REGULAMIN ZASAD OCHRONY DANYCH OSOBOWYCH I WIZERUNKU W ZAKRESIE NIEPEŁNOSPRAWNOŚCI

Regulamin powstał w ramach projektu pn. „Kompleksowy program wsparcia osób z niepełnosprawnościami w Wyższej Szkole Gospodarki w Bydgoszczy” (nr POWR.03.05.00-00-A079/19), dofinansowanego ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój na lata 2014-2020

2022

W Wyższej Szkole Gospodarki w Bydgoszczy (zwana w dalszej części dokumentu również jako WSG lub Uczelnia) osoby z niepełnosprawnościami są równoprawnymi członkami społeczności akademickiej, którzy funkcjonują we wszystkich obszarach prowadzonej przez Uczelnię działalności.

Osoby z niepełnosprawnościami nie stanowią odrębnej grupy, a jedynie część społeczności, która jest równouprawniona w dziedzinie edukacji, pracy i życia WSG a zapisy niniejszego regulaminu dotyczą wszystkich członków Uczelni.

Niniejszy Regulamin stanowi zbiór zasad postępowania w związku z ochroną i przetwarzaniem zarówno danych osobowych, jak i wizerunku w Wyższej Szkole Gospodarki w Bydgoszczy w szczególności z uwzględnieniem danych w zakresie niepełnosprawności. Orzeczenia o niepełnosprawności zawierają dane osobowe szczególnej kategorii, dlatego w celu ich ochrony WSG dokłada wszelkiej staranności.

Wprowadzenie Regulaminu zasad ochrony danych osobowych i wizerunku w zakresie niepełnosprawności w Wyższej Szkole Gospodarki w Bydgoszczy (zwanego dalej „regulaminem") ma na celu m.in.:

1) wsparcie w stosowaniu przepisów RODO w realizacji funkcjonowania procesów;
2) uwzględnienie specyfiki działania WSG i potrzeb społeczności akademickiej;
3) doprecyzowanie obowiązków uczelni do realizacji praw osób fizycznych;

Integralną część przedmiotowego regulaminu stanowią jego załączniki, które zawierają informacje, wnioski i dokumentację niezbędną do prawidłowego przetwarzania danych osobowych.

W celu wsparcia osób z niepełnosprawnościami studiującymi w WSG, na wniosek i za zgodą zainteresowanych Uczelnia może przetwarzać dane szczególne, w tym dane dotyczące stanu zdrowia.

Postanowienia regulaminu dotyczą wszystkich członków społeczności Wyższej Szkoły Gospodarki w Bydgoszczy.

Należy pamiętać, o konieczności konsultowania wszelkich zapisów odnoszących się do osób z niepełnosprawnościami w dokumentach normatywnych, strategiach oraz treściach marketingowych i promocyjnych przez Pełnomocnika Rektora i Kanclerza ds. Osób z Niepełnosprawnościami.

PODSTAWOWE POJĘCIA

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

Administratorem Danych przetwarzanych na WSG, jest Wyższa Szkoła Gospodarki w Bydgoszczy z siedzibą przy ul. Garbary 2, 85-229 Bydgoszcz, reprezentowana przez organ wykonawczy tj. Prezydenta WSG.

Administrator Systemu Informatycznego to osoba odpowiedzialna za funkcjonowanie systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień. Administrator Systemu Informatycznego jest odpowiedzialny za przestrzeganie zasad i wymagań bezpieczeństwa danych w systemie informatycznym.

Biuro ds. Osób z Niepełnosprawnościami - zgodnie z zapisem Ustawy Prawo o Szkolnictwie Wyższym stwarzanie osobom z niepełnosprawnościami warunków do pełnego udziału w procesie kształcenia i badaniach naukowych to jedno z podstawowych zadań uczelni wyższych. Jednostką odpowiedzialną za realizacje tych zadań w WSG jest Biuro ds. Osób z Niepełnosprawnościami (BON)

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, wizerunkową, zdrowotną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane osobowe dzielą się na trzy kategorie:

1) dane tzw. zwykłe, takie jak imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek, adres e-mail itp.,

2) szczególne kategorie danych osobowych (uprzednio zwane danymi wrażliwymi), wymienione

w art. 9 RODO ujawniające:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,

- dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia, niepełnosprawności, seksualności lub orientacji seksualnej tej osoby,
3) dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa wymienione w art. 10 rozporządzenia (uprzednio również zaliczane do danych wrażliwych).

RODO to skrót od: 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 do uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). RODO stanowi główny element europejskiej reformy ochrony danych osobowych. RODO powstało w związku z koniecznością ujednolicenia przepisów regulujących ochronę danych osobowych w państwach UE. Na pakiet reformujący ochronę danych osobowych w Unii Europejskiej składa się także Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW – tzw. dyrektywa policyjna. RODO stosuje się do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz w przypadku przetwarzania w sposób inny niż zautomatyzowany, np. w formie tradycyjnej - papierowej, jeżeli dane stanowią lub mogą stanowić część zbioru. Przykładami takich zbiorów danych w uczelni są: dzienniki zajęć, listy obecności, listy zatrudnionych pracowników, arkusze ocen, księgi arkuszy ocen, które są prowadzone zarówno w systemie informatycznym, jak i przetwarzane tradycyjnie.

Niepełnosprawność, wg Światowej Organizacji Zdrowia, ograniczenie lub brak zdolności do wykonywania czynności w sposób lub w zakresie uważanym za normalny dla człowieka, wynikające z wrodzonego lub nabytego upośledzenia funkcji organizmu. Ustawa z 27 sierpnia 1997 o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych: niepełnosprawność oznacza trwałą lub okresową niezdolność do wypełniania ról społecznych z powodu stałego lub długotrwałego naruszenia sprawności organizmu, w szczególności powodującą niezdolność do pracy.

Orzeczenia o niepełnosprawności

Można się spotkać z kilkoma rodzajami dokumentów potwierdzających niepełnosprawność, mogą to być:

1) orzeczenia powiatowego/ wojewódzkiego zespołu do spraw orzekania o stopniu niepełnosprawności;
2) orzeczenia wydawane przez lekarza orzecznika Zakładu Ubezpieczeń Społecznych
3) orzeczenia wydawane przez komisje do spraw inwalidztwa i zatrudnienia (sprzed 1998 roku)

Stopnie niepełnosprawności. Ustala się trzy stopnie niepełnosprawności:

1) znaczny
2) umiarkowany
3) lekki

Stopień niepełnosprawności osoby zainteresowanej orzeka się na czas określony lub na stałe. Decyduje ocena możliwości poprawy funkcjonowania osoby zainteresowanej. Orzeczenie o stopniu niepełnosprawności wydaje się osobie, która ukończyła 16 rok życia.

Przetwarzanie danych osobowych oznacza szereg różnych operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub ręczny. Przetwarzanie obejmuje takie działania jak zbieranie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie danych osobowych.

Przetwarzanie danych szczególnych wiąże się z koniecznością wypełnienia dodatkowych gwarancji ich ochrony ujętych w art. 9 ust. 2 i art. 10 RODO.

Przetwarzanie szczególnych kategorii danych osobowych jest zabronione, chyba, że m.in.:

1) Osoba, której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych,
2) Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw administratora danych osobowych wynikających z przepisów prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
3) Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości,
4) Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.
5) Orzeczenia o niepełnosprawności zawierają dane osobowe szczególnej kategorii. Zgodnie z prawem, osobom z niepełnosprawnością przysługują określone uprawnienia, wskazane przede wszystkim w ustawie o rehabilitacji zawodowej i społecznej, zatrudnianiu osób

niepełnosprawnych oraz wewnątrzuczelnianych postanowieniach dotyczących wsparcia procesów edukacyjnych ww.

6) Przedstawienie WSG dokumentów potwierdzających dane osobowe dotyczące stanu zdrowia jest dobrowolne (Podstawa: Art. 2 b ust. 2 Ustawa o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych) i winno wynikać z inicjatywy zainteresowanego, należy jednak pamiętać, że podanie tych danych jest konieczne do przyznania osobie z niepełnosprawnością ulg i świadczeń przysługujących jej z tego tytułu.

Inspektor Ochrony Danych to wyznaczona przez Prezydenta Wyższej Szkoły Gospodarki w Bydgoszczy osoba, która została wpisana do prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych rejestru inspektorów ochrony danych osobowych, odpowiedzialna za nadzór i bezpieczeństwo danych osobowych przetwarzanych w Wyższej Szkole Gospodarki w Bydgoszczy. Inspektor Ochrony Danych odpowiada za nadzór nad funkcjonowaniem i efektywnością procesów prawidłowego przetwarzania danych osobowych.

WIZERUNEK

Wizerunek w polskim systemie prawnym prezentowany jest jako z dóbr osobistych, które wymieniono w art. 23 Kodeksu cywilnego. Stanowi on, że „Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach".

Drugim ważnym aktem prawnym odnoszącym się do prawa do wizerunku jest ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych. W art. 81 tej ustawy przyjęto, że dla zgodnego z prawem rozpowszechniania wizerunku, potrzebne jest zezwolenie osoby na nim przedstawionej, chyba że otrzymała ona zgodnie z umową zapłatę za pozowanie. Wymóg uzyskania zgody jest najprostszą, ale także skuteczną formą ochrony wizerunku. Przewidziano jednak ograniczenia tej ochrony, w wyniku których nie jest konieczne uzyskanie zgody na rozpowszechnianie w dwóch przypadkach, tj., gdy:

- publikowany jest wizerunek osoby powszechnie znanej, wykonany w związku z pełnieniem przez nią funkcji publicznych, np. społecznych, politycznych, zawodowych (przy czym osoba powszechnie znana to osoba należąca do grona osób, które godzą się na upublicznianie informacji dotyczących ich życia, np. polityków, aktorów, muzyków
- publikowany wizerunek jest tylko szczegółem całości takiej jak zgromadzenie, krajobraz, impreza publiczna11. W tym miejscu należy zaznaczyć, że ochrona wizerunku jaką przyznaje mu ustawa o prawie autorskim jest węższa niż ta przyznana przez Kodeks cywilny12. Gdyż Kodeks umożliwia ochronę przed zagrożeniami takimi jak np. utrwalenie, publikacja, rozpowszechnienie bądź inny rodzaj eksploatacji, natomiast ustawa o prawie autorskim obejmuje ochronę przed rozpowszechnianiem. Wizerunek może być także traktowany jako dane osobowe, gdyż pozwala na identyfikację danej osoby, a zgodnie z ustawą o ochronie danych osobowych „za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej".

O ważności wizerunku, traktowanego jako dane osobowe świadczy poruszanie tego zagadnienia w sprawozdaniach z działalności Generalnego Inspektora Ochrony Danych Osobowych. Prowadzone przez niego sprawy w zakresie wizerunku dotyczą głównie nieuprawnionego utrwalania i publikowania wizerunków osób z wykorzystaniem monitoringu wizyjnego. GIODO w kampaniach informacyjnych często zwraca uwagę na niezgodną z prawem publikację wizerunku innych osób szczególnie za pośrednictwem Internetu, gdyż liczbę takich incydentów należy minimalizować.

PODSTAWOWE ZASADY POSTĘPOWANIA W ZAKRESIE ZABEZPIECZENIA DANYCH OSOBOWYCH

1) **zasada legalności** – przetwarzanie danych osobowych musi odbywać się zgodnie z prawem tj. musi istnieć podstawa prawna przetwarzania.

2) **zasada celowości** – cel przetwarzania danych musi z góry być określony i informacja ta musi zostać przekazana osobie, której dane dotyczą.

3) **zasada merytorycznej poprawności** – dane osobowe muszą być prawdziwe, kompletne i aktualne ze względu na cel jakiemu mają służyć. Nie powinno się zbierać danych osobowych ze źródeł nieznanego pochodzenia.

4) **zasada adekwatności** – można przetwarzać tylko de dane osobowe, które są niezbędna do celu jaki administrator danych chce osiągnąć.

5) **zasada ograniczenia czasowego** – dane osobowe nie mogą być przetwarzane dłużej niż jest to konieczne do osiągnięcia celu, w którym zostały zebrane.

6) **polityka czystego biurka** – należy pamiętać o konieczności usuwania wszelkich nośników danych osobowych poza zasięg wzroku i zasięg dłoni osób postronnych i ich przechowywania pod kluczem.

7) **polityka czystego druku** – należy pamiętać o konieczności odbierania wszelkich wydruków z urządzeń drukujących niezwłocznie po ich wydrukowaniu.

8) **polityka czystego ekranu** – należy pamiętać o konieczności blokowania komputerów nawet przed krótkotrwałym opuszczeniem stanowiska pracy (WIN+L). Dodatkowo należy uniemożliwiać wgląd w treści wyświetlane na monitorach osobom nieupoważnionym – odpowiednia ustawienie ekranu.

9) **procedura niszczenia** – należy pamiętać o konieczności niszczenia dokumentów zawierających dane osobowe z wykorzystaniem niszczarek lub pojemników do utylizacji dokumentacji poufnej, gdy już staną się nie potrzebne.

10) **polityka haseł** – należy pamiętać o konieczności zmiany hasła w cyklach nie rzadszych niż 90 dni oraz o zakazie współdzielenie dostępów do systemów informatycznych z wykorzystaniem jednego identyfikatora/loginu.

11) **procedura korzystania z urządzeń mobilnych** – należy pamiętać o konieczności zabezpieczania sprzętu informatycznego (laptopy, smartfony, tablety, pendrive) w trakcie ich wynoszenia poza obszar pracy (obszar przetwarzania danych) – hasło , PIN, technologia biometryczna)

12) **procedura korzystania z internetu** – należy pamiętać o zakazie stosowania zapamiętywania haseł w przeglądarkach internetowych oraz historii wyszukiwania – okresowo należy czyścic historię przeglądania lub wyłączyć jej zapamiętywanie.

13) **procedura korzystania z poczty elektronicznej** – należy pamiętać o weryfikacji w procesie wysyłania tak aby adresacja była prawidłowa – w szczególności należy weryfikować opcje kopia ukryta/kopia jawna. Dodatkowo nie wolno korzystać z odnośników znajdujących się w mailach nieznanego pochodzenia.

PODMIOTY, KTÓRYCH DANE PRZETWARZANE SĄ W UCZELNI

Administrator przetwarza następujące dane osobowe osób fizycznych:

1) studentów, kandydatów na studia, studia podyplomowe (szanując niezależność osób z niepełnosprawnością oraz ich prawa, pomoc Biura ds. Osób z Niepełnosprawnościami udzielana jest wyłącznie tym osobom, które same zwrócą się z wnioskiem o wsparcie do Biura i udokumentują swoją niepełnosprawność).
2) słuchaczy studiów podyplomowych
3) uczestników kursów, szkoleń, konferencji
4) absolwentów
5) pracowników, rodzin pracowników, w tym kandydatów do pracy oraz byłych pracowników
6) osób świadczących pracę w innej formie niż stosunek pracy
7) czytelników biblioteki
8) kontrahentów
9) osób zaproszonych do udziału w eventach promocyjnych.

ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

WSG przetwarza dane między innymi w zakresie:

1) imion i nazwisk,
2) dat urodzenia,
3) numeru PESEL,
4) numeru indeksu,
5) serii i numeru dokumentu potwierdzającego tożsamość,
6) adresu e-mail,
7) numeru telefonu,
8) wizerunku,
9) obywatelstwa.

W zakresie danych osobowych przetwarzanych przez uczelnię występują także szczególne kategorie danych dotyczące stanu zdrowia, stopnia niepełnosprawności,

MIEJSCA PRZETWARZANIA DANYCH OSOBOWYCH

W WSG dane osobowe przetwarzane są w:

1) systemach informatycznych,
2) pakietach biurowych,
3) systemach pocztowych,
4) zbiorach tradycyjnych (papierowych) np.: akta pracownicze, korespondencja papierowa itp.

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

W Wyższej Szkole Gospodarki w Bydgoszczy do przetwarzania danych osobowych, zostają dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania tego rodzaju danych.

Upoważnienie służy realizacji obowiązku rozliczalności wynikającego z RODO, tzn. uczelnia musi wykazać, iż do przetwarzania danych osobowych zostały dopuszczone tylko osoby uprawnione. Upoważnienie jest także dokumentem, który ogranicza dostęp do zasobów danych przez osoby nieuprawnione. Upoważnienia do przetwarzania danych osobowych zostają wydane osobom, które przetwarzają dane zwykłe oraz szczególne tj. związane ze stanem zdrowia oraz informacjami dotyczącymi niepełnosprawności tj.:

1) kandydatów na studia i słuchaczy studiów podyplomowych
2) studentów i absolwentów
3) pracowników.

Obowiązek posiadania upoważnienia dotyczy także sytuacji, w której dane przetwarzane są w wersji papierowej.

REJESTR CZYNNOŚCI PRZETWARZANIA

Uczelnia prowadzi rejestr czynności przetwarzania dokument, który obrazuje, w jakich procesach Wyższa Szkoła Gospodarki w Bydgoszczy przetwarza dane osobowe.

Rejestr uwzględnienia m.in. cel przetwarzania danych, podstawy przetwarzania danych, kategorię oraz zakres przetwarzanych danych oraz w jaki sposób dane są zabezpieczone. Rejestr czynności przetwarzania prowadzony jest w formie elektronicznej.

PODSTAWY PRAWNE ORAZ CELE PRZETWARZANIA DANYCH OSOBOWYCH

Podstawę przetwarzania danych osobowych przez Uczelnię stanowią:

1) Realizacja obowiązku prawnego do którego zobowiązany jest Administrator (art. 6 ust. 1 pkt. C; art. 9 ust.2 pkt b RODO),
2) Wykonanie umowy, której stroną jest osoba, której dane dotyczą, lub podjęcie działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art.6 ust. 1 pkt b RODO),
3) Realizacja celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora (art. 6 ust 1 pkt f RODO),
4) Zgoda osoby, której dane dotyczą (art. 6 ust. 1 pkt a/art.9 ust.2 pkt a RODO).
5) Przetwarzanie danych osobowych kandydatów na studentów / słuchaczy studiów lub studiów podyplomowych jest niezbędne w celu rejestracji na studia / studia podyplomowe. Przetwarzanie danych ma związek z realizacją obowiązku prawnego ciążącego na Administratorze i jest niezbędne do zawarcia umowy.
6) Przetwarzanie danych osobowych studentów jest niezbędne w celu realizacji obowiązku prawnego ciążącego na Administratorze (realizacja procesu kształcenia), jak również prawnie uzasadnionych interesów Administratora, a związanych z prowadzeniem ewaluacji jakości kształcenia, wsparciu kształcenia osób z niepełnosprawnościami, marketingiem. Dane osobowe, w tym szczególne kategorie danych osobowych takie np. dotyczące zdrowia mogą być także przetwarzane w celu realizacji procesu wsparcia osoby z niepełnosprawnościami.
7) Przetwarzanie danych osobowych członków rodzin studentów może by niezbędne w celu realizacji obowiązku prawnego ciążącego na Administratorze związanego z realizacją procesu przyznawania pomocy materialnej.
8) Przetwarzanie danych osobowych uczestników kursów/szkoleń/konferencji jest niezbędne w celu realizacji usługi edukacyjnej / naukowej, a także w celu wykonania prawnie uzasadnionych interesów Administratora związanych z ewaluacją i marketingiem bezpośrednim.
9) Przetwarzanie danych osobowych jest niezbędne do wypełnienia obowiązku prawnego związanego z archiwizacją, a także w celu wykonania prawnie uzasadnionych interesów Administratora związanych z badaniem losów absolwentów, marketingiem bezpośrednim.
10) Przetwarzanie danych osobowych kandydatów do prac jest niezbędne do przeprowadzenia procesu rekrutacyjnego, a następnie realizacji obowiązku prawnego związanego z zatrudnianiem.

11) Przetwarzanie danych osobowych pracowników jest niezbędne do realizacji obowiązku prawnego związanego z zatrudnieniem oraz z uwagi na uzasadniony interes prawny Administratora np. prezentacja wizerunku pracowników pełniących funkcje reprezentacyjne.
12) Przetwarzanie danych osobowych członków rodzin pracowników, może by niezbędne do realizacji obowiązku prawnego np. związanego z ubezpieczeniem czy przyznawaniem świadczeń socjalnych.
13) Przetwarzanie danych osobowych osób świadczących pracę w innej formie niż stosunek pracy jest niezbędne do realizacji współpracy i ma związek z realizacją obowiązku prawnego.
14) Przetwarzanie danych osobowych kontrahentów jest niezbędne do realizacji umowy.
15) Przetwarzanie danych osobowych czytelników biblioteki jest niezbędne w celu udostępniania zbiorów bibliotecznych.
16) Przetwarzanie danych osobowych osób zaproszonych do udziału w eventach jest niezbędne do realizacji marketingu bezpośredniego.

AKTY PRAWNE, W OPARCIU O KTÓRE WSG PRZETWARZA DANE OSOBOWE

1) 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 osobowych)
2) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019.1781 t.j. z dnia 2019.09.19)
3) Ustawa z dnia 20 lipca 2018r. Prawo o szkolnictwie wyższym i nauce. Dz.U.2022.574 t.j. z dnia 2022.03.11)
4) Ustawa z dnia 26 czerwca 1974r. Kodeks pracy Dz.U.2022.1510 t.j. z dnia 2022.07.19, ze szczególnym uwzględnieniem art. 21 ind. 1-5
5) Ustawa z dnia 27 sierpnia 1997r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz.U.2021.573 t.j. z dnia 2021.03.29) ze szczególnym uwzględnieniem art. 2b
6) Ustawa z dnia 14 lipca 1993r. o narodowym zasobie archiwalnym i archiwach (Dz.U.2020.164 t.j. z dnia 2020.02.03
7) Postanowienia wewnątrzuczelniane.

OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

1) Dane osobowe kandydatów na studia są przechowywane przez okres prowadzenia rekrutacji, a następnie podlegają archiwizacji przez okres 6 miesięcy.
2) Dane osobowe studentów, w tym studentów z niepełnosprawnościami, członków rodzin studentów są przetwarzane przez okres niezbędny do załatwienia sprawy, realizacji świadczenia pomocy materialnej lub wsparcia oferowanego przez Biuro ds. Osób z Niepełnosprawnościami.
3) Dane osobowe absolwentów studiów wyższych są archiwizowane przez okres 50 lat.
4) Dane osobowe absolwentów studiów podyplomowych są archiwizowane przez okres 10 lat.
5) Dane osobowe kandydatów do pracy są przetwarzane przez okres rekrutacji, a następnie podlegają archiwizacji przez okres 3 miesięcy, chyba, że kandydat na pracownika wyraził zgodę na przetwarzanie danych osobowych na potrzeby przyszłych rekrutacji w maksymalnym okres w maksymalnym okresie do 3 lat.
6) Dane pracowników są przetwarzane przez okres zatrudnienia, a następnie podlegają archiwizacji przez okres wynikający z obowiązujących przepisów prawa pracy (50 lat lub 10 lat).
7) Dane osobowe studentów, członków rodzin są przetwarzane przez okres niezbędny do załatwienia sprawy, realizacji świadczenia socjalnego, wsparcia osób z niepełnosprawnościami. Dane osobowe osób świadczących pracę w innej formie niż stosunek pracy są przetwarzane przez okres niezbędny do realizacji współpracy, a następnie podlegają archiwizacji przez okres 10 lat.
8) Dane osobowe kontrahentów są przetwarzane przez okres współpracy z Administratorem, a następnie podlegają archiwizacji przez okres 10 lat.
9) Dane osobowe czytelników są przechowywane przez okres realizacji usługi udostępniania zbiorów bibliotecznych.
10) Dane osobowe osób zaproszonych do udziału w eventach promocyjnych są przetwarzane przez okres 15 lat.

WYPEŁNIANIE OBOWIĄZKU INFORMACYJNEGO

Obowiązek informacyjny należy spełnić podczas pozyskiwania danych od osoby, której dane dotyczą, np.: w procesie rekrutacji na studia/do pracy, zapisu uczestników na organizowane wydarzenie, w procesie dotyczącym prowadzenia badań naukowych. Najbezpieczniejszym rozwiązaniem jest umieszczanie klauzul informacyjnych tam, gdzie przetwarzamy dane osobowe.

ZASADY POZYSKIWANIA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

1) zgoda na przetwarzanie danych osobowych może przyjąć formę oświadczenia woli, wyrażonego w formie pisemnej lub elektronicznej, np. klauzula zgody dołączona do kwestionariusza osobowego w formie papierowej lub umieszczenie klauzuli zgody w formularzu elektronicznym.
2) zgoda na przetwarzanie danych osobowych musi być wyrażona na jasno określony cel np. zgoda na przetwarzanie danych osobowych w procesie rekrutacji do pracy czy udziału w konkursie, konferencji itp.
3) w WSG na podstawie zgody przetwarzane są m.in. dane następujących kategorii osób:
   - kandydatów do pracy,
   - absolwentów,
   - uczestników badań/projektów,
   - uczestników konferencji/szkoleń/seminariów.
4) jeżeli dane osobowe przetwarzane są na podstawie zgody, osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody ma być równie proste do realizacji jak jej wyrażenie.

ZASADY POSTĘPOWANIA W PRZYPADKU PODEJRZENIA LUB STWIERDZENIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

W przypadku podejrzenia/stwierdzenia naruszenia ochrony danych osobowych należy zaprzestać przetwarzania danych osobowych, poinformować o incydencie / podejrzeniu incydentu przełożonego oraz Inspektora Ochrony Danych Osobowych.

W zgłoszeniu podejrzenia/stwierdzenia naruszenia należy wskazać datę, okoliczności, możliwą przyczynę, skutki oraz dotychczasowe zabezpieczenia. opisać znane danej osobie sposoby zabezpieczenia danych osobowych.

ZABEZPIECZENIE DANYCH OSOBOWYCH

W WSG stosuje się m.in.:

Zabezpieczenia organizacyjne:

1) wyznaczenie Inspektora Ochrony Danych,
2) opracowanie i polityki bezpieczeństwa ochrony danych osobowych,
3) do przetwarzania danych osobowych dopuszczone zostają wyłącznie osoby do tego upoważnione,

4) prowadzenie ewidencji osób upoważnionych,
5) przeszkolenie i zaznajomienie pracowników z przepisami ochrony danych osobowych,
6) procedura wydawania kluczy do pomieszczeń osobom uprawnionym,
7) nadzór obszarów przez służbę ochrony,
8) monitoring osób wchodzących i wychodzących z budynków,
9) osoby trzecie w obszarze przetwarzania danych osobowych przebywają w obecności osób upoważnionych,
10) osoby upoważnione zobowiązane są do zachowania danych osobowych i sposobów zabezpieczeń w tajemnicy.

Zabezpieczenia fizyczne:

1) drzwi zamykane na klucz,
2) szafy niemetalowe/metalowe zamykane na klucz,
3) niszczarki dokumentów,
4) systemy alarmowe,
5) systemy monitoringu wizyjnego,
6) identyfikatory użytkowników oraz hasła.

INSTRUKCJA POSTĘPOWANIA PRACOWNIKA W PRZYPADKU CZASOWEGO OPUSZCZENA STANOWISKA PRACY

1) w przypadku zaistnienia potrzeby opuszczenia obszaru przetwarzania danych osobowych, gdy pozostaje on bez nadzoru osób upoważnionych, należy zamknąć pomieszczenie na klucz. Klucze do pomieszczeń powinny pozostawać pod nadzorem osób upoważnionych.
2) czasowo opuszczając stanowisko pracy należy wylogować się z systemu lub uruchomić wygaszacz ekranu chroniony hasłem. Nie należy pozostawiać dokumentów zawierających dane osobowe w miejscu widocznym.
3) po zakończonej pracy należy wylogować się ze wszystkich systemów, z których korzystaliśmy podczas pracy, zamknąć w szafach dokumenty zawierające dane osobowe lub inne tajemnice ustawowo chronione.

ZASADY POSTĘPOWANIA Z DOKUMENTAMI PAPIEROWYMI ZAWIERAJĄCYMI DANE OSOBOWE

1) dokumenty i wydruki w pomieszczeniach nieupoważnionych zawierające dane osobowe należy przechowywać zabezpieczonych fizycznie przed dostępem osób trzecich,

2) użytkownicy są zobowiązani do stosowania „polityki czystego biurka”, polega ona na zabezpieczeniu dokumentów zawierających dane osobowe w szafach, biurkach, pomieszczeniach zamykanych na klucz, ograniczając wgląd przez osoby nieupoważnione,
3) dokumenty należy przenosić w sposób zapobiegający ich kradzieży, zgubieniu lub utracie,
4) zalecane jest niszczenie dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

ZASADY POSTĘPOWANIA Z ELEKTRONICZNYMI NOŚNIKAMI DANYCH OSOBOWYCH

1) dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika danych podlega skasowaniu,
2) dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po upływie tego celu dane podlegają archiwizacji, skasowaniu lub anonimizacji,
3) przenośne elektroniczne nośniki danych są przechowywane przez użytkowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych,
4) w przypadku konieczności wyniesienia nośników danych poza jednostkę organizacyjną, użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia nośnika, konieczne jest użycie środków ochrony kryptograficznej (szyfrowanie danych),
5) w przypadku wykorzystywania elektronicznych urządzeń mobilnych (m.in. smartphone, tablet) wymaga się zastosowania następujących środków bezpieczeństwa: blokada ekranu (pin/hasło/symbol graficzny), szyfrowanie pamięci/karty pamięci, program antywirusowy, wyłączenie nieużywanych usług (np.wi-fi, bluetooth, nfc), instalowanie oprogramowania z zaufanych źródeł, używanie szyfrowania lub VPN podczas korzystania z publicznych hotspot-ów,
6) w przypadku korzystania z komputerów przenośnych poza obszarem przetwarzania danych jednostki organizacyjnej, należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby nieuprawnione i stosować środki ochrony kryptograficznej,
7) za bezpieczeństwo komputerów przenośnych, urządzeń mobilnych, nośników danych odpowiadają ich użytkownicy. Zabrania się pozostawiania nośników danych bez nadzoru osoby upoważnionej.

PUBLIKACJA ZDJĘĆ

Publikacje wizerunku wymagające zgody. Publikacja zdjęcia osoby, np. na stronie internetowej uczelni, zgodnie z ustawą o ochronie danych osobowych, ustawą o prawie autorskim wymaga zgody art. 81 ust.1 i art.23 kodeksu cywilnego wymaga zgody osoby na nim przedstawionej. Publikacja zdjęć osoby umożliwia identyfikację wizerunku, co mogłoby narazić osoby niepełnosprawne na różnego rodzaju niedogodności i niebezpieczeństwa, dlatego niezbędne jest umożliwienie studentom i pracownikom wyrażenia decyzji w tym zakresie. Wyrażenie zgody na publikację wizerunku pracownika lub studenta, powinno być zrozumiałe dla odbiorcy, precyzyjnie określone w postaci celu i zakresu udostępnienia.

Publikacje wizerunku niewymagające zgody. Zezwolenia nie wymaga rozpowszechnianie wizerunku:

- osoby powszechnie znanej, jeżeli wizerunek upubliczniono w związku z pełnieniem przez nią funkcji publicznych, społecznych, zawodowych, politycznych,
- osoby stanowią jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Co oznacza, że dozwolone jest upublicznianie zdjęć z wydarzeń WSG na których sylwetka osoby stanowi jedynie szczegół całości prezentowanej na zdjęciu.

Podczas organizowanych wydarzeń typu konferencje, targi itp. nie ma konieczności uzyskania zgody na fotografowanie / filmowanie uczestników, ale warto poinformować gości, że event będzie rejestrowany i może zostać upubliczniony przez WSG.

POSTĘPY W NAUCE

Publikacja ocen studentów (np. z egzaminów, kolokwiów i prac dyplomowych)

Dozwolone jest publikowanie wyników w nauce z użyciem pojedynczego identyfikatora np. nr albumu.

Niedozwolone jest

- publikowanie na ogólnodostępnej stronie internetowej i wywieszanie list w gablotach dot. postępów w nauce np. wyników egzaminów ze wskazaniem imion i nazwisk studentów;
- przekazywanie ocen studentów osobom trzecim np. staroście roku.

Informacja o przebiegu nauki studenta i zakończenia studiów udzielana jest wyłącznie osobie, której dane dotyczą (studenta / absolwenta). WSG zachowuje prawo do weryfikacji tożsamości osoby, której dane dotyczą i która o takie dane występuje.

Publikacja danych studentów dozwolona jest:

- podczas uczelnianych uroczystości w zakresie wyczytywania imion oraz nazwisk studentów wyróżnionych za wybitne osiągnięcia i nie wymaga uprzedniej zgody,

- na stronie internetowej WSG lub w gablotach w zakresie imienia i nazwiska w celu ich wyróżnienia za szczególne osiągnięcia;
- wywieszanie pod pracami typu wizualnego tj. artystycznymi np. obrazami, grafikami itp. podpisów zawierających pełne imiona i nazwiska studentów, którzy je wykonali.

Na zajęciach prowadzonych ze studentami i słuchaczami dozwolone jest weryfikowanie ich obecności poprzez wyczytywanie imienia i nazwiska.

MONITORING WIZYJNY

1. przetwarzanie danych osobowych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na WSG, w tym w celu zapewnienia bezpieczeństwa osób i ochrony mienia. Podstawę prawną przetwarzania danych osobowych stanowi art. 6 ust. 1 lit. c RODO w związku z art. 222 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917 z późn. zm.).
2. monitoring obejmuje zewnętrzny oraz wewnętrzny teren obiektów.
3. dane mogą być przekazywane podmiotom przetwarzającym dane osobowe na zlecenie administratora danych, a także innym podmiotom uprawnionym na podstawie przepisów prawa.
4. nagrania obrazu będą przetwarzane wyłącznie do celów, dla których zostały zebrane i będą przechowywane przez okres nieprzekraczający 3 miesięcy od dnia nagrania.
5. osobie, której dane dotyczą przysługuje prawo:
- dostępu do danych osobowych,
- żądania ich sprostowania,
- ograniczenia przetwarzania, w przypadkach wymienionych w RODO,
- usunięcia danych, w przypadku, gdyby dane były przetwarzane niezgodnie z prawem.

6. w związku z tym, że przetwarzanie danych osobowych odbywa się na podstawie art. 6 ust. 1 lit. c RODO osobie, której dane dotyczą nie przysługuje prawo do przenoszenia danych ani prawo do złożenia sprzeciwu.
7. przetwarzanie danych osobowych utrwalonych na nagraniach obrazu jest dla WSG niezbędne do zapewnienia bezpieczeństwa studentów, pracowników, ochrony mienia.

SZKOLENIA

1) szkolenia z ochrony danych osobowych pracowników prowadzone są w formie stacjonarnej lub elektronicznej.
2) udział w szkoleniu e-learningowym jest równoważny ze szkoleniem stacjonarnym.

3) po ukończeniu szkolenia pracownik uzyskuje certyfikat, który zobowiązany jest przedstawić kierownikowi jednostki i działowi personalnemu Wyższej Szkoły Gospodarki w Bydgoszczy.

ZAŁĄCZNIKI:

zał. 1 Polityka ochrony danych osobowych w Wyższej Szkole Gospodarki w Bydgoszczy

zał. 2 Polityka prywatności WSG

zał. 3 Rejestr czynności przetwarzania

zał. 3a Ewidencja osób upoważnionych do przetwarzania danych osobowych – wzór w załączeniu

zał. 4 Zgoda na przetwarzanie danych osobowych szczególnej kategorii

zał. 5 klauzula informacyjna i zgoda dotycząca przetwarzania danych studentów WSG

zał. 6 klauzula informacyjna dotycząca przetwarzania danych kandydatów do pracy w WSG

zał. 7 zgoda na przetwarzanie danych dla kandydatów do pracy w WSG

zał. 8 klauzula informacyjna dotycząca przetwarzania danych kandydatów na słuchaczy studiów podyplomowych WSG

zał. 9 zgoda na przetwarzanie danych dla kandydatów na słuchaczy studiów podyplomowych, kursów oraz szkoleń WSG

zał. 10 upoważnienie do przetwarzania danych osobowych w celu spełnienia wymogów art. 29 (RODO)

zał. 11 klauzula informacyjna dotycząca monitoringu wizyjnego

zał. 12 wniosek o cofnięcie zgody na przetwarzanie danych osobowych

zał. 13 żądanie sprostowania danych osobowych

zał. 14 żądanie usunięcia danych osobowych

zał. 15 zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

zał.16 zgłoszenie w sprawie naruszenia ochrony danych osobowych

zał. 17 wykaz pomieszczeń w których przetwarzane są dane osobowe