**Załącznik nr 16** –Rejestr naruszeń z zakresu ochrony danych osobowych