Załącznik nr 1
do zarządzenia Rektora
Nr 2/2026 z dnia 8 stycznia 2026 r.

Państwowa Akademia Nauk Stosowanych w Głogowie

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W PAŃSTWOWEJ AKADEMII NAU STOSOWANYCH W GŁOGOWIE

Spis treści

W ramach realizacji celów statutowych oraz innych celów wynikających z przepisów prawa Państwowa Akademia Nauk Stosowanych w Głogowie, jako administrator danych osobowych stosuje Politykę bezpieczeństwa w zakresie danych osobowych i spełnia wymagane prawem obowiązki wobec osób, których dane dotyczą.

Mając powyższe na uwadze ustala się następujące wytyczne Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Uczelni, zwane dalej „Polityką bezpieczeństwa" lub „Polityką".

I. PODSTAWA PRAWNA

§ 1.

Dane osobowe w Państwowej Akademii Nauk Stosowanych w Głogowie przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, w szczególności przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego Ogólnym Rozporządzeniem o Ochronie Danych, a także innych aktów prawnych, które znajdują zastosowanie do przetwarzania danych osobowych i ochrony prywatności.

§ 2.

Uczelnia przetwarza dane osobowe:

1) w związku z realizacją zadań Uczelni, wynikających z Ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz.U. z 2024 r., poz. 1571, ze zm.),
2) w celu zapewnienia prawidłowej, zgodnej z prawem polityki personalnej oraz wypełnienia obowiązków prawnych ciążących na administratorze, jako pracodawcy,
3) dla realizacji innych celów i zadań – w szczególności wynikających z przepisów prawa lub prawnie uzasadnionych interesów administratora,
4) w pozostałych, prawnie uzasadnionych celach – za zgodą osób, których dane dotyczą.

II. SŁOWNIK POJĘĆ

§ 3.

Użyte w niniejszym dokumencie określenia oznaczają:

1) Administrator Danych Osobowych (Administrator, ADO) – Państwowa Akademia Nauk Stosowanych w Głogowie reprezentowana przez Rektora;
2) Administrator Systemu Informatycznego (ASI) – pracownik odpowiedzialny za prawidłową pracę systemów informatycznych;
3) Czynność przetwarzania - zespół powiązanych ze sobą operacji na danych, które można określić w sposób zbiorczy, w związku z celem w jakim te czynności są podejmowane;
4) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) Dane osobowe szczególne - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;

6) Dane osobowe zwykłe – wszystkie dane osobowe nie stanowiące danych osobowych szczególnych;
7) Hasło – ciąg znaków literowych, cyfrowych lub innych specjalnych znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
8) Incydent – naruszenie ochrony danych osobowych;
9) Integralność danych – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) Inspektor Ochrony Danych (IOD) – osobę wyznaczoną przez Administratora, nadzorującą przestrzeganie zasad ochrony przetwarzania danych osobowych w Uczelni;
11) Miejsce przetwarzania danych osobowych – obszar gdzie wykonywane są jakiekolwiek operacje na danych osobowych w ramach jednostki organizacyjnej Administratora;
12) Naruszenie ochrony danych osobowych - przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
13) Osoba upoważniona – osobę, która upoważniona została w formie pisemnej przez Administratora do przetwarzania danych osobowych;
14) Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
15) Poufność danych – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
16) Proces przetwarzania danych – zespół czynności przetwarzania danych osobowych;
17) Przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak, zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
18) Rozliczalność – właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
19) RODO - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
20) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
21) Uczelnia lub PANS – Państwowa Akademia Nauk Stosowanych w Głogowie;
22) Upoważnienie – uprawnienie do przetwarzania danych osobowych wydane w formie pisemnej (elektronicznej lub papierowej);
23) Usuwanie danych – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
24) Uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

25) Użytkownik/pracownik (w tym podmiotu trzeciego) - osoba przetwarzająca dane w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w Uczelni lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;

26) Współadministrowanie – sytuacja w której co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych;

27) Zabezpieczenie danych osobowych – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

28) Zbiór danych – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

29) Zdarzenie – informacja lub okoliczność dająca podejrzenie naruszenia ochrony danych osobowych na podstawie, której dokonuje się oceny ryzyka naruszenia praw i wolności. W przypadku stwierdzenia braku zagrożenia dla praw i wolności zdarzenie nie stanowi naruszenia tych praw:

30) Zgoda na przetwarzanie danych osobowych - oświadczenie woli osoby, której dane są przetwarzane przez administratora danych, w której wyraża swoją aprobatę dla tego procesu.

III. CEL WPROWADZENIA POLITYKI BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

§ 4.

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych stanowi zbiór zasad obowiązujących przy przetwarzaniu danych osobowych w Państwowej Akademii Nauk Stosowanych w Głogowie.
2. Celem Polityki jest:
   1) zapewnienie właściwego poziomu bezpieczeństwa danych osobowych w Uczelni poprzez wdrożenie odpowiedniego systemu ich ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi;
   2) podniesienie poziomu świadomości pracowników Uczelni co do istoty problemu bezpieczeństwa danych osobowych.
3. Polityka bezpieczeństwa jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych. Ma ona pomóc w zapewnieniu: poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.

IV. ZAKRES STOSOWANIA POLITYKI

§ 5.

Polityka bezpieczeństwa odnosi się do danych osobowych przetwarzanych w:

1) zbiorach danych tradycyjnych, na papierowych nośnikach danych (dokumentacja papierowa, np. kartoteki, księgi, wykazy, listy itp.),
2) systemach informatycznych i na nośnikach cyfrowych,
3) systemach dozoru wizyjnego (monitoring).

§ 6.

1. Polityka bezpieczeństwa zapewnia, przy uwzględnieniu zasad wynikających z art. 5 RODO zapewnia, aby dane były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada zgodności z prawem, rzetelności i przejrzystości);
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami (zasada ograniczenia celu, celowości);
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
   4) 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 (zasada prawidłowości);
   5) 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 art. 89 ust. 1 RODO 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 (zasada ograniczenia przechowywania);
   6) 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 (zasada integralności i poufności);
   7) przetwarzane w sposób, który pozwoli administratorowi wykazać, iż spełnione są zasady wymienione w pkt 1-6 (zasada rozliczalności).
2. Szczególnej ochronie podlegają dane osobowe wymienione w art. 9 ust. 1 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, a także dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa – art. 10 RODO.

§ 7.

1. Procedury określone w niniejszym dokumencie mają zastosowanie do wszystkich osób wykonujących prace związane z działalnością Uczelni lub na rzecz Uczelni (niezależnie od formy współpracy, czy rodzaju umowy) w szczególności pracowników, współpracowników (w tym zleceniobiorców i osób realizujących umowy o dzieło) oraz innych osób, którym zostało udzielone upoważnienie do przetwarzania danych osobowych.
2. PANS, jego pracownicy i współpracownicy deklarują pełne zaangażowanie dla bezpieczeństwa przetwarzania danych osobowych przetwarzanych zarówno w sposób tradycyjny, jak i w systemach informatycznych oraz na nośnikach cyfrowych.
3. Ochrona danych osobowych wynikająca z Polityki jest realizowana na każdym etapie przetwarzania informacji.
4. Uczelnia, jako administrator danych stosuje środki organizacyjne i techniczne, w tym informatyczne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, w szczególności wprowadza rozwiązania dotyczące:
   1) pseudonimizacji (polegającej na zamianie posiadanych danych np. imienia i nazwiska na ciąg liter albo cyfr, które można rozszyfrować wyłącznie na podstawie przechowywanych oddzielnie informacji tzw. Klucza) i szyfrowania danych osobowych,
   2) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych,
   3) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, skutkującego naruszeniem ochrony danych osobowych,
   4) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

V. OBSZAR PRZETWARZANIA DANYCH

§ 8.

1. Uczelnia ustala obszar przetwarzania danych osobowych, który obejmuje wszystkie pomieszczenia, w których wykonuje się jakiekolwiek operacje na danych osobowych, w szczególności wprowadzanie, modyfikowanie, archiwizowanie, usuwanie dane, a także wszystkie miejsca, gdzie przechowuje się systemy informatyczne lub nośniki informacji zawierające dane osobowe, jak szafy z dokumentacją papierową lub zawierającą elektroniczne nośniki informacji.
2. W celu zapewnienia bezpieczeństwa pracowników i studentów, ochrony mienia, dochodzenia roszczeń, zachowania tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę stosuje się wideomonitoring zgodnie z zapisami Regulaminu Pracy. Dostęp do nagrań z wideomonitoringu jest ograniczony do osób upoważnionych i wykorzystywany wyłącznie w celach bezpieczeństwa i dochodzenia roszczeń.
3. W celu ochrony obszaru przetwarzania przed dostępem osób nieuprawnionych stosuje się instalację alarmową oraz procedurę dotyczącą kluczy, zabezpieczając w ten sposób budynki i pomieszczenia. Ewidencję poboru i zdania kluczy prowadzi portiernia/recepcja.
4. Procedura dotycząca kluczy stanowi załącznik nr 2 do niniejszej Polityki.

VI. CHARAKTERYSTYKA ZBIORÓW DANYCH

§ 9.

1. Przetwarzane w Uczelni dane osobowe są gromadzone w zbiorach, tworzonych w taki sposób, aby odpowiednie dane były dostępne w oparciu o określone kryteria, niezależnie od tego, czy zestaw danych jest scentralizowany lub zdecentralizowany.
2. Wykaz prowadzonych w Uczelni zbiorów danych osobowych stanowi załącznik nr 3 do niniejszej Polityki.
3. W Uczelni mogą być tworzone również inne niż te zawarte w załączniku nr 3, zbiory danych w celach doraźnych, ze względów technicznych lub w związku z realizacją określonego zadania. Zbiory te, po ich wykorzystaniu są niezwłocznie usuwane albo poddane modyfikacji tak, by danych w nich zawartych nie można było przypisać konkretnej lub dającej się ustalić osobie.
4. Zabronione jest przetwarzanie danych osobowych, w tym tworzenie zbiorów danych, a także gromadzenie w zbiorach lub poza nimi danych osobowych - innych niż niezbędne dla realizacji celów, do których dane te zostały zebrane.
5. Wszelkie nowe programy i systemy informatyczne, które mają służyć gromadzeniu i przetwarzaniu danych osobowych w Uczelni muszą zapewniać możliwość obsługi określonych zbiorów danych oraz spełniać wymogi bezpieczeństwa wskazane przez Administratora.

VII. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Zakresy czynności i zarządzanie danymi osobowymi

Administratorem przetwarzanych w Uczelni danych osobowych w rozumieniu rozporządzenia jest Państwowa Akademia Nauk Stosowanych w Głogowie reprezentowana przez Rektora. W trakcie nieobecności Rektora funkcję Administratora pełni zastępujący go Prorektor.

§ 10.

1. Administrator jest zobowiązany do przestrzegania przepisów dotyczących ochrony danych osobowych, w szczególności poprzez:
   1) zapewnienie właściwych warunków organizacyjnych i technicznych, gwarantujących ochronę danych osobowych przetwarzanych w podległych im obszarach oraz ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   2) dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnienie, aby dane te były:
      a) przetwarzane zgodnie z prawem,
      b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddane dalszemu przetwarzaniu niezgodnemu z tymi celami,
      c) merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane,
      d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;

3) dopuszczanie do przetwarzania danych wyłącznie osób posiadających stosowne upoważnienie;
4) wdrożenie, a następnie nadzorowanie przestrzegania przez pracowników przepisów wewnętrznych obowiązujących w tym zakresie, tj. Polityki ochrony danych osobowych i Instrukcji zarządzania systemem informatycznym;
5) wykonywanie zaleceń IOD w zakresie ochrony danych osobowych;
6) uwzględnianie zaleceń ASI w zakresie zabezpieczeń systemów informatycznych, w tym akceptowanie, niezbędnych dla zgodności z prawem, modyfikacji stosowanych systemów informatycznych;
7) sprawowanie kontroli nad przetwarzaniem danych osobowych.

2. Administrator zapewnia i stosuje odpowiednie środki informatyczne, techniczne i organizacyjne (wykaz w/w środków stanowi załącznik nr 4 do niniejszej Polityki), zapewniając ochronę przetwarzanych danych osobowych odpowiednią do wyników analizy ryzyka, a w szczególności:
   1) podejmuje decyzje o celach i środkach przetwarzanie danych osobowych,
   2) podejmuje decyzje o technicznych i organizacyjnych zabezpieczeniach oraz wdraża zasady i procedury postępowania mające na celu zapewnienie adekwatnego poziomu bezpieczeństwa przetwarzanych danych,
   3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków,
   4) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych,
   5) prowadzi kontrolę przestrzegania procedur przetwarzania danych osobowych,
   6) zapewnia realizację praw osób, których dane osobowe są przetwarzane (m.in. prawo wglądu, poprawiania danych i wniesienia sprzeciwu wobec przetwarzanych danych),
   7) reprezentuje PANS w Głogowie w postępowaniach przed organami publicznymi oraz w kontaktach z podmiotami trzecimi w sprawach związanych z pozyskiwaniem, przetwarzaniem, ochroną i powierzeniem danych osobowych,
   8) decyduje o formach przeciwdziałania ewentualnym zagrożeniom,
   9) zapewnia udział osób o odpowiednich kompetencjach i wiedzy (pracowników Administratora i podmiotów zewnętrznych) przy realizacji audytów i weryfikacji systemu ochrony danych osobowych prowadzonego przez IOD,
   10) zapewnia bezpieczne usunięcie danych osobowych w przypadku uzasadnionego żądania niezwłocznego usunięcia danych osobowych, bez zbędnej zwłoki.

§ 11.

1. Rektor wyznacza Inspektora Ochrony Danych (IOD), który nadzoruje przestrzeganie zasad ochrony danych osobowych.
2. W zakresie obowiązków wynikających z niniejszej Polityki, IOD podlega bezpośrednio Rektorowi.
3. IOD wykonuje swoje zadania we współpracy z Administratorem Danych Osobowych (ADO) Administratorem Systemów Informatycznych (ASI)

4. Do zadań IOD należy, w szczególności:
   1) zapewnienie przestrzegania przepisów o ochronie danych osobowych w PANS w Głogowie, w tym również udzielanie zaleceń odnośnie ochrony danych osobowych oraz monitorowanie ich wykonania;
   2) podejmowanie działań monitorujących i kontrolnych w jednostkach organizacyjnych Uczelni, lub podmiotach, którym Uczelnia powierzyła przetwarzanie danych osobowych, a w przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych wnioskowanie o niezwłoczne ich usunięcie;
   3) prowadzenie centralnej ewidencji osób upoważnionych do przetwarzania danych osobowych, a także nadzorowanie przyznawania i odwoływania uprawnień w tym zakresie;
   4) prowadzenie centralnego rejestru czynności przetwarzania danych osobowych oraz – gdy ma to zastosowanie - rejestru kategorii czynności przetwarzania dokonywanych w imieniu Administratora, a także innych ewidencji związanych z ochroną danych osobowych;
   5) koordynowanie procesu przyznawania/zmiany/odwoływania uprawnień do przetwarzania danych osobowych w ramach Uczelni;
   6) współpracowanie z organem nadzorczym, w tym monitorowanie jego zaleceń w zakresie ochrony danych osobowych i implementowanie ich w Uczelni;
   7) informowanie Administratora, podmiotu przetwarzającego oraz pracowników o obowiązkach spoczywających na nich na mocy rozporządzenia i doradzanie im w tym zakresie;
   8) opiniowanie wprowadzonych przez Administratora polityk, procedur, analiz oraz rejestrów czynności;
   9) reagowanie na zdarzenia i incydenty ochrony danych osobowych w Uczelni;
   10) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem praw przysługujących im na mocy rozporządzenia.
   11) wzór powołania IOD stanowi załącznik nr 5 do niniejszej Polityki.

§ 12.

1. Rektor powołuje Administratora Systemów Informatycznych (ASI) oraz określa zakres jego zadań i czynności w zakresie ochrony danych osobowych w systemach (wzór powołania ASI stanowi załącznik nr 6 do niniejszej Polityki).
2. Do zadań ASI należą czynności związane z bieżącą aktualizacją i utrzymaniem ciągłości działania systemów informatycznych; a także:
   1) przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych, w których przetwarzane są dane osobowe, w tym stosowanie wszelkich dostępnych mechanizmów ochrony celem właściwego ich zabezpieczenia;
   2) przydzielanie użytkownikom dostępu do systemów informatycznych a także blokowanie tego dostępu w przypadku cofnięcia uprawnień lub rozwiązania stosunku pracy;
   3) prowadzenie i aktualizację wykazu osób upoważnionych do przetwarzania danych osobowych w administrowanych przez nich systemach;
   4) szkolenie użytkowników z obsługi i bezpiecznej eksploatacji systemów;

5) informowanie IOD o wszelkich naruszeniach ochrony danych osobowych w przetwarzanych systemach informatycznych, a także współdziałanie przy usuwaniu skutków tych naruszeń;

6) usuwanie danych osobowych z administrowanych systemów informatycznych.

2. Przyznawanie i odwoływanie uprawnień do przetwarzania danych

§ 13.

1. Każda osoba przetwarzająca dane osobowe na potrzeby Uczelni jest obowiązana zapoznać się z treścią niniejszej Polityki oraz bezwzględnie stosować się do jej zapisów. Osoby przetwarzające dane osobowe czynią to na polecenie Administratora oraz na podstawie wydanego przez niego upoważnienia (załącznik nr 1).
2. Upoważnienie przyznawane jest na czas trwania umowy o pracę lub innej umowy cywilnoprawnej chyba, że bezpośredni przełożony zadecyduje inaczej, a także na czas określonego zadania, które nierozerwalnie związane jest z przetwarzaniem danych.
3. Upoważnienie jest przyznawane przed rozpoczęciem przetwarzania danych osobowych.
4. Uprawnienia do przetwarzania danych osobowych wygasają z chwilą ustania stosunku pracy/wygaśnięcia umowy cywilnoprawnej, porozumień lub z upływem okresu ważności upoważnienia.
5. Decyzję o cofnięciu uprawnień w okresie ich trwania podejmuje Administrator (ADO)
6. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Inspektor Ochrony Danych.
7. Nadane upoważnienia przechowywane są w systemie informatycznym oraz w formie papierowej.

3. Zasady przetwarzania danych osobowych

§ 14.

1. Pracownicy/użytkownicy są zobowiązani do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:
   a) pisemnego wnioskowania o zaewidencjonowanie nowych zbiorów danych osobowych w wykazie prowadzonym przez Inspektora Ochrony Danych,
   b) bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
   c) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych,
2. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z RODO, czy Ustawy, stosuje się przepisy tych ustaw.
3. Pracownicy/użytkownicy przetwarzający dane osobowe obowiązani są dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:
   a) przetwarzane zgodnie z powszechnie obowiązującym prawem i regulacjami wewnętrznymi,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu

przetwarzaniu niezgodnemu z tymi celami,

c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

e) oraz by wypełniany był obowiązek informacyjny, w przypadkach wskazanych w przepisach prawa powszechnie obowiązującego.

4. Zasady bezpieczeństwa przetwarzania danych osobowych

§ 15.

1. W Uczelni stosowane są następujące zasady bezpiecznego przetwarzania danych osobowych:
   1) zakaz udostępniania haseł dostępu do systemów informatycznych lub pozostawiania ich w łatwo dostępnych miejscach na stanowisku pracy,
   2) zakaz udzielania informacji zawierających dane osobowe w rozmowach przez telefon, z osobami, których tożsamości nie można jednoznacznie zweryfikować i potwierdzić,
   3) wymóg przestrzegania tzw. „polityki czystego biurka" i „polityki czystego pulpitu",
   4) do codziennej pracy w systemie informatycznym wymóg używania zwykłego konta użytkownika, bez uprawnień administratora,
   5) wymóg zachowania podwyższonej ostrożności wobec wiadomości e-mail otrzymanych od niezweryfikowanych nadawców – zakaz klikania w podejrzane linki i otwierania nieznanych załączników,
   6) wymóg stosowania szyfrowania załączników zawierających dane osobowe, wysyłanych e-mailem poza obszar domeny Uczelni,
   7) wymóg pracy w odpowiednim skupieniu i bez nadmiernego pośpiechu,
   8) podczas opuszczania systemu informatycznego - wymóg wyrobienia nawyku wylogowania poprzez przycisk „Wyloguj/Wyloguj się" zamiast używania krzyżyka w celu zamknięcia okna lub pozostawiania aktywnego dostępu do systemu (bez wylogowania),
   9) po zakończeniu pracy – wymóg bieżącego usuwania zbędnych danych, zarówno w odniesieniu do dokumentów papierowych, jak i w wersji elektronicznej.
2. Podczas pracy w każdym systemie informatycznym stosowane są następujące zasady ogólne:
   1) dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca pisemne upoważnienie administratora. Pracownicy/współpracownicy mają dostęp wyłącznie do danych w takim zakresie, jaki został wskazany w upoważnieniu i wynika z umowy o pracę lub umowy cywilnoprawnej oraz przydzielonych zadań/obowiązków (zasada wiedzy koniecznej i zasada minimalizacji danych);
   2) dostęp do systemu jest możliwy wyłącznie po podaniu identyfikatora i właściwego hasła (logowanie). Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi, który jest odpowiedzialny za wszystkie czynności wykonywane przy jego użyciu,
   3) użytkownik systemu informatycznego jest zobowiązany do logowania się w taki sposób, aby uniemożliwić poznanie loginu i hasła przez osoby nieupoważnione.

3. Zasady szczególne pracy w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym" rozdział VI: Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

§ 16.

1. Czasowe (w trakcie pracy) opuszczenie przez pracownika stanowiska, na którym przetwarzane są dane osobowe, wiąże się z zastosowaniem dostępnych środków zabezpieczających, by chronić używane zasoby danych osobowych przed dostępem do nich osób nieuprawnionych.
2. Całkowite (po zakończeniu pracy w danym dniu) opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, wiąże się z zastosowaniem wszystkich dostępnych środków zabezpieczających to pomieszczenie przed wejściem tam osób niepowołanych.
3. Zabronione jest opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zastosowania odpowiedniego zabezpieczenia. Wszelkie konsekwencje takiego naruszenia mogą być traktowane jako niedopełnienie podstawowych obowiązków pracowniczych.

5. Udostępnianie danych osobowych

§ 17.

1. Udostępnianie danych osobowych podmiotom lub osobom spoza Uczelni może nastąpić na podstawie rozporządzenia (RODO) – w przypadkach wskazanych w art. 6 i 9 albo na podstawie regulacji zawartych w przepisach krajowych ustaw szczególnych.
2. Dane osobowe udostępniane są podmiotom kontrolnym uprawnionym do kontroli działalności administratora oraz podmiotom uprawnionym do przetwarzania danych osobowych zgodnie z przepisami prawa powszechnie obowiązującego.
3. Podmiotami, o których mowa w pkt 2 powyżej, są w szczególności: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy kontroli skarbowej, Policja i służby specjalne (Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego), sądy powszechne, Najwyższa Izba Kontroli, Urząd Ochrony Danych Osobowych, a także inne osoby, podmioty i organy upoważnione przez przepisy prawa i działające w granicach przyznanych im uprawnień.

6. Powierzenie przetwarzania danych osobowych

§ 18.

1. Umowa powierzenia przetwarzania danych osobowych dotyczy wyłącznie danych osobowych wynikających z realizacji umowy zasadniczej.
2. Przetwarzanie danych osobowych może zostać powierzone, w zakresie działalności prowadzonej przez Uczelnię, innemu podmiotowi, pod warunkiem zawarcia z tym podmiotem pisemnej umowy, na zasadach określonych w art. 28 rozporządzenia (RODO).
3. Zezwala się na korzystanie wyłącznie z usług takich podmiotów przetwarzających, które zobowiązują się do ochrony danych osobowych oraz zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych wskazanych w art. 32 rozporządzenia.
4. Umowa, o której mowa w ust. 1 powinna w szczególności określać:
   1) przedmiot i czas trwania przetwarzania;

2) charakter i cel przetwarzania;

3) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;

4) obowiązki i prawa Administratora oraz podmiotu przetwarzającego wynikające bezpośrednio z art. 28 rozporządzenia, a także zapewniać Administratorowi możliwość kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych w podmiocie, będącym stroną umowy zarówno przed jak i w trakcie trwania umowy.

5. Umowa o powierzenie przetwarzania danych powinna zostać przed podpisaniem, przekazana do Inspektora Ochrony Danych celem zaopiniowania.

6. Wzór umowy powierzenia stanowi załącznik nr 7 do niniejszej Polityki.

7. W uzasadnionych przypadkach dopuszcza się zastosowanie innego wzorca umowy – pod warunkiem, iż będzie on uwzględniał elementy o jakich mowa w ust 4.

8. Współadministrowanie

§ 19.

1. W przypadku wspólnego przetwarzanie danych w zbiorach przez Uczelnię z innym podmiotem, na mocy zawartej umowy lub porozumienia, ustalają one wspólnie cele i sposoby przetwarzania danych (są współadministratorami danych). W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów prawa powszechnie obowiązującego oraz aktów prawa wewnętrznego obowiązujących w obu podmiotach, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo powszechnie obowiązujące. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

2. Uzgodnienia, o których mowa w pkt 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a osobami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana osobom, których dane dotyczą.

3. Niezależnie od uzgodnień, o których mowa w pkt 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z przepisów prawa powszechnego wobec każdego z Administratorów.

4. Informacja o współadministrowaniu zbiorem danych (wskazanie współadministratorów) odnotowywane jest w Rejestrze Czynności Przetwarzania.

9. Obowiązek informacyjny

§ 20.

1. Osoba, której dane osobowe dotyczą, na podstawie art. 15 RODO ma prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane w Uczelni, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji o:

1) celu przetwarzania;

2) kategorii odnośnych danych osobowych;

3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

4) w miarę możliwości - planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
5) prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz prawie do wniesienia sprzeciwu wobec takiego przetwarzania;
6) prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Uczelnia, jako administrator danych, w ramach wypełnienia tzw. obowiązku informacyjnego określonego w art. 13 i 14 RODO podaje informacje wskazane w ust.1 w stosownych klauzulach informacyjnych przygotowywanych pod nadzorem IOD. Klauzule informacyjne są zamieszczane na stronach internetowych Uczelni, stanowią załączniki w poczcie elektronicznej lub są przekazywane odpowiednim adresatom wraz z dokumentacją papierową.
3. W przypadkach i na zasadach określonych w art. 16-22 RODO, osoba, której dane osobowe dotyczą ma prawo do:
   1) żądania, aby jej dane osobowe zostały niezwłocznie sprostowane, jeżeli są nieprawidłowe lub aby zostały uzupełnione, jeżeli dane te są niekompletne,
   2) żądania usunięcia danych osobowych,
   3) żądania ograniczenia przetwarzania danych osobowych,
   4) otrzymania w określonym formacie danych osobowych i przesłania ich do innego administratora lub żądania przesłania takich danych bezpośrednio innemu administratorowi,
   5) wniesienia sprzeciwu – z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania jej danych osobowych,
   6) niepodlegania decyzji podjętej wyłącznie na podstawie przetwarzania, które odbywa się w sposób zautomatyzowany (np. profilowanie).
4. Procedura dotycząca realizacji praw osób których dane dotyczą, stanowi załącznik nr 8 do Polityki.

10. Przekazanie danych osobowych do państwa trzeciego

§ 21.

Szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej są określone w RODO w Rozdziale V (artykuły 44-50), które dopuszczają przekazanie danych, gdy państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych, co może być stwierdzone przez Komisję Europejską w drodze decyzji, lub gdy zastosowano odpowiednie mechanizmy zabezpieczające, takie jak standardowe klauzule umowne, wiążące regułu korporacyjne czy mechanizmy certyfikacji.

VIII. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

§ 22.

1. Wprowadza się jako obowiązującą w Uczelni „Instrukcję postępowania w przypadku naruszenia ochrony danych osobowych", stanowiącą załącznik nr 9 do Polityki.
2. W przypadku gdy zdarzenie dotyczy systemów teleinformatycznych zastosowanie mają przepisy „Instrukcji zarządzania systemem informatycznym" rozdział XIV: Procedury zarządzania incydentami z zakresu bezpieczeństwa informatycznego.
3. W przypadku wpłynięcia do Uczelni informacji o zdarzeniu, IOD lub ASI analizuje otrzymane informacje oraz podejmuje niezbędne czynności wyjaśniające.

IX. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

1. Inspektor Ochrony Danych prowadzi rejestr czynności przetwarzania danych osobowych w Państwowej Akademii Nauk Stosowanych w Głogowie opracowany na podstawie zgłoszeń otrzymywanych z poszczególnych jednostek organizacyjnych.
2. Rejestr, o którym mowa w ust. 1 stanowi zestawienie wszystkich podstawowych procesów i czynności związanych z przetwarzaniem danych osobowych w Uczelni. W rejestrze tym zamieszcza się następujące informacje:
   1) nazwę oraz dane kontaktowe Administratora oraz inspektora ochrony danych;
   2) cele przetwarzania;
   3) podstawę prawną przetwarzania;
   4) nazwę systemu lub oprogramowania służącego do przetwarzania danych;
   5) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
   6) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   7) transfer danych do państwa trzeciego lub organizacji międzynarodowej;
   8) planowane terminy usunięcia poszczególnych kategorii danych;
   9) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
3. Kierownicy jednostek organizacyjnych są zobowiązani do zgłaszania do IOD wszystkich czynności przetwarzania danych osobowych realizowanych w ramach podległych im jednostek, o ile nie zostały one zgłoszone wcześniej.

X. OCHRONA DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH

1. W przypadku opracowywania, projektowania, dokonywania wyboru, a także w toku samego wykorzystywania usług, aplikacji czy innych produktów opierających się na przetwarzaniu danych niezbędnym jest uwzględnienie ochrony danych już w fazie projektowania (privacy by design) oraz domyślnej ochrony danych (privacy by default) przy zastosowaniu odpowiednich środków technicznych i organizacyjnych.
2. Przy tworzeniu i wdrażaniu technologii opartych na przetwarzaniu danych wymagana jest konsultacja z Inspektorem Ochrony Danych, w zakresie informatyki - z Administratorem Sieci Informatycznych.

XI. POSTANOWIENIA KOŃCOWE

1. Niniejsza Polityka jest na bieżąco poddawana analizie i w razie potrzeby aktualizowana. IOD analizuje, czy Polityka jest adekwatna do zmian:
   a) organizacyjnych w Uczelni, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
   b) w obowiązującym prawie.
2. Wraz z przeglądem Polityki bezpieczeństwa IOD kontroluje również pracowników i inne podmioty upoważnione do przetwarzania danych osobowych pod kątem przestrzegania przez te osoby niniejszej Polityki, Instrukcji zarządzania systemem informatycznym oraz przepisów RODO (audyty doraźne).
3. Każda osoba upoważniona do przetwarzania danych osobowych, przed dopuszczeniem do przetwarzania danych zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie potwierdzające znajomość jego treści.

XII. LISTA ZAŁĄCZNIKÓW

Załącznik nr 1 – Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 2 – Procedura dotycząca kluczy

Załącznik nr 3 – Wykaz zbiorów danych

Załącznik nr 4 – Wykaz zastosowanych środków ochrony

Załącznik nr 5 – Wzór powołania Inspektora Ochrony Danych

Załącznik nr 6 – Wzór powołania Administratora Systemów Informatycznych

Załącznik nr 7 – Wzór umowy powierzenia przetwarzania danych osobowych

Załącznik nr 8 - Procedura dotycząca realizacji praw osób których dane dotyczą

Załącznik nr 9 – Instrukcja postepowania w przypadku naruszenia ochronnych danych osobowych