AKADEMIA NAUK STOSOWANYCH
im. H. Cegielskiego w Gnieźnie
UCZELNIA PAŃSTWOWA

Załącznik do Zarządzenia nr 13/2023
Rektora ANS Gniezno
z dnia 31.03.2023 roku

POLITYKA OCHRONY DANYCH OSOBOWYCH

DOKUMENT WEWNĘTRZNY

Gniezno 2022

Spis treści

I. Wstęp

Akademia Nauk Stosowanych im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa jest administratorem danych osobowych w rozumieniu przepisów *„Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679z 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)”*. Administrator uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia wdraża odpowiednie środki techniczne i organizacyjne.

Stosowanie Polityki ochrony ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Akademię Nauk Stosowanych im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa, przed przypadkowym lub niezgodnym z prawem zbieraniem, zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogących w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

II. Postanowienia ogólne

1. Słownik pojęć.

Ilekroć w polityce ochrony danych jest mowa o:

1) ***administratorze*** - rozumie się przez to Akademię Nauk Stosowanych im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa reprezentowaną przez JM Rektora decydującego o celach i sposobach przetwarzania danych osobowych, w myśl art. 4 rozporządzenia;
2) ***inspektorze ochrony danych (IOD)***– rozumie się przez to osobę, którą administrator wyznaczył na podstawie artykułu 37 rozporządzenia;
3) ***administratorze systemu informatycznego (ASI)*** – rozumie się przez to pracownika obsługującego systemy informatyczne, odpowiedzialnego za bezpieczną eksploatację tych systemów;
4) ***gestorze*** – rozumie się przez to osobę wyznaczoną przez kierownika jednostki organizacyjnej pełniącą funkcje administratora danych dla określonego zbioru danych;
5) ***osobie upoważnionej do przetwarzania danych osobowych*** – rozumie się przez to osobę, która upoważniona została na piśmie do przetwarzania danych osobowych;

6) ***Akademii Nauk Stosowanych (ANS)*** - rozumie się przez to Akademię Nauk Stosowanych im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa
7) ***haśle*** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
8) ***identyfikatorze*** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9) ***integralności danych*** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) ***odbiorcy*** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
11) ***poufności danych*** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) ***podmiocie przetwarzającym*** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
13) ***przetwarzaniu –*** rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
14) ***raporcie*** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
15) ***rozliczalności*** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
16) ***rozporządzeniu (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 (ogólne rozporządzenie o ochronie danych, RODO);
17) ***ryzyku*** - rozumie się przez to prawdopodobieństwo, że występujące zagrożenie może spowodować straty w zasobach.
18) ***serwisancie*** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu informatycznego;
19) ***systemie informatycznym administratora danych*** – rozumie się przez to sprzęt komputerowy, oprogramowanie i dane eksploatowane w zespole

współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;

20) ***uwierzytelnianiu*** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
21) ***użytkowniku*** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

2. Cel.

Wdrożenie Polityki ochrony ma na celu zapewnienie ochrony osób fizycznych, ich praw i wolności w związku z przetwarzaniem przez Akademię Nauk Stosowanych im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa danych osobowych, zabezpieczenie danych osobowych przetwarzanych w sposób zautomatyzowany i niezautomatyzowany poprzez wykonanie obowiązków wynikających z rozporządzenia.

W związku z tym, że w zbiorach Administratora przetwarzane są między innymi dane osobowe szczególnej kategorii, a system informatyczny posiada bezpośrednie połączenie z siecią publiczną, niniejsza Polityka ochrony służy zapewnieniu odpowiedniego poziomu bezpieczeństwa danych.

Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczania.

3. Zakres stosowania.

Niniejsza Polityka ochrony dotyczy danych osobowych przetwarzanych w sposób tradycyjny w formie papierowej, jak również w systemach informatycznych.

Procedury i zasady określone w niniejszym dokumencie obowiązują wszystkie osoby upoważnione do przetwarzania danych osobowych w ANS.

III. Osoby odpowiedzialne za ochronę danych osobowych

1. Administrator.

Administratorem przetwarzanych danych osobowych jest Akademia Nauk Stosowanych im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa.

Do obowiązków Administratora należy:

1) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie Inspektora ochrony danych;
2) Podejmowanie niezbędnych i odpowiednich kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych;
3) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;
4) Wspieranie Inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do ich wykonywania.

2. Inspektor ochrony danych

Inspektor ochrony danych (IOD) powoływany jest na stanowisko przez Administratora.
Do obowiązków Inspektora ochrony danych należy:

1) Informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie;
2) Działania zwiększające świadomość w dziedzinie ochrony danych osobowych oraz szkolenie personelu uczestniczącego w operacjach przetwarzania danych osobowych;
3) Monitorowanie przestrzegania ogólnego Rozporządzenia o ochronie danych, innych przepisów oraz niniejszej Polityki ochrony danych osobowych;
4) Udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;
5) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem zgodnie z art. 36 Rozporządzenia;
6) Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

3. Gestor danych osobowych w jednostce.

Gestor danych osobowych w jednostce wyznaczany jest przez kierownika jednostki organizacyjnej ANS i w jego imieniu realizuje przedsięwzięcia z zakresu ochrony danych osobowych.
Do obowiązków Gestora danych osobowych jednostki organizacyjnej należy:

1) Zapoznawanie osób zatrudnionych w jednostce przy przetwarzaniu danych osobowych z obowiązującymi przepisami.
2) Bieżące zgłaszanie do Administratora osób, które należy przeszkolić w celu wydania upoważnienia do przetwarzania danych.
3) Dbałość o to, żeby dane osobowe były:
   a) przetwarzane zgodnie z prawem;
   b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddane dalszemu przetworzeniu;
   c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą nie dłużej, niż jest to niezbędne do osiągnięcia celu przetworzenia.
4) Dokonywanie wspólnie z Administratorem systemu informatycznego, raz w roku przeglądu osób uprawnionych do przetwarzania danych osobowych pod kątem ich aktualności, sporządzenie notatki i przesłanie jej do Inspektora ochrony danych.
5) Dokonywanie wspólnie z ASI, Oceny skutków dla ochrony danych w projektowanych systemach przetwarzania danych osobowych zgodnie z art. 35 ust. 3 rozporządzenia.

6) Zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa danych osobowych.
7) Dokonywanie raz w roku przeglądu osób upoważnionych do przetwarzania danych osobowych w jednostce organizacyjnej pod kątem ich aktualności, sporządzenie notatki i przesłanie jej do Inspektora ochrony danych.
8) Zgłaszanie do IOD nowych czynności przetwarzania.
9) Natychmiastowe zgłaszanie zauważonych incydentów naruszenia bezpieczeństwa danych osobowych i dalsze postępowanie zgodnie z „Procedura postępowania w sytuacji naruszenia ochrony danych osobowych".
10) Określenie osób, których dane zastały naruszone.
11) Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych oraz sposobu zabezpieczenia danych po incydencie.
12) Bieżąca współpraca z IOD w zakresie przedsięwzięć realizowanych w jednostce organizacyjnej, w których występuje przetwarzanie danych osobowych (umowy, konferencje, …).

4. Osoby upoważnione do przetwarzania danych osobowych

Pracownicy mogą przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora w upoważnieniu i tylko w celu wykonywania nałożonych na niego obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych. Ponadto osoby upoważnione zobowiązane są do:

a) zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
b) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki ochrony danych osobowych;
c) stosowania określonych przez Administratora oraz Inspektora ochrony danych procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
d) korzystania z systemów informatycznych Administratora sposób zgodny ze wskazówkami zawartymi w ich instrukcjach obsługi;
e) zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym;
f) współpracy z Inspektorem Ochrony Danych w zakresie przeprowadzanych audytów ochrony danych osobowych.

IV. Organizacja przetwarzania danych osobowych

1. Przetwarzanie danych osobowych

Przetwarzanie danych osobowych w Akademii Nauk Stosowanych odbywa się z poszanowaniem praw i wolności osób, których dane są przetwarzane, w zgodzie z Rozporządzeniem o ochronie danych osobowych oraz niniejszą Polityką ochrony danych.

Oznacza to, że dane osobowe przetwarza się:

1) zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (zasada legalności),
2) w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (zasada rzetelności),
3) w sposób przejrzysty dla osób, których dane dotyczą (zasada przejrzystości),
4) w konkretnych, wyraźnych i prawnie uzasadnionych celach (zasada ograniczenia celu),
5) w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (zasada minimalizacji danych),
6) przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (zasada prawidłowości),
7) przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane
   (zasada ograniczenia przechowywania),
8) w sposób zapewniający odpowiednie bezpieczeństwo (integralność i poufność).

Administrator gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

Niniejsza Polityka nie wyklucza stosowania przepisów Ustawy z dnia 5 sierpnia 2010 r. „O ochronie informacji niejawnych”, tajemnicy zawodowej oraz zarządzenia Rektora ANS w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego wykazu akt oraz instrukcji archiwalnej.

2. Realizacja obowiązków informacyjnych przy przetwarzaniu danych osobowych

1) Gestorzy danych osobowych oraz wszystkie osoby odpowiedzialne za procesy, w których zbierane są dane osobowe, mają obowiązek zachowania szczególnej staranności, w tym:
   a. sprawdzać czy są spełnione podstawy prawne na pozyskiwanie danych osobowych, zgodnie z art. 6 RODO oraz art. 9 – 10 RODO;

b. zbierać dane osobowe dla określonych, zgodnych z prawem, celów realizowanych w Akademii Nauk Stosowanych;
c. zbierać dane w zakresie adekwatnym do celów, w jakich dane będą przetwarzane.

1) W przypadku konieczności odbierania zgody na przetwarzanie danych osobowych, należy zapewnić dobrowolność jej pozyskania oraz powiadamiać o prawie do odwołania takiej zgody.
3) Treść oświadczeń zgody na przetwarzanie danych osobowych musi być konsultowana z Inspektorem ochrony danych oraz w uzasadnionych przypadkach z Radcą prawnym.
4) Osoby, które wykonują zadania związane ze zbieraniem danych osobowych, są:
   a. odpowiedzialne za realizację obowiązków informacyjnych określonych w art. 13 i 14 RODO.
   b. zobowiązane sprawdzać, czy na formularzach lub innego typu dokumentach (w formie papierowej lub elektronicznej) dedykowanych do zbierania danych, jest zamieszczona stosowna klauzula informacyjna.
5) Za stosowanie właściwych klauzul informacyjnych przy zbieraniu danych osobowych, odpowiada Kierownik jednostki organizacyjnej, osoby odpowiedzialnej za proces zbierania danych.
6) Treść klauzul informacyjnych musi być konsultowana z Inspektorem ochrony danych oraz w uzasadnionych przypadkach z Radcą prawnym.

3. Retencja danych.

Administrator wyznacza okres legalnego przetwarzania danych osobowych, biorąc pod uwagę następujące czynniki:

1) Cel, w którym dane są przetwarzane,
2) Podstawę prawną legalizującą przetwarzanie danych w tym celu.

Zgodnie z ogólnym rozporządzeniem o ochronie danych, dane osobowe mogą być przetwarzane jedynie przez okres nie dłuższy, niż jest to niezbędne do realizacji celów, w których zostały zebrane. Koniec okresu niezbędności przetwarzania wynika z następujących przesłanek:

1) Osiągnięcia celu przetwarzania – np. gdy dane osobowe przetwarzane są przed zawarciem umowy w celu prowadzenia rokowań, zakończenie negocjacji i podpisanie umowy czyni bezprzedmiotowym ten cel.

2) Wygaśnięcia okresu legalnego przetwarzania danych wynikającego z przepisu prawa – np. jeżeli dane osobowe są przetwarzane w celu obrony przed potencjalnymi roszczeniami z tytułu wykonanej umowy, to upływ terminu przedawnienia powoduje wygaśnięcie tej podstawy prawnej.

3) Cofnięcia udzielonej zgody, jeżeli dane osobowe przetwarzane były wyłącznie na podstawie zgody osoby, której dane dotyczą.

W przypadku, gdy administrator nie jest w stanie precyzyjnie wskazać okresu retencji, może poprzestać na wskazaniu przesłanek ustalenia tego okresu. Wskazuje się sposób określenia okresu przetwarzania danych osobowych, nie zaś konkretną datę, w której zostaną one przez administratora danych usunięte.

Okresy retencji danych osobowych są odnotowywane w poniższych dokumentach:

1) Klauzuli informacyjnej o przetwarzaniu danych osobowych udostępnianej osobie, której dane dotyczą.
2) Rejestrze czynności przetwarzania, w którym wskazuje się planowane terminy usunięcia poszczególnych kategorii danych osobowych.

Zasady ustalania czasu retencji i usuwania danych osobowych znajdują się w załączniku nr 13 – Procedura retencji danych osobowych.

4. Powierzenie przetwarzania danych osobowych.

1) Akademia Nauk Stosowanych dopuszcza, by dane osobowe, których jest administratorem, były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia przetwarzania danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2) Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3) Zawierana przez Administratora umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO. Wzór umowy znajduje się w Załączniku Nr 12.
4) Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.
5) W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w art. 28, znajdują się w już zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6) Każdorazowo, przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, należy poinformować Inspektora ochrony danych oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.

5. Upoważnienie do przetwarzania danych.

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych, przetwarzają je wyłącznie na pisemne polecenie administratora na podstawie art. 29 Rozporządzenia.

Procedura nadawania oraz odwoływania upoważnień wraz ze wzorem upoważnienia zawarta jest w załączniku nr 1.
Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Inspektor ochrony danych. Upoważnienia przechowuje się w teczkach osobowych w Dziale Kadr.

6. Realizacja praw osób, których dane dotyczą.

Realizacja praw osób, których dane dotyczą odbywa się na podstawie art. 15 – 18 oraz art. 20 – 22 rozporządzenia o ochronie danych osobowych.
Sposób zgłaszania żądania oraz zasady realizacji zawarte są w „Procedura realizacji żądań osób, których dane dotyczą", stanowiącej załącznik nr 2.
Ewidencję zgłoszeń i odpowiedzi prowadzi Inspektor ochrony danych.

7. Rejestrowanie czynności przetwarzania.

Na podstawie art. 30 ust. 1 rozporządzenia, Administrator – a w jego imieniu Inspektor ochrony danych prowadzi rejestr czynności przetwarzania danych osobowych.
Na podstawie art. 30 ust. 2 rozporządzenia, Podmiot przetwarzający – a w jego imieniu Inspektor ochrony danych prowadzi rejestr kategorii czynności przetwarzania danych osobowych.
Rejestry prowadzone są w formie pisemnej, w tym elektronicznej.
Wzory rejestrów umieszczone są z załącznikach nr 3 i 4.

8. Szacowanie ryzyka przetwarzania danych

Zasada podejścia opartego na ryzyku (risk based approach) uzależnia sposób realizacji obowiązków nałożonych na administratora od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów administratora.
Szacowanie ryzyka ma na celu określenie, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i jak dotkliwe straty mogą powstać.
Ryzyko mierzone jest na podstawie czynników realnie wpływających na bezpieczeństwo danych osobowych o różnej wadze zagrożenia z jednoczesnym uwzględnieniem naruszenia praw lub wolności osób fizycznych. Szacowanie ryzyka jest procesem ciągłym.
Sposób szacowania ryzyka zawiera załącznik nr 5 - „Procedura szacowania ryzyka przetwarzania danych".

9. Ocena skutków dla ochrony danych.

Zgodnie z art. 35 ust. 1 RODO, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Oznacza to, że przeprowadzenie oceny skutków dla ochrony danych jest wymagane zawsze wtedy, gdy:

1) poziom ryzyka określony został jako wysoki w wyniku jego szacowania przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania,
2) dany rodzaj przetwarzania został wskazany w przepisie prawa (np. art. 35 ust. 3 RODO),
3) dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy, zgodnie z art. 35 ust. 4 RODO.

Sposób oceny skutków dla ochrony danych zawarty jest w „Procedurze oceny skutków dla ochrony danych" stanowiącej załącznik nr 6.

10. Naruszenie bezpieczeństwa danych osobowych

Naruszenie bezpieczeństwa danych osobowych prowadzi do przypadkowego lub celowego zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Każdy pracownik Akademii Nauk Stosowanych, który podejrzewa, że doszło do naruszenia zasad ochrony danych osobowych, zobowiązany jest niezwłocznie wykonać czynności określone w „Procedurze postępowania w sytuacji naruszenia ochrony danych osobowych" (nie później jednak niż 12 godzin po stwierdzeniu naruszenia) – załącznik nr 7. Incydent naruszenia bezpieczeństwa danych osobowych odnotowany zostaje w „Rejestrze naruszeń ochrony danych osobowych" - załącznik nr 8.

11. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki (w miarę możliwości, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia) – zgłasza je właściwemu organowi nadzorczemu.

Sposób zgłaszania zawarty jest w załączniku nr 9 - „Procedura zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu"

12. Zawiadamianie osoby, której dane dotyczą.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Sposób zawiadamiania zawarty jest w załączniku nr 10 - „Procedurze zawiadamiania osoby, której dane dotyczą".

V. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

1. Bezpieczeństwo osobowe.

a) Zachowanie poufności.

Bezpieczeństwo osobowe realizowane jest poprzez wdrożenie zasady poufności oraz dzięki prowadzonym szkoleniom z zakresu ochrony danych osobowych, obejmujących procedury wynikające z RODO oraz z niniejszej Polityki ochrony danych osobowych. W celu zachowania poufności danych osobowych, wszyscy pracownicy Akademii Nauk Stosowanych im. Hipolita Cegielskiego w Gnieźnie oraz osoby współpracujące, zobowiązywane są do zachowania tajemnicy na podstawie pisemnego oświadczenia.

Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

b) Szkolenia w zakresie ochrony danych osobowych.

Inspektor ochrony danych prowadzi następujące szkolenia:

- dla osób nowo zatrudnionych, które mają zostać upoważnione do przetwarzania danych osobowych;
- szkolenia wewnętrzne dla wszystkich osób upoważnionych do przetwarzania danych osobowych - w przypadku zmiany zasad lub procedur ochrony danych osobowych (również metodą e-learningu);
- cyklicznie - dla wszystkich osób (przede wszystkim metodą e-learningu).

Tematyka szkoleń głównie obejmuje:

- przepisy dotyczące ochrony danych osobowych;
- obowiązki osób upoważnionych do przetwarzania danych osobowych;
- odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych;
- zasady i procedury określone w Polityce ochrony danych osobowych.

2. Bezpieczeństwo pomieszczeń, w których przetwarzane są dane osobowe.

W siedzibie Administratora wydzielono pomieszczenia szczególnie chronione (dostęp dla ściśle określonych osób) oraz ogólnodostępne (dla wszystkich osób).

W pomieszczeniach szczególnie chronionych dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tych pomieszczeń wchodzą min. serwerownie, punkt obsługi dokumentów niejawnych. W tych pomieszczeniach mogą przebywać wyłącznie pracownicy obsługujący serwery i punkt obsługi, inne osoby upoważnione

do przetwarzania danych osobowych tylko w towarzystwie tych pracowników, a osoby postronne w ogóle nie mają dostępu.

W pomieszczeniach ogólnodostępnych, dostęp do danych osobowych mają tylko osoby upoważnione do przetwarzania danych osobowych, zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w nich przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie Administratora.
Klucze do lokali wchodzących w skład wymienionych stref przechowywane są w depozytorze kluczy i pobierane przez upoważnione osoby, co jest odnotowane w elektronicznym systemie wydawania kluczy. Wykonywanie osobistych kopii kluczy do tych pomieszczeń jest zabronione. Ochrona pozostałych pomieszczeń realizowana jest za pomocą kontroli dostępu – poprzez nadanie uprawnień dla wybranych pracowników.

3. Zabezpieczenie sprzętu.

Sprzęt służący do przetwarzania danych osobowych zlokalizowany jest ww. strefach. Wszystkie komputery, na których odbywa się przetwarzanie danych osobowych, muszą mieć zainstalowane przez pracowników Działu IT certyfikowane oprogramowanie oraz zablokowane możliwości samodzielnego instalowania innego oprogramowania przez użytkowników. Próby samodzielnego instalowania oprogramowania umożliwiającego przetwarzanie danych osobowych są zabronione.
W celu zapewnienia niezawodności zasilania serwery administratora podłączone są do zasilaczy awaryjnych (UPS).
Bieżąca konserwacja sprzętu wykorzystywanego przez administratora do przetwarzania danych, prowadzona jest tylko przez jego pracowników obsługujących systemy informatyczne. Naprawy wykraczające poza możliwości osób obsługujących, wykonywane są przez personel zewnętrzny w siedzibie administratora, po zawarciu z podmiotem wykonującym naprawę umowy, o powierzeniu przetwarzania danych osobowych, określającej min. kary umowne za naruszenie bezpieczeństwa danych.

4. Obowiązki osób przetwarzających dane osobowe.

Niezwykle ważne dla bezpieczeństwa danych jest przestrzeganie przez każdą osobę upoważnioną do przetwarzania danych poniższych zaleceń:

1) W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
   a) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych);
   b) loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.
2) Użytkownik nie zapisuje hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku i nie pozostawia go w pobliżu komputera.
3) W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć osoba nieuprawniona, należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób, uniemożliwiający wgląd w wyświetlaną treść.

4) Zabrania się samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych) nawet, gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych.
5) Przestrzeganie swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła.
6) Udostępnianie danych osobowych pocztą elektroniczną należy realizować tylko w postaci zaszyfrowanej.
7) Rozsyłanie informacji pocztą elektroniczną do wielu odbiorców należy realizować w kopii ukrytej.
8) W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym, należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu.
9) Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.
10) Przed opuszczeniem miejsca pracy lub po zakończeniu dnia pracy, wszelkie wydruki zawierających dane osobowe należy zniszczyć w niszczarce (jeżeli nie będą już przydatne lub schować do szaf zamykanych na klucz).
11) Po zakończeniu pracy w danym dniu należy zamknąć drzwi na klucz i pozostawić go na portierni (nie dotyczy pomieszczeń chronionych Kontrolą dostępu).
12) Należy zachować w tajemnicy poznane dane osobowe oraz sposób zabezpieczenia pomieszczeń i sprzętu komputerowego.

5. Postępowanie z nośnikami i ich bezpieczeństwo.

Osoby upoważnione do przetwarzania danych osobowych powinny szczególnie pamiętać o tym, że:

1) dane osobowe w postaci tradycyjnej należy przechowywać w zamykanych na klucz szafach lub szufladach. Dostęp do tych danych mają ściśle określone osoby, posiadające upoważnienie do przetwarzania danych osobowych;
2) zabrania się powtórnego używania jednostronnie zadrukowanych kartek do sporządzania brudnopisów pism, jeśli zawierają one dane osobowe;
3) po wykorzystaniu, wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce;
4) wynoszenie danych osobowych poza obszar przetwarzania jest zabroniony. Dopuszczalne jest przemieszczanie akt osobowych pomiędzy obiektami, np. w celu złożenia ich w archiwum lub dostarczenia do dziekanatu. Ze względów bezpieczeństwa zabrania się przewożenia akt osobowych publicznymi środkami transportu;
5) dane osobowe kopiowane na przenośne nośniki (płyty CD/DVD/BLU-RAY, pendrive'y, karty pamięci, inne) niebędące kopiami zapasowymi, należy przechowywać w postaci zaszyfrowanej lub pseudonimizowanej. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach lub szufladach, nieudostępnianych osobom postronnym. Po wykorzystaniu danych, należy

je trwale usunąć z tych nośników np. przez fizyczne zniszczenie (nośniki optyczne) lub usunięcie programem trwale usuwającym pliki, dostępnym w Dziale IT;

6) uszkodzone nośniki na których znajdowały się dane osobowe, przed ich wyrzuceniem należy zniszczyć fizycznie (nośniki optyczne) lub oddać do Działu IT, który zniszczy je zgodnie z „Procedurą niszczenia danych poufnych".

6. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator lub zewnętrzna firma z którą podpisano umowę przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła.

7. Kontrola dostępu do sieci

Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej. Używanie służbowej poczty elektronicznej jest dozwolone wyłącznie przy zapewnieniu, że wykorzystywane do odczytu urządzenie posiada aktualny program antywirusowy. Jest to minimalnym wymogiem stawianym w celu zapewnienia bezpieczeństwa.

8. Komputery przenośne i praca na odległość.

Korzystanie ze sprzętu służbowego poza terenem uczelni dozwolone jest tylko za pisemną zgodą Administratora. Komputery przenośne oraz nośniki danych zawierające dane osobowe, wynoszone z siedziby administratora należy zabezpieczyć hasłami (o ile jest to możliwe) a same dane osobowe powinny być zaszyfrowane lub pseudonimizowane. Komputery przenośne należy przewozić w odpowiednich torbach i chronić je przed czynnikami zewnętrznymi mogącymi spowodować uszkodzenie.

Wykorzystywanie komputerów przenośnych administratora w miejscach publicznych jest dozwolone, o ile otoczenie w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. Nie należy pozostawiać w widocznym miejscu bez nadzoru: dokumentów, nośników danych i sprzętu informatycznego.

Zdalny dostęp do systemów informatycznych ANS realizowany jest za pomocą połączenia szyfrowanego VPN.

Praca zdalna może być wykonywana pod warunkiem przestrzegania zasad zawartych w załączniku nr 11 – Zasady pracy zdalnej.

9. Monitoring wizyjny.

W celu zapewnienia bezpieczeństwa osób przebywających na terenie uczelni oraz ochrony mienia, Administrator prowadzi monitoring wizyjny terenu Uczelni. Monitorowany jest teren wokół budynków, wejścia do budynków, korytarze oraz część sal wykładowych. Programy do obsługi monitoringu nie posiadają funkcji rozpoznawania twarzy ani żadnej innej, umożliwiającej identyfikację osób. Zebrane dane wizyjne nie podlegają dalszej obróbce. Dostęp do miejsca przechowywania nagrań jest chroniony
a liczba osób mająca dostęp ograniczona do minimum i ściśle określona. Miejsca monitorowane oznakowane są w widoczny i czytelny sposób, za pomocą odpowiednich znaków informacyjnych.

10. Przeglądy okresowe.

Inspektor ochrony danych przeprowadza raz w roku przegląd zakresu przetwarzanych danych osobowych pod kątem ich zgodności z prawem.
Kierownicy poszczególnych jednostek organizacyjnych Akademii Nauk Stosowanych oraz Gestorzy danych osobowych, są obowiązani dokonać przeglądu danych osobowych, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.
Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez kierownika jednostki organizacyjnej, Gestora danych osobowych i Administratora systemu informatycznego, z którego usunięto dane osobowe. Protokół należy przesłać do Inspektora ochrony danych.
Administrator systemu informatycznego wspólnie z Gestorem, przeprowadzają raz w roku przegląd osób upoważnionych do przetwarzania danych osobowych w danym systemie, pod kątem ich aktualności. Z przeglądu sporządzają notatkę, którą przesyłają do Inspektora ochrony danych.
Wszystkie powyższe przeglądy należy wykonać do 30 kwietnia.
Inspektor ochrony danych sporządza zbiorczą informację ze zrealizowanych przeglądów i przedstawia ją Administratorowi.
Inspektor ochrony danych może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora.

11. Udostępnianie i przekazywanie danych osobowych.

A. Udostępnianie danych osobowych

Udostępnianie danych osobowych w celach innych niż włączenie do zbioru, innym odbiorcom danych może nastąpić wyłącznie na pisemny, umotywowany wniosek chyba, że przepis innej ustawy stanowi inaczej.

Udostępnianie danych na żądanie osoby, której dane dotyczą

Wniosek o udostępnienie danych może być realizowany w ramach procedury uregulowanej w art. 15 ust. 1 RODO (dostępu do danych), jak i też art. 15 ust. 3 RODO (uzyskania kopii danych). Wnioskodawca, tj. osoba, której dane dotyczą, powinien jasno

określić, czy chce skorzystać z prawa dostępu do swoich danych osobowych, czy też z prawa do uzyskania kopii przetwarzanych danych osobowych. Sposób zgłaszania żądania oraz zasady realizacji zawarte są w załączniku nr 2 - „Procedura realizacji żądań osób, których dane dotyczą".

Udostępnianie danych osobowych na żądanie podmiotu zewnętrznego

1. Udostępnianie danych osobowych podmiotowi zewnętrznemu może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:

a) oznaczenie wnioskodawcy;
b) wskazanie przepisów uprawniających do dostępu do informacji;
c) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia;
d) wskazanie imienia i nazwiska osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.

Osoba udostępniająca dane osobowe jest obowiązana zażądać pokwitowania pobrania dokumentów zawierających informacje, przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.

B. Przekazywanie danych osobowych do państw trzecich

Przekazanie danych do państwa trzeciego (poza Europejski Obszar Gospodarczy), może nastąpić tylko po spełnieniu określonych warunków, wskazanych w Rozdziale V rozporządzenia.

Zgodnie z RODO, legalne przekazanie danych osobowych może nastąpić w jednym z trzech trybów:

a) przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony (art. 45 RODO),
b) przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń (art. 46–47 RODO),
c) przekazywanie na zasadzie wyjątku w szczególnych sytuacjach (art. 49 RODO).

Bezpieczne przekazanie danych jest procesem skomplikowanym i wymaga dogłębnej analizy oraz wyboru odpowiednich narzędzi transferu danych, zapewniających poziom ochrony równoważny do krajów EOG.

Analizę należy przeprowadzić zgodnie z załącznikiem nr 14 – Procedura wyboru narzędzi przekazywania danych do państw trzecich.

C. Dodatkowe warunki udostępniania i przekazywanie danych osobowych.

Każdorazowo, przed planowanym udostępnieniem lub przekazaniem danych osobowych, pracownik jest zobowiązany skontaktować się z Inspektorem ochrony danych oraz skonsultować z nim warunki ujawnienia danych osobowych. Udostępnienie lub przekazanie danych osobowych może odbyć się wyłącznie po uzyskaniu akceptacji warunków ujawnienia tych danych przez IOD.

12. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych.

Niezastosowanie się przez pracownika do wprowadzonej Polityki ochrony danych osobowych, jest równoznaczne z naruszeniem obowiązków pracowniczych, zgodnie

z Kodeksem pracy i Regulaminem pracy ANS i może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 266 Kodeksu karnego.
Naruszenie postanowień Polityki ochrony danych przez kontrahenta lub jego pracowników może stanowić podstawę do odstąpienia od umowy i żądanie pokrycia powstałej szkody.

VI. Przeglądy polityki ochrony danych i audyty systemu

Polityka ochrony danych powinna być poddawana przeglądowi przynajmniej raz na rok lub częściej w razie:
a) istotnych zmian w budowie systemu informatycznego;
b) zmian organizacyjnych administratora, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych;
c) zmian w obowiązującym prawie.
Przeglądu Polityki ochrony danych osobowych dokonuje Inspektor ochrony danych wspólnie z Administratorem systemu informatycznego oraz Gestorami danych osobowych.
W celu zapewnienia wysokiego poziomu bezpieczeństwa danych osobowych, okresowo przeprowadzany jest audyt wewnętrzny realizowany przez Inspektora danych osobowych przy wsparciu osób wskazanych przez IOD. Audyt może zostać przeprowadzony w każdej jednostce organizacyjnej ANS. Inspektor Ochrony Danych informuje, z co najmniej tygodniowym wyprzedzeniem, kierownika jednostki organizacyjnej o terminie oraz zakresie audytu. Po przeprowadzeniu audytu IOD sporządza i przekazuje raport, w którym ujęte są ewentualne nieprawidłowości i uchybienia. W ciągu dwóch tygodni kierownik jednostki organizacyjnej zobowiązany jest do poprawienia wskazanych nieprawidłowości oraz poinformowania Inspektora Ochrony Danych o podjętych i zrealizowanych czynnościach.

VII. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
Polityka ochrony danych osobowych Akademii Nauk Stosowanych jest zasadniczym dokumentem normującym sposób ochrony danych osobowych przez wszystkie osoby upoważnione do ich przetwarzania na terenie ANS.

VIII. Załączniki

Załącznik nr 1 – Procedura nadawania oraz odwoływania upoważnień wraz ze wzorem upoważnienia.
Załącznik nr 2 – Procedura realizacji żądań osób, których dane dotyczą.
Załącznik nr 3 – Wzór rejestru czynności przetwarzania.
Załącznik nr 4 – Wzór rejestr kategorii czynności przetwarzania.
Załącznik nr 5 – Procedura szacowania ryzyka przetwarzania danych.
Załącznik nr 6 – Procedura oceny skutków dla ochrony danych.
Załącznik nr 7 – Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.
Załącznik nr 8 – Wzór rejestru naruszeń ochrony danych osobowych.
Załącznik nr 9 – Procedura zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu
Załącznik nr 10 – Procedura zawiadamiania osoby, której dane dotyczą
Załącznik nr 11 – Zasady pracy zdalnej
Załącznik nr 12 –Wzór umowy powierzenia przetwarzania danych osobowych
Załącznik nr 13 – Procedura retencji danych osobowych
Załącznik nr 14 – Procedura wyboru narzędzi przekazywania danych do państw trzecich