ZARZADZENIE nr 15/2022

Rektora Akademii Nauk Stosowanych im. Józefa Gołuchowskiego

z dnia 1 października 2022 r.

w sprawie wprowadzenia dokumentów regulujących zagadnienia bezpieczeństwa informacji w zakresie ochrony danych osobowych przetwarzanych w Akademii Nauk Stosowanych im. Józefa Gołuchowskiego

Na podstawie art. 23 ust. 2 pkt. 11 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (T. j. Dz. U. 2022. poz. 574 z późn. zm.) , art. 24 ust. 2 i art.35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/629 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. U. UE 4.5.2016) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019, poz.1781), działając w oparciu o postanowienia § 21 ust.2 i ust.5 pkt.1 Statutu Akademii Nauk Stosowanych im. Józefa Gołuchowskiego (zwanej dalej ANSG),wprowadzonego uchwałą nr 4/2022 Zgromadzenia Wspólników Ostrowieckiej Szkoły Biznesu - spółki z o. o. (założyciela ANSG) z dnia 20 kwietnia 2022 r., **zarządza się co następuje**.

§1

1. Wprowadzam Politykę Ochrony Danych Osobowych w ANSG, która stanowi ***załącznik nr 1*** do niniejszego zarządzenia.

2. Zatwierdzam Analizę i Ocenę Zagrożeń oraz Ryzyka przy przetwarzaniu danych osobowych w ANSG, która stanowi ***załącznik nr 2*** do niniejszego zarządzenia

§ 2

1. Dokumenty, o których mowa w § 1 pkt. 1 i 2 mają zastosowanie na wszystkich stanowiskach i miejscach pracy, w których przetwarzane są dane osobowe w ANSG. Z treścią dokumentów, o których mowa w § 1 kierownicy jednostek organizacyjnych zapoznają wszystkich pracowników zatrudnionych w danej jednostce przy przetwarzaniu danych osobowych lub pracujących w systemach informatycznych.

2. Zgodnie z zaleceniami Urzędu Ochrony Danych osobowych (UODO) opublikowanymi na stronie https://www.uodo.gov.pl/ dokumenty Polityki ochrony danych osobowych należy traktować jako dokumenty wewnętrzne udostępniane jedynie ograniczonemu kręgowi osób np. tylko tym osobom, którym są niezbędne w związku z powierzonymi im zadaniami.

3. Inspektora Ochrony Danych ANSG zobowiązuję do:

    1) prowadzenia nadzoru nad realizacją zadań i przestrzeganiem zasad zawartych polityce ochrony danych osobowych, o której mowa w § 1 pkt. 1 przez poszczególne jednostki organizacyjne w ANSG;

    2) wykonania zadań określonych w § 10 (Audyt i Szkolenia) Polityki w/w polityki ochrony danych osobowych;

3) zamieszczenia na podmiotowej stronie internetowej uczelni:

   a) klauzuli informacyjnej o przetwarzaniu danych osobowych w ANSG;
   b) danych dotyczących inspektora ochrony danych ANSG, o których mowa w art.10 ust.1 ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

§ 3

Zarządzenie wchodzi w życie z dniem 1 października 2022 r. podpisania. Jednocześnie traci moc zarządzenie nr 17.1/2018 Rektora WSBiP z dnia 25 maja 2018 października 2019 r. w sprawie **wprowadzenia dokumentów regulujących zagadnienia bezpieczeństwa informacji w zakresie ochrony danych osobowych przetwarzanych** w WSBiP w Ostrowcu Świętokrzyskim i zarządzenie nr 2/2020 rektora WSBiP z dnia 10 lutego 2020 r. w sprawie zmian w Polityce Ochrony Danych Osobowych w WSBiP w Ostrowcu Świętokrzyskim.

.

Wykonano w 1 egz.
Egz. nr 1- Rektorat
Dok. wykonał: Stefan SUSKA- Dyrektor Biura Org.- Prawnego
Marek GAWLIK- Inspektor Ochrony Danych Osobowych

Załącznik. nr1 *do zarządzenia nr 15/2022*
Rektora ANSG z dnia 1.10.2022r.

POLITYKA OCHRONY DANYCH OSOBOWYCH
w Akademii Nauk Stosowanych im. Józefa Gołuchowskiego

Sporządzona w oparciu o 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 (zwane dalej: RODO)

Na niniejszy dokument składają się następujące zagadnienia:

§1. Zagadnienia ogólne

1. Polityka bezpieczeństwa określa sposób prowadzenia i zakres dokumentacji opisującej zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
2. Przez użyte w treści sformułowania należy rozumieć:

bezpieczeństwo - stan faktyczny uniemożliwiający wykorzystanie, przepływ, modyfikację danych osobowych przetwarzanych ANSG, przez osoby postronne i nieupoważnione lub zniszczenie tych danych;

dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej);

przetwarzanie danych osobowych – operacje dokonywane na danych osobowych, takie 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;

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

Administrator Danych Osobowych (ADO) – **Akademia Nauk Stosowanych im. Józefa Gołuchowskiego**. (dalej: ANSG lub Uczelnia),

Administrator Systemu Informatycznego (ASI) informatyk uczelni odpowiedzialny za systemy informatyczne;

system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

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

3. ANSG jako ADO przetwarza dane osobowe w celach:
   1) właściwego wykonywania zobowiązań wynikających z zawartych umów,
   2) prawidłowego wykonywania innych czynności niezbędnych w ramach realizacji umów (wystawianie faktur, księgowanie, kontakt ze studentami, obsługa procedury przyznawania stypendiów),
   3) realizacji przepisów wynikających z prawa pracy i kodeksu cywilnego (pracownicy, osoby zatrudnione na podstawie umów cywilnoprawnych),
   4) wypełniania prawnie usprawiedliwionych celów (np. dochodzenia roszczeń).
4. Przetwarzanie danych osobowych w ANSG odbywa się na podstawie:
   1) zawartych umów (art. 6 ust. 1 pkt. b RODO),
   2) wyrażonych zgód (art. 6 ust. 1 pkt. a RODO),
   3) obowiązku prawnego ciążącego na ADO (art. 6 ust. 1 pkt. c RODO),
   4) prawnie usprawiedliwionych interesów ADO (art. 6 ust. 1 pkt. f RODO).

§2. Zakres odpowiedzialności

1. Administrator danych osobowych, czyli ANSG, zobowiązany jest do przestrzegania wszystkich przepisów RODO, w szczególności poprzez:

1) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z przepisów o ochronie danych osobowych,
   2) określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe,
   3) zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w zakresie danych osobowych,
   4) wdrażanie i nadzorowanie przestrzegania polityki ochrony danych,
   5) wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   6) działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
   7) stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania przepisów o ochronie danych osobowych,
   8) odpowiedzialność za poprawność merytoryczną gromadzonych danych ,
   9) informowanie osób, których dane są przetwarzane o celu zbierania danych, ich zakresie, podmiotach (osobach), którym dane są udostępniane, terminie przetwarzania danych,
   10) informowanie osób, których dane są przetwarzane o ich prawach wynikających z RODO.
2. Za bezpieczeństwo informacji odpowiedzialny jest ponadto każdy pracownik ANSG. Pracownicy Uczelni oraz inne osoby przetwarzające w imieniu ADO dane osobowe:
   1) odpowiadają za prawidłową realizację RODO w ramach powierzonych im do przetwarzania danych osobowych,
   2) monitorują prawidłowość fizycznych zabezpieczeń pomieszczeń, w których dane są przetwarzane oraz zwracają uwagę na przebywające w nich osoby,
   3) zwracają uwagę, czy zostało zapewnione awaryjne zasilanie komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, a w przypadku ich braku, informują ASI,
   4) monitorują bezpieczeństwo danych zawartych w komputerach przenośnych, dyskach wymiennych, laptopach, w których przetwarzane są dane osobowe,
   5) dbają o prawidłowy obieg oraz przechowywanie dokumentów zawierających dane osobowe,
   6) dbają o działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
   7) kontrolują dostęp do danych.
3. Pracownicy, którzy sprzątają pomieszczenia, mają obowiązek zachowania w tajemnicy informacji dotyczących danych osobowych, jeżeli zdarzyłoby się, że miałyby do nich dostęp.
4. Administrator systemu informatycznego odpowiedzialny jest za:

1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2) optymalizację wydajności systemu informatycznego, baz danych,
3) instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4) instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5) konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8) zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10) przyznawanie na wniosek ADO praw dostępu do informacji w danym systemie,
11) prowadzenie profilaktyki antywirusowej.

§3. Przetwarzanie danych osobowych

1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
5. Archiwizacja informacji zawierających dane osobowe odbywa się w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonych pomieszczeniach, które są zabezpieczone przed dostępem osób nieupoważnionych.
6. Dokumenty zawierające dane osobowe, które nie służą już celowi przetwarzania i nie są niezbędna do przechowywania z prawnego punku widzenia, podlegają trwałemu zniszczeniu poprzez specjalistyczne firmy zajmujące się niszczeniem dokumentacji.

§4. Nadawanie upoważnień do przetwarzania danych osobowych

1. Administrator danych osobowych nadaje imienne upoważnienia do przetwarzania danych osobowych wszystkim pracownikom oraz innym osobom pozostającym w zatrudnieniu, które przetwarzają dane osobowe.
2. W upoważnieniu określane są:
    1) data nadania upoważnienia,
    2) imię i nazwisko osoby przetwarzającej (upoważnionej),
    3) zajmowane stanowisko osoby upoważnionej (wykonywane czynności),
    4) zakres upoważnienia - kategorie osób, których dane będą przetwarzane, rodzaj przetwarzanych danych,
    5) okres trwania upoważnienia,
    6) zobowiązanie do zachowania w tajemnicy przetwarzanych danych osobowych, do których zostało nadane upoważnienie.
3. Upoważnienie wygasa:
    1) w momencie zakończenia stosunku pracy (lub umowy cywilnoprawnej),
    2) z okresem, na który zostało wydane,
    3) w chwili jego odwołania – z przyczyn wskazanych przez ADO (np. zmiana stanowiska pracy, naruszenie ochrony danych osobowych etc.).
4. Upoważnienia umieszczane są w aktach osobowych pracownika lub w przypadku osób zatrudnionych na podstawie umów cywilnoprawnych, w miejscu przechowywania umów.
5. ADO prowadzi rejestr nadanych upoważnień, w którym określa w sposób chronologiczny wykaz upoważnionych osób, datę nadania upoważnień, zakres upoważnienia oraz datę jego wygaśnięcia.

§5. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz programów informatycznych służących do przetwarzania danych

1. Dane osobowe przetwarzane są w siedzibie ANSG w Ostrowcu Św. przy ul. Akademickiej 12.
2. Przetwarzanie danych osobowych odbywa się przy wykorzystaniu systemu informatycznego. Dane zapisywane są również poza systemem informatycznym w formie dokumentacji papierowej.
3. W siedzibie ANSG dane osobowe przetwarzane są w następujących pomieszczeniach: Serwerownia blok B, kwestura blok C, dziekanat blok C, rektorat blok C, sekcja kadr blok C, biblioteka blok C, archiwum blok C, pomieszczenie techniczne blok A

4. Do pomieszczeń, o których mowa w ust. 3 mają dostęp jedynie upoważnieni pracownicy

ANSG. W przypadku pomieszczeń, w których charakter wykonywanych czynności powoduje czasową obecność osób nieupoważnionych, mogą one przebywać w tych pomieszczeniach wyłącznie w obecności osób upoważnionych - w czasie wymaganym na wykonanie niezbędnych czynności.
5. Pomieszczenia, w których przetwarzane są dane osobowe, muszą być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych osobowych, w taki sposób, aby uniemożliwić dostęp do nich osobom nieuprawnionym.

§6. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności przetwarzania danych osobowych

W ANSG rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   1) pomieszczenia zamykane na klucz,
   2) szafy metalowe i drewniane zamykane na klucz, metalowe kasetki,
   3) monitoring wizyjny,
   4) antywłamaniowy system alarmowy,
   5) rejestracja w formie papierowej wejść i wyjść personelu.
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:

1) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   2) przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.

3. Zabezpieczenia organizacyjne:
   1) Wszystkie osoby dopuszczone przez ADO do przetwarzania danych osobowych zapoznają się z polityką, instrukcjami i zasadami prawidłowego i zgodnego z prawem przetwarzania danych osobowych,
   2) wykaz pracowników ANSG uprawnionych do przetwarzania danych osobowych prowadzi ADO,
   3) przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez ADO,
   4) w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
   5) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone oraz, czy zabezpieczenia te nie były naruszone,
   6) w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu bądź zmiany przez osoby do tego celu nieupoważnione,
   7) po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

4. Środki techniczne i organizacyjne służące bezpieczeństwu danych w systemie informatycznym zostały szczegółowo opisane w „**Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”**.

§7. Naruszenie ochrony danych osobowych

1. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:
1) stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
3) zagubiono klucz do pomieszczeń, gdzie przetwarzane są dane osobowe,
4) zagubiono lub zniszczono dokumenty lub elektroniczny nośnik danych z zawartymi danymi osobowymi.
2. Każdy pracownik ANSG, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym lub przetwarzanych w inny sposób zobowiązany jest do niezwłocznego poinformowania o tym ADO lub ASI.
3. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.
4. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.
5. Administrator Danych Osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych zobowiązany jest w ciągu 72 godzin od uzyskania informacji o naruszeniu ochrony danych poinformować o incydencie organ nadzorczy oraz osobę, której dane zostały naruszone. Ponadto ADO zobowiązany jest do niezwłocznego:
    1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
    2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
    3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,
    4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych (fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej, wylogowania użytkownika podejrzanego o naruszenie ochrony danych, zmianę

hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu),
5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

6. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
7. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
8. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
9. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby upoważnionej do przetwarzania danych osobowych, należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz przepisów o ochronie danych osobowych.

§8. Postępowanie w stosunku do osób, których dane są przetwarzane

1. ANSG na swojej oficjalnej stronie internetowej zamieszcza informację o polityce bezpieczeństwa.
2. Pracownicy ANSG mają prawo przetwarzać dane osobowe wyłącznie wówczas, gdy jest to niezbędne do realizacji umowy zawartej ze studentem, usługi, zlecenia lub, jeśli Kontrahent wyrazi na to zgodę. Dane mogą być przetwarzane jedynie w celu, do którego zostały przeznaczone i w czasie niezbędnym do realizacji celu.
3. ADO ma obowiązek informowania osób fizycznych, których dane przetwarza o:
   1) celu przetwarzania,
   2) kategorii przetwarzanych danych,
   3) odbiorcach danych, jeżeli są one dalej przekazywane,
   4) planowanym terminie ich usunięcia, o ile jest on możliwy do określenia.
4. Każda osoba fizyczna, której dane przetwarza ANSGma prawo:

1) wglądu do swoich danych,
2) w przypadku, gdy są one nieprawidłowe, nieaktualne – do ich sprostowania,
3) usunięcia danych („prawo do bycia zapomnianym”), jeżeli ADO nie ma już celu ich przetwarzania, przetwarza je niezgodnie z prawem albo osoba cofnęła wcześniej wyrażoną zgodę,

4) żądać ograniczenia przetwarzania w przypadku kwestionowania poprawności danych, wniesienia sprzeciwu, braku celu ADO do przetwarzania danych lub ich przetwarzania sprzecznego z prawem,
5) wniesienia sprzeciwu do przetwarzania danych, jeżeli istnieją okoliczności i fakty, niemające prawnie usprawiedliwionych podstaw do przetwarzania.

Dochodzenie swoich praw osoba fizyczna, której dane przetwarza Uczelnia, może realizować osobiście w siedzibie ANSG lub zwrócić się na piśmie pod adres uczelni. ANSG zobowiązana jest udzielić odpowiedzi osobie zainteresowanej bez zbędnej zwłoki, najpóźniej w ciągu 30 dni.

§9. Powierzenie przetwarzania danych innemu podmiotowi, rejestrowanie czynności przetwarzania oraz ocena skutków dla ochrony danych

1. ANSG może w drodze umowy zawartej na piśmie - powierzyć innemu podmiotowi przetwarzanie danych w zakresie niezbędnym do wykonywania zadań wynikających ze Statutu ANSG. Zawierana jest wówczas umowa na powierzenie danych osobowych do przetwarzania.

1a. Umowa o której mowa w pkt.1 , jest rejestrowana i nadaje się jej numer wynikający z rejestru o którym mowa niżej w pkt. 1b.

1b. Rejestr umów powierzenia danych osobowych" (pracowników, studentów i słuchaczy ANSG), o których mowa w pkt.1, jest prowadzony przez Rektorat Uczelni.

2. ANSG może zostać podmiotem przetwarzającym dane, jeżeli podpisze umowę powierzenia danych z innym administratorem danych

3. ANSG rejestruje czynności przetwarzania. Rejestr stanowi odrębny dokument, który zawiera:

1) czynności przetwarzania,
2) opis kategorii osób, których dane są przetwarzane,
3) komórkę, dział lub stanowisko dokonujące czynności przetwarzania,
4) podstawę prawną upoważniającą do przetwarzania,
5) cel przetwarzania,
6) kategorie danych osobowych,
7) sposób zbierania danych do zbioru,
8) sposób udostępniania danych ze zbioru i kategorie odbiorców, którym dane są udostępniane,
9) opis technicznych i organizacyjnych środków bezpieczeństwa,
10) planowy termin usunięcia danych, o ile jest on możliwy do wskazania.

4. ANSG dokonuje oceny skutków dla ochrony danych. Dokument ten wskazuje zbiory danych, ocenę ryzyka naruszenia danych oraz stosowane środki zapobiegawcze w celu zminimalizowania i wyeliminowania ryzyka.

§10. Audyt i szkolenia

1. Inspektora ochrony danych ANSG lub wyznaczony przez ADO pracownik posiadający wiedzę na temat prawa i praktyk w zakresie ochrony danych osobowych przeprowadza szkolenia dla nowo przyjętych pracowników. ADO może również zlecić przeszkolenie pracownika zewnętrznej osobie/podmiotowi specjalizującej(-mu) się w zakresie ochrony danych osobowych.
2. Szkolenia przeprowadzane są każdorazowo w razie konieczności (zmiana przepisów z zakresu ochrony danych, zmiana Polityki, zmiana zasad przy przetwarzaniu danych osobowych).
3. Co najmniej raz do roku, ADO lub wyznaczony przez niego pracownik, przeprowadza audyt ochrony danych osobowych, mający na celu wykrycie nieprawidłowości w bezpieczeństwie informacji oraz sprawdzenie przestrzegania Polityki ochrony danych osobowych przez pracowników. W przypadku wystąpienia częstego naruszania bezpieczeństwa, audyty powinny być przeprowadzane częściej.
4. Audyt kończy się sprawozdaniem z przeprowadzonych czynności.

Wykaz załączników

Załącznik nr 1. Upoważnienie do przetwarzania danych osobowych
Załącznik nr 2. Rejestr upoważnień do przetwarzania danych osobowych
Załącznik nr 3. Wzór umowy powierzenia danych do przetwarzania
Załącznik nr 4. Wzór rejestru czynności przetwarzania
Załącznik nr 5. Raport z naruszenia danych osobowych
Załącznik nr 6. Wniosek o dostęp do danych
Załącznik nr 7. Oświadczenie pracownika o zapoznaniu się z postanowieniami Polityki ochrony danych.
Załącznik nr 8 Klauzula informacyjna o przetwarzaniu danych osobowych w ANSG.

……..

data i podpis Administratora Danych