POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Uniwersytet Ekonomiczny we Wrocławiu

I. PRZEDMIOT POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Niniejsza Polityka bezpieczeństwa danych osobowych stanowi politykę ochrony danych, realizującą wymogi art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: „Rozporządzenie").

Niniejsza Polityka bezpieczeństwa danych osobowych stanowi element obowiązującej na Uniwersytecie Ekonomicznym we Wrocławiu polityki bezpieczeństwa informacji regulowanej w szczególności Polityką Bezpieczeństwa Informacji, Zasadami Bezpieczeństwa Informacji oraz Zasadami Zarządzania Systemami Informatycznymi. Akty prawa wewnętrznego, o których mowa w zdaniu poprzedzającym należy odczytywać łącznie z niniejszą Polityką bezpieczeństwa danych osobowych, w szczególności w zakresie, w jakim opisują one wdrożone na Uniwersytecie Ekonomicznym środki techniczne i organizacyjne, aby przetwarzanie danych osobowych (zwanych dalej również „danymi") odbywało się zgodnie z Rozporządzeniem oraz w zakresie obowiązujących na Uczelni zasad korzystania z infrastruktury Administratora danych, w tym infrastruktury teleinformatycznej, w której dane osobowe są przetwarzane.

II. DEFINICJE

Użyte w dokumencie pojęcia oznaczają:

1. **Administrator danych, Administrator – Uniwersytet Ekonomiczny we Wrocławiu**, ul. Komandorska 118/120, 53-345 Wrocław, NIP: 896-000-69-97, tel. +48 71 36 80 100, , e-mail: kontakt@ue.wroc.pl.

   Administrator danych decyduje o celach i środkach przetwarzania danych osobowych.

2. **Dane osobowe** - oznaczają 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, numer identyfikacyjny, np. PESEL, NIP, dane o lokalizacji, np. adresy zamieszkania, zameldowania, identyfikator internetowy, adres e-mail lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, np. dane o wynagrodzeniu, kulturową lub społeczną tożsamość osoby fizycznej. Rozporządzenie nie wyłącza ochrony danych osób fizycznych prowadzących działalność gospodarczą, jednoosobowo albo w ramach spółek cywilnych. Dane osobowe osób fizycznych prowadzących działalność gospodarczą chronione są na równi z danymi osób fizycznych nieprowadzących działalności gospodarczej. Za dane niepodlegające Polityce

bezpieczeństwa danych osobowych uważa się informacje dotyczące osób prawnych, np. spółek z o.o., akcyjnych lub jednostek organizacyjnych nieposiadających osobowości prawnej, np. spółek jawnych, komandytowych.

3. **Przetwarzanie danych** - oznacza 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;
4. **Jednostka organizacyjna lub Jednostka** – jednostka lub komórka organizacyjna określona w Regulaminie organizacyjnym UEW;
5. **Kierujący jednostką organizacyjną** – kierownik jednostki organizacyjnej w rozumieniu Regulaminu Organizacyjnego Uniwersytetu Ekonomicznego we Wrocławiu;
6. **Ograniczenie przetwarzania –** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania, w szczególności zgodnie z artykułem 18 Rozporządzenia.
7. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
8. **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
9. **Odbiorca** – oznacza 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; za odbiorców uznaje się w szczególności podmioty przetwarzające, takie jak np. przedsiębiorstwa obsługujące podróże krajowe i zagraniczne, informatyków, serwisantów programów komputerowych, obsługę prawną, tłumaczy, przedsiębiorstwa kurierskie.
10. **Strona trzecia** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
11. **Zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
12. **Naruszenie ochrony danych osobowych** – oznacza naruszenie bezpieczeństwa

prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13. **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

III. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe przetwarzane są u Administratora danych zgodnie z poniższymi zasadami:

1. „**Zgodność z prawem, rzetelność i przejrzystość**" – dane osobowe są przetwarzane zgodnie z prawem i rzetelnie, a także w sposób przejrzysty dla osoby, której dane dotyczą poprzez należyte informowanie o istotnych dla tej osoby aspektach przetwarzania danych;

2. „**Ograniczenie celu**" - dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

3. „**Minimalizacja danych**" – dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami;

4. „**Prawidłowość**" – dane osobowe są prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

5. **„Ograniczenie przechowywania**" – dane osobowe są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

6. „**Integralność i poufność**" – dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;

7. „**Rozliczalność**" - Administrator jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie.

IV. PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH

1. Uwzględniając określone niniejszą Polityką zasady prowadzenia Rejestru czynności przetwarzania danych osobowych oraz obowiązek jego bieżącej aktualizacji, Administrator danych przetwarza dane osobowe co najmniej następujących kategorii osób fizycznych:

a) studentów (członków rodzin studentów, kandydatów)

b) doktorantów (członków rodzin doktorantów, kandydatów);

c) innych osób korzystających z procesu dydaktycznego realizowanego przez Uczelnię, w tym uczestników studiów podyplomowych i szkoleń (ich pracodawców), kandydatów;

d) absolwentów;

e) autorów i recenzentów,

f) osób prowadzących zajęcia dydaktyczne lub badania naukowe (spoza UEW);

g) gości domów studenckich;

h) osób korzystających z Biblioteki;

i) osób korzystających z księgarni internetowej UEW;

j) osób zatrudnionych (członków rodzin);

k) kandydatów na pracowników, zleceniobiorców, wykonawców;

l) wolontariuszy;

m) dostawców, nabywców, usługodawców, usługobiorców (w tym przyszłych).

2. Dane osobowe osób, o których mowa w punkcie 1 przetwarzane są na podstawie Rozporządzenia, w tym na podstawie artykułu 6 ust. 1 pkt „a", „b" „c", „e", artykułu 9 ust. 2 pkt „a", „b", tj.

a) przetwarzanie danych osobowych studentów (odpowiednio członków rodzin studentów, kandydatów na studentów) jest niezbędne do przeprowadzenia procesu rekrutacyjnego, wykonania umowy, udzielania dodatkowych świadczeń nieobjętych umową, np. pomocy materialnej lub zakwaterowania w domach studenckich, wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora w dziedzinie ochrony socjalnej, wypełniania obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e", artykuł 9 ust. 2 pkt „a", „b" Rozporządzenia);

b) przetwarzanie danych osobowych doktorantów (odpowiednio członków rodzin doktorantów, kandydatów na doktorantów) jest niezbędne do przeprowadzenia procesu rekrutacyjnego, wykonania umowy, udzielania dodatkowych świadczeń nieobjętych umową, np. pomocy materialnej, wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora w dziedzinie ochrony socjalnej, wypełniania obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e", artykuł 9 ust. 2 pkt „a", „b" Rozporządzenia);

c) przetwarzanie danych osobowych innych osób korzystających z procesu

dydaktycznego realizowanego przez Uczelnię, w tym uczestników studiów podyplomowych i szkoleń (ich pracodawców) oraz kandydatów jest niezbędne do przeprowadzenia procesu rekrutacyjnego i wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e" Rozporządzenia);

d) przetwarzanie danych osobowych absolwentów jest niezbędne do wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi w tym w szczególności w celu dostosowania programu studiów do potrzeb rynku (Administrator danych prowadzi monitoring karier zawodowych swoich absolwentów) oraz informowania absolwentów o działalności statutowej Administratora (w tym: wydarzeniach, konferencjach, sympozjach, szkoleniach, zjazdach lub osiągnięciach), co pozwala na popularyzowanie działalności statutowej prowadzonej przez Administratora oraz na rozwój kompetencji i umiejętności (artykuł 6 ust. 1 pkt „c", „e", „f");

e) przetwarzanie danych osobowych autorów i recenzentów jest niezbędne do podjęcia działań przed zawarciem umowy, a następnie do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e" Rozporządzenia);

f) przetwarzanie danych osobowych osób prowadzących zajęcia dydaktyczne lub badania naukowe (spoza UEW) jest niezbędne do podjęcia działań przed zawarciem umowy lub porozumienia, a następnie do wykonania umowy lub porozumienia, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e" Rozporządzenia);

g) przetwarzanie danych osobowych gości domów studenckich jest niezbędne do podjęcia działań przed zawarciem umowy, a następnie do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e" Rozporządzenia);

h) przetwarzanie danych osobowych osób korzystających z Biblioteki jest niezbędne do przeprowadzenia procesu rejestracyjnego, a następnie do wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „c", „e" Rozporządzenia);

i) przetwarzanie danych osobowych osób korzystających z księgarni internetowej UEW jest niezbędne do przeprowadzenia procesu rejestracyjnego, a następnie do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych (artykuł 6 ust. 1 pkt „a", „b" „c" Rozporządzenia);

j) przetwarzanie danych osobowych pracowników (emerytów i rencistów - byłych pracowników, odpowiednio członków rodzin) i osób zatrudnionych na podstawie umów cywilnoprawnych przez Administratora danych jest niezbędne do wykonania umowy, udzielania dodatkowych świadczeń nieobjętych umową, np. pomocy materialnej, wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora w dziedzinie ochrony socjalnej, wypełniania obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e", artykuł 9 ust. 2 pkt „a", „b" Rozporządzenia);

k) przetwarzanie danych osobowych kandydatów na pracowników, zleceniobiorców, wykonawców jest niezbędne do przeprowadzenia procesu rekrutacyjnego (artykuł 6 ust. 1 pkt „a" Rozporządzenia);

l) przetwarzanie danych osobowych wolontariuszy przez Administratora danych jest niezbędne do podjęcia działań przed zawarciem porozumienia lub umowy, a następnie do wykonania porozumienia lub umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „a", „b" „c", „e" Rozporządzenia);

m) przetwarzanie danych osobowych dostawców, nabywców, usługodawców, usługobiorców (usługobiorców tym przyszłych) jest niezbędne do tworzenia bazy danych oraz ewentualnego przeprowadzenia negocjacji przed zawarciem umowy z Administratorem danych (artykuł 6 ust. 1 pkt „a" i „b" Rozporządzenia), a w przypadku zawarcia umowy przetwarzanie danych osobowych jest niezbędne do wykonania umowy, wypełnienia obowiązków prawnych ciążących na Administratorze danych oraz jest niezbędne w ramach sprawowania władzy publicznej powierzonej Administratorowi (artykuł 6 ust. 1 pkt „b" „c", „e" Rozporządzenia);

3. W przypadku osób, o których mowa w ust. 1, z zachowaniem zasady Minimalizacji danych i o ile z przepisów prawa powszechnie obowiązującego nie wynika potrzeba przetwarzania szerszego zakresu danych, Administrator danych przetwarza co najmniej następujące kategorie danych osobowych:

a) w przypadku studentów (kandydatów): imiona i nazwisko, nazwisko poprzednie, płeć, data, miejscowość i kraj urodzenia, imiona rodziców, obywatelstwo, numer PESEL, rodzaj, seria, numer i data ważności dokumentu potwierdzającego tożsamość oraz kraj wydania dokumentu tożsamości, nr telefonu kontaktowego komórkowy i alternatywny, adres e-mail prywatny i uczelniany, adres zamieszkania, adres do korespondencji, miejsce zamieszkania przed rozpoczęciem studiów: wieś lub miasto; nr rachunku bankowego, numer indywidualnego konta rozliczeniowego, wybrane języki obce, informacje dotyczące powszechnego obowiązku służby wojskowej, zdjęcie, rodzaj, nazwa, miejscowość, kraj ukończenia szkoły, rodzaj matury, rok uzyskania dokumentu, kraj, numer i data wydania dokumentu, rodzaj i nazwa instytucji wystawiającej dokument, uczestnictwo i

osiągnięcia w olimpiadach szczebla centralnego, tytuł zawodowy, rodzaj niepełnosprawności i datę ważności badań lekarskich, informacje wynikające z z zaświadczenia lekarskiego o braku przeciwskazań do odbywania studiów, przebieg studiów, nr dyplomu, numer albumu, wykształcenie, marka i numer rejestracyjny samochodu studentów, którzy korzystają z parkingu, informacje w przedmiocie przyznanych świadczeń pomocy materialnej, dane, które były podstawą do przyznania świadczeń (w tym dane członków rodziny studenta), np. oświadczenia o dochodach studenta i członów jego rodziny, orzeczenia o niepełnosprawności studenta lub członków jego rodziny, dokumenty stwierdzające wysokość dochodu rodziny studenta, potwierdzające stan rodzinny (w tym stopień pokrewieństwa) i sytuację rodzinną, rodzaj niepełnosprawności,; w przypadku cudzoziemców dodatkowo: podstawa przyjęcia i kształcenia, tryb odbywania studiów/finansowania, informacje o posiadaniu Karty Polaka, o spełnianiu wymagań określonych w art. 5 ust. 1 ustawy z dnia 9 listopada 2000 r. o repatriacji, posiadaniu statusu UKR (ochrony czasowej obywateli Ukrainy), informację o legalności pobytu w RP, posiadaniu ubezpieczenia zdrowotnego;

b) w przypadku doktorantów (kandydatów): imię i nazwisko, nazwisko poprzednie, płeć, data, miejscowość i kraj urodzenia, imiona rodziców, narodowość i obywatelstwo, numer PESEL, a w przypadku jego braku – seria i numer dokumentu potwierdzającego tożsamość oraz kraj wydania dokumentu tożsamości, dziedziny nauki i dyscypliny naukowej, daty rozpoczęcia kształcenia w Szkole Doktorskiej i przebieg kształcenia, informacje o przyznanym stypendium doktoranckim, informacje o pozostawaniu w stosunku pracy z uczelnią, w której kształci się w Szkole Doktorskiej, w przypadku cudzoziemców: kraj pochodzenia, informacje o podjęciu i odbywaniu kształcenia na zasadach obowiązujących obywateli polskich, informacje o podstawie przyjęcia do Szkoły Doktorskiej, informacje o warunkach finansowych kształcenia, informacje o posiadaniu Karty Polaka lub o spełnianiu wymagań określonych w art. 5 ust. 1 ustawy z dnia 9 listopada 2000 r. o repatriacji, niezbędne dane członków rodziny, w szczególności w przypadku zgłoszenia do ubezpieczenia;

c) w przypadku innych osób korzystających z procesu dydaktycznego realizowanego przez Uczelnię, w tym uczestników studiów podyplomowych i szkoleń (ich pracodawców), kandydatów: imię i nazwisko, nazwisko poprzednie/panieńskie, płeć, data i miejsce urodzenia, imiona rodziców, narodowość i obywatelstwo, numer PESEL, a w przypadku jego braku – seria i numer dokumentu potwierdzającego tożsamość oraz kraj wydania dokumentu tożsamości, adres zamieszkania, nr telefonu kontaktowego, adres e-mail, wykształcenie (nazwa ukończonej szkoły, rok ukończenia, nr dyplomu), tytuł/stopień zawodowy, miejsce pracy, stanowisko, staż pracy (lata) dane dotyczące pracodawcy, dane dotyczące odpłatności za studia/szkolenie, przebieg studiów, szkolenia, w przypadku pracodawców - nazwa i adres firmy, NIP, REGON, imię, nazwisko oraz stanowisko osoby reprezentującej firmę;

d) w przypadku absolwentów (poza danymi pobranymi na potrzeby kształcenia i w

okresie legalnego ich przechowywania, o ile tak pobrane dane osobowe mogą służyć celom związanym z utrzymaniem kontaktu z absolwentem): informacja o posiadanym statusie absolwenta, nazwa ukończonego kierunku i rok ukończenia studiów, nazwa firmy i stanowisko.

e) w przypadku autorów, recenzentów: imię i nazwisko, numer PESEL, a w przypadku jego braku – seria i numer dokumentu tożsamości, miejsce urodzenia, właściwy urząd skarbowy, oddział NFZ, obywatelstwo, kraj rezydencji, imiona rodziców, nazwisko matki adres zamieszkania, numer rachunku bankowego, numery ewidencyjne, nr telefonu kontaktowego, adres e-mail, dane dotyczące publikacji, recenzji;

f) w przypadku osób prowadzących zajęcia dydaktyczne lub badania naukowe (spoza UEW): imię, nazwisko, płeć, data urodzenia, PESEL, a w przypadku jego braku – seria i numer dokumentu tożsamości, imiona i nazwiska rodziców, miejsce urodzenia, obywatelstwo, kraj rezydencji, adres zamieszkania, telefon, e-mail, właściwy Oddział NFZ, urząd skarbowy, nazwa uczelni/firmy, stanowisko, tytuł, numer rachunku bankowego;

g) w przypadku gości domów studenckich: imię, nazwisko, numer PESEL, a w przypadku jego braku – seria i numer dokumentu tożsamości, adres zamieszkania, telefon, e-mail, w przypadku odwiedzin przez członków rodziny mieszkańca - stopień pokrewieństwa;

h) w przypadku osób korzystających z Biblioteki: imię i nazwisko, adres zamieszkania, numer PESEL, a w przypadku jego braku – seria i numer dokumentu tożsamości, adres e-mail, numer telefonu, miejsce pracy, nazwę uczelni, formę i kierunek studiów, rok studiów, numer albumu, loginy, hasła.

i) w przypadku osób korzystających z księgarni internetowej UEW: imię, nazwisko, firma, adres zamieszkania, adres e-mail, numer telefonu, dane dotyczące zamówienia, loginy, hasła.

j) w przypadku osób zatrudnionych: imię, nazwisko, firmy, PESEL/NIP, dane teleadresowe, obywatelstwo, numery ewidencyjne, pozostałe dane z dowodów osobistych i innych dokumentów tożsamości, numery rachunków bankowych, wynagrodzenia, informacje o stanie rodzinnym, majątkowym, warunkach i przebiegu zatrudnienia, informacje dotyczące dodatkowego zatrudnienia, informację o prowadzeniu działalności gospodarczej, wykształceniu, właściwym Oddziale NFZ, urzędzie skarbowym, uprawnieniach, umiejętnościach, informacje dotyczące powszechnego obowiązku służby wojskowej, informacje dot. przynależności do PPK i programu opieki medycznej, informacje dot. pobieranej emerytury/renty, niekaralności, informacje o zajęciu wynagrodzenia za pracę, zasiłku chorobowego, dane niezbędne do wypłaty zasiłku opiekuńczego, dane osoby, którą należy zawiadomić w razie wypadku, informacje o zdrowiu niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej oraz inne dane osobowe

znajdujące się w aktach osobowych, wymagane albo dopuszczalne przez obowiązujące przepisy prawa; w przypadku obcokrajowców dodatkowo także informacje potwierdzające legalność pobytu i zatrudnienia; w przypadku zgonu pracownika dane spadkobierców; przy wnioskach o nadanie orderu/odznaczenia pracownikowi: imię ojca, imię i nazwisko rodowe matki, miejsce urodzenia, poprzednie nazwiska, informacje o byciu posłem, senatorem lub zajmowaniu stanowiska kierowniczego w rozumieniu art. 2 ustawy z dnia 31.07.1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe;

k) w przypadku kandydatów na pracowników, zleceniobiorców, wykonawców: imię, nazwisko, dane teleadresowe, numery ewidencyjne, informacje o zatrudnieniu, wykształceniu, kwalifikacje zawodowe, informacja o dopuszczeniu do pracy, u obcokrajowców dokumenty potwierdzające legalność pobytu i zatrudnienia, wizerunek na zdjęciach załączonych do CV;

l) w przypadku wolontariuszy (opiekunów prawnych wolontariuszy niepełnoletnich, korzystających oraz opiekunów wolontariuszy): imię, nazwisko, PESEL, adres zamieszkania;

m) w przypadku dostawców, nabywców, usługodawców, usługobiorców (tym przyszłych): imię, nazwisko, firmy, dane teleadresowe, numery ewidencyjne, numery rachunków bankowych, informacje o oferowanych usługach, towarach, dane finansowe.

4. Administrator danych nie zbiera i nie przetwarza danych osobowych dotyczących wyroków skazujących osób fizycznych i naruszeń prawa przez osoby fizyczne, w tym zaświadczeń o niekaralności, nawet jeżeli osoba wyrazi zgodę na przetwarzanie tych danych, chyba że przetwarzanie danych osobowych dotyczących wyroków skazujących osób fizycznych i naruszeń prawa przez osoby fizyczne, w tym zaświadczeń o niekaralności, jest dozwolone lub wymagane przez powszechnie obowiązujące przepisy prawa polskiego lub Unii Europejskiej.

5. Administrator danych nie zbiera i nie przetwarza danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, chyba że osoba fizyczna wyrazi zgodę na przetwarzanie tych danych albo jest to niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, w szczególności związane z medycyną pracy, zatrudnieniem osób niepełnosprawnych, zakwaterowaniem studentów, udzielaniem zapomóg dla studentów, prowadzeniem Zakładowego Fundusz Świadczeń Socjalnych.

6. Dane osobowe studentów (członków rodzin studentów) są przechowywane do upływu okresu przechowywania dokumentacji, wynikającego z powszechnie obowiązujących przepisów prawa. Dane osobowe kandydatów są przechowywane przez okres

przeprowadzania procesu rekrutacji.

7. Dane osobowe doktorantów (członków rodzin doktorantów) są przechowywane do upływu okresu przechowywania dokumentacji, wynikającego z powszechnie obowiązujących przepisów prawa. Dane osobowe kandydatów są przechowywane przez okres przeprowadzania procesu rekrutacji.
8. Dane osobowe innych osób korzystających z procesu dydaktycznego realizowanego przez Uczelnię, w tym uczestników studiów podyplomowych i szkoleń (ich pracodawców) są przechowywane do upływu okresu przechowywania dokumentacji związanej z umową, wynikającego z powszechnie obowiązujących przepisów prawa. Dane osobowe kandydatów są przechowywane przez okres przeprowadzania procesu rekrutacji.
9. Dane osobowe absolwentów są przechowywane do upływu okresu przechowywania dokumentacji, wynikającego z powszechnie obowiązujących przepisów prawa.
10. Dane osobowe autorów i recenzentów są przechowywane do upływu okresu przechowywania dokumentacji związanej z umową, wynikającego z powszechnie obowiązujących przepisów prawa.
11. Dane osobowe osób prowadzących zajęcia dydaktyczne lub badania naukowe (spoza UEW) są przechowywane przez okres niezbędny do wykonania zadań przez tych pracowników, chyba że z powszechnie obowiązujących przepisów prawa wynika dłuższy okres przechowywania dokumentacji związanej z tymi zadaniami.
12. Dane osobowe gości domów studenckich są przechowywane do upływu okresu przechowywania dokumentacji związanej z umową, wynikającego z powszechnie obowiązujących przepisów prawa.
13. Dane osobowe osób korzystających z Biblioteki są przechowywane do dnia usunięcia konta czytelnika, chyba że obowiązujące przepisy prawa nakazują przechowywanie danych osobowych przez okres dłuższy.
14. Dane osobowe osób korzystających z księgarni internetowej UEW są przechowywane do dnia usunięcia konta zamawiającego. W przypadku dokonania zamówień dane osobowe są przechowywane do upływu okresu przechowywania dokumentacji związanej z umową, wynikającego z powszechnie obowiązujących przepisów prawa.
15. Dane osobowe pracowników i osób zatrudnionych na podstawie umów cywilnoprawnych są przechowywane do upływu okresu przechowywania dokumentacji związanej z umową, wynikającego z powszechnie obowiązujących przepisów prawa.
16. Dane osobowe kandydatów są przechowywane przez okres przeprowadzania procesu rekrutacji, a po jego zakończeniu są przechowywane w bazie danych kandydatów przez okres nie dłuższy niż 3 miesiące. W przypadku braku prowadzenia rekrutacji dane osobowe kandydatów są przechowywane w bazie danych przez okres nie dłuższy niż 3 miesiące.

17. Dane osobowe wolontariuszy są przechowywane do upływu okresu przechowywania dokumentacji związanej z porozumieniem lub umową, wynikającego z powszechnie obowiązujących przepisów prawa. Dane osobowe kandydatów na wolontariuszy, z którymi nie została zawarta porozumienie lub umowa, są przechowywane w bazie danych przez okres nie dłuższy niż 3 miesiące.

18. Dane osobowe dostawców, nabywców, usługodawców, usługobiorców są przechowywane przez okres ważności ofert lub przez okres niezbędny do przeprowadzenia procesu negocjacji przed zawarciem umowy, a po zawarciu umowy dane osobowe są przechowywane do upływu okresu przechowywania dokumentacji związanej z umową, wynikającego z powszechnie obowiązujących przepisów prawa.

19. Dane osobowe mogą być przechowywane przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

    Osoba, której dane dotyczą, ma prawo wówczas wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

    Administrator danych zobowiązany jest ocenić czy do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych możliwe jest przetwarzanie danych anonimowych. Jeżeli jest to niemożliwe przetwarzanie danych powinno podlegać odpowiednim zabezpieczeniom w szczególności poprzez wdrożenie środków technicznych i organizacyjnych, zapewniających poszanowanie zasady Minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele.

20. Administrator danych przed zawarciem umowy ze studentem, uczestnikiem, autorem, pracownikiem, dostawcą, usługobiorcą, itp., w szczególności podczas pierwszego kontaktu z kandydatem na studenta, pracownika, z przyszłym dostawcą, usługobiorcą uzyskuje w razie potrzeby zgodę na przetwarzanie danych osobowych, od osoby, której dane dotyczą.

    Analogicznie Administrator danych uzyskuje zgodę na przetwarzanie danych od osób które złożyły wniosek o stypendium, zapomogę, świadczenie socjalne, pokój w Domu Studenckim oraz w innych przypadkach, gdy następuje przetwarzanie nowych danych osobowych, a podstawą przetwarzania jest zgoda

    Przetwarzanie danych osobowych osób, z którymi została zawarta przez Administratora danych umowa albo zostało przyznane świadczenie, następuje na podstawie tej umowy, decyzji lub innego orzeczenia i w celu jej realizacji oraz realizacji obowiązków wynikających z obowiązujących przepisów prawa.

21. Zgoda może być udzielona w formie pisemnej lub elektronicznej. Niedopuszczalne jest stosowanie na stronach internetowych Administratora danych domyślnie zaznaczonego okienka ze zgodą na przetwarzanie danych osobowych.

W przypadku braku albo utrudnionej możliwości uzyskania zgody pisemnej lub elektronicznej uzyskuje się zgodę w formie ustnej. Zgoda w formie ustnej powinna być udokumentowana poprzez sporządzenie notatki z rozmowy, z podaniem:

a) daty udzielenia zgody,

b) imienia i nazwiska osoby, która udzieliła zgody,

c) wykonania obowiązku poinformowania przed udzieleniem zgody o prawie do cofnięcia zgody w dowolnym momencie,

d) treści zgody,

e) imienia i nazwiska osoby, która otrzymała oświadczenie o zgodzie.

Notatka powinna być podpisana przez osobę, która otrzymała oświadczenie o zgodzie.

22. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę.

23. Oświadczenie o wycofaniu zgody może być wyrażone w dowolnej formie, w tym pisemnej, elektronicznej, ustnej. Cofnięcie zgody w formie ustnej powinno być udokumentowane poprzez sporządzenie notatki z rozmowy, z podaniem:

a) daty cofnięcia zgody,

b) imienia i nazwiska osoby, która cofnęła zgodę,

c) treści cofnięcia zgody,

d) imienia i nazwiska osoby, która otrzymała oświadczenie o cofnięciu zgody.

Notatka powinna być podpisana przez osobę, która otrzymała oświadczenie o cofnięciu zgody i przekazana kierującemu właściwą jednostkę organizacyjną.

24. Wycofanie zgody na przetwarzanie danych osobowych kandydata na studenta, doktoranta, uczestnika procesu dydaktycznego realizowanego przez Uczelnię (pracodawcy uczestnika), wolontariusza, kandydata na pracownika, zleceniobiorcę, wykonawcę, przyszłego autora, dostawcy, usługobiorcy, uniemożliwia dalsze prowadzenie procesu rekrutacyjnego, rejestracyjnego, negocjacji.

Po zawarciu umowy czy przyznaniu świadczeń wycofanie zgody na przetwarzanie danych osobowych nie powoduje, że zakazane jest przetwarzanie danych osobowych. Przetwarzanie danych następuje wówczas na innej podstawie prawnej, tj. na podstawie tej umowy i w celu jej realizacji oraz w celu wykonania obowiązków prawnych wynikających z powszechnie obowiązujących przepisów prawa.

W przypadku zwiększenia zakresu przetwarzanych danych lub zmiany celu przetwarzania danych, osoba, której dane dotyczą, powinna wyrazić zgodę na przetwarzanie danych w zwiększonym zakresie lub w innym celu niż pierwotny, jeżeli

podstawą przetwarzania jest zgoda. Brak zgody skutkuje brakiem możliwości podjęcia stosownych działań przez Administratora.

V. PROFILOWANIE OSOBY FIZYCZNEJ

1. Administrator danych korzysta na swoich stronach internetowych z mechanizmów pozwalających, przy wykorzystaniu danych osobowych, na profilowanie osoby fizycznej (w szczególności z **plików *cookies***) (profilowanie zwykłe).

   W pozostałym zakresie Administrator danych nie stosuje profilowania osób fizycznych, w tym nie korzysta z programów, które w zautomatyzowany sposób gromadzą lub porządkują dane osobowe w celu analizy aspektów dotyczących efektów pracy osoby fizycznej.

2. W związku z korzystaniem przez Administratora danych na swoich stronach internetowych z plików pozwalających na profilowanie osoby fizycznej, Administrator stosuje niniejszą Politykę oraz dodatkowo wykonuje opisane w niniejszym punkcie obowiązki.

3. Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

4. Administrator danych stosuje pliki *cookies* w celach określonych w polityce prywatności na stronie internetowej Administratora danych.

5. Administrator danych poinformuje na stronie internetowej osobę, której dane dotyczą, o:

   a) fakcie profilowania i sposobie wyrażenia zgody na profilowanie, a także udostępni pozostałe informacje, o których mowa w Rozdziale VI, w szczególności poprzez odniesienie się do zamieszczonej na stronie internetowej „polityki prywatności”.

      Zgoda na profilowanie może być wyrażona w postaci elektronicznej.

   b) prawie do wniesienia bezpłatnego sprzeciwu wobec profilowania, jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego służącego promocji produktów lub usług i profilowanie jest powiązane z takim marketingiem.

      Prawo to będzie wyraźnie podane do wiadomości osobie, której dane dotyczą, najpóźniej przy okazji pierwszej komunikacji z tą osobą oraz będzie przedstawione jasno i oddzielnie od wszelkich innych informacji. Sprzeciw może zostać wniesiony w dowolnej formie i nie wymaga uzasadnienia. Wniesienie sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego powoduje, że danych nie wolno już przetwarzać do takich celów.

6. W przypadku wdrożenia podejmowania decyzji opartych wyłącznie na profilowaniu (profilowanie szczególne), np. elektroniczne metody rekrutacji albo wyłącznie zautomatyzowane decyzje dotyczące zawarcia, rozwiązania lub zmiany umowy z osobą, której dane dotyczą, Administrator danych poinformuje osobę, której dane dotyczą, o:

   a) fakcie profilowania oraz o zasadach profilowania, znaczeniu i przewidywanych konsekwencjach profilowania;

   b) prawie do niepodlegania decyzji, która opiera się wyłącznie na profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

7. Zautomatyzowane podejmowanie decyzji opartych wyłącznie na profilowaniu jest dopuszczalne w szczególności pod warunkiem, że jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem danych lub opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

8. W przypadku wdrożenia zautomatyzowanego podejmowania decyzji opartego wyłącznie na profilowaniu, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator danych przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, na zasadach określonych w art. 35 i n. Rozporządzenia.

VI. OBOWIĄZKI INFORMACYJNE ADMINISTRATORA DANYCH

1. Administrator danych podaje osobie, której dane dotyczą informacje o:

   a) nazwie, adresie, numerach identyfikacyjnych, danych kontaktowych Administratora danych;

   b) danych kontaktowych inspektora ochrony danych;

   c) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji;

   d) prawnie uzasadnionych interesach realizowanych przez Administratora, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f Rozporządzenia;

   e) odbiorcach danych osobowych lub o kategoriach odbiorców danych osobowych;

   f) istnieniu albo braku istnienia wymogu podania danych osobowych oraz konsekwencjach niepodania danych osobowych;

   g) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję

Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;

h) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;

i) prawie dostępu do danych osobowych, żądania ich sprostowania, uzupełnienia, usunięcia lub ograniczenia przetwarzania danych osobowych, prawie do wniesienia sprzeciwu wobec przetwarzania, prawie do przenoszenia danych, prawie do wniesienia skargi do organu nadzorczego;

j) prawie cofnięcia w dowolnym momencie zgody na przetwarzania danych osobowych, w przypadku jej udzielenia;

k) stosowaniu zautomatyzowanego przetwarzania danych osobowych (profilowanie);

l) prawie do wniesienia bezpłatnego sprzeciwu wobec przetwarzania danych osobowych do celów marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim, w przypadku prowadzenie działalności marketingowej, np. przez wydawnictwo Administratora danych;

m) stosowaniu zautomatyzowanego podejmowania decyzji, w tym o służącemu temu profilowaniu, oraz o prawie wniesienia sprzeciwu wobec zautomatyzowanego podejmowania decyzji.

2. Powyższe dane przekazywane są podczas pozyskiwania danych osobowych, w szczególności przy:

a) uzyskiwaniu pisemnej lub elektronicznej zgody na przetwarzanie danych osobowych, w szczególności podczas procesów rekrutacyjnych czy rejestracyjnych, według wzorów stosowanych przez Administratora danych i wynikających z właściwego (odnoszącego się do danego procesu rekrutacyjnego lub rejestracyjnego) zarządzenia Rektora, a w braku takiego zarządzenia – według wzoru przyjętego przez właściwą jednostkę organizacyjną, prowadzącą proces rekrutacji lub rejestracji;

Zastrzega się, że w przypadku zastosowania zgód udzielanych na stronie internetowej Administratora danych podczas rekrutacji lub rejestracji, odpowiednie oświadczenia o udzieleniu zgody na przetwarzanie danych powinny być zawarte również w formularzach zgłoszeniowych, które wypełnia, podpisuje i składa osoba uczestnicząca w rekrutacji lub dokonująca rejestracji.

W przypadku pozyskiwania nowych danych osobowych od studentów, doktorantów, osób zatrudnionych, np. danych o dochodach członków rodziny na potrzeby postępowania o przyznanie miejsca w domu studenckim, stypendium czy zapomogi, w sytuacji **gdy następuje zmiana podstawy prawnej przetwarzania danych osobowych, celu przetwarzania danych osobowych oraz okresu przechowywania danych osobowych**, Administrator danych powinien przekazać

nowe informacje osobie, której dane dotyczą. Dane osobowe członków rodziny, bez których rozpatrzenie wniosku o przyznanie stypendium lub zapomogi nie jest możliwe przetwarzane są na podstawie artykułu 6 ust. 1 pkt „c" oraz artykułu 9 ust. 2 pkt „b" Rozporządzenia. W przypadku osób, o których mowa w zdaniu poprzedzającym znajduje zastosowanie zwolnienie z obowiązku informacyjnego, o którym mowa w artykule 14 ust. 5 pkt „c" Rozporządzenia.

b) zawieraniu umowy ze studentem, uczestnikiem (pracodawcą uczestnika), autorem podręcznika, umowy o pracę, umowy zlecenia, umowy o dzieło lub innej umowy z osobami zatrudnionymi, umowy z dostawcami, usługobiorcami, przyznaniu stypendium, zapomogi czy innych świadczeń według wzorów stosowanych przez Administratora danych i wynikających z właściwego (odnoszącego się do stosunku danego rodzaju) zarządzenia Rektora, a w braku takiego zarządzenia – według wzoru przyjętego przez właściwą jednostkę organizacyjną;

c) w odpowiedzi na zgłoszenie kandydata, dostawcy, usługobiorcy, który udzielił zgody na przetwarzanie danych osobowych (np. w treści CV, oferty albo wysłał CV/ofertę mailem), chyba że otrzymane dane osobowe kandydata, dostawcy, usługobiorcy zostaną niezwłocznie usunięte; o ile w odpowiedzi na zgłoszenie dojdzie do przekazania informacji, o których mowa w ust. 1 powyżej, należy wskazać nadawcy zgłoszenia, że podstawą prawną przetwarzania jego danych osobowych pozostają przepisy Rozporządzenia, w tym art. 6 ust. 1 lit a.

3. W przypadku pozyskiwania danych osobowych, w sposób inny niż od osoby, której dane dotyczą, np. gdy wnioskodawca poda we wniosku dane osobowe innej osoby, Administrator co do zasady przekazuje tej osobie informacje, o których mowa w ust. 1, oraz dodatkowo informuje o źródle pochodzenia danych osobowych i kategoriach przetwarzanych danych.

   Administrator nie jest zobowiązany do podawania osobie, które dane dotyczą, powyższych informacji, jeżeli pozyskiwanie danych osobowych jest wyraźnie uregulowane przez powszechnie obowiązujące przepisy prawa polskiego lub Unii Europejskiej przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą.

4. Informacje, o których mowa w ust. 1, będą przekazywane w formie pisemnej lub elektronicznej, np. w systemach informatycznych przeznaczonych do obsługi wniosków lub podań.

   W przypadku braku albo utrudnionej możliwości przekazania pisemnych lub elektronicznych informacji, o których mowa w punkcie 1, informacje przekazuje się w formie ustnej, jeżeli osoba, której dane dotyczą, tego zażąda i o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą, np. numer telefonu wynika z dokumentów przesyłanych przez kandydata.

   Przekazanie informacji w formie ustnej powinno być udokumentowane poprzez sporządzenie notatki z rozmowy, z podaniem daty rozmowy, treści żądania podania informacji w formie ustnej, treści przekazanych informacji, imienia i nazwiska osoby,

która otrzymała informację, imienia i nazwiska osoby, która sporządziła notatkę. Notatka powinna być podpisana przez osobę, która ją sporządziła.

5. Administrator danych w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem prowadzi z osobą, której dane dotyczą, wszelką komunikację w sprawie informacji, o których mowa w punkcie 1 powyżej, a także w sprawie sprostowania, uzupełnienia, usuwania danych, ograniczenia przetwarzania, przenoszenia danych, zautomatyzowanego podejmowania decyzji, sprzeciwu wobec zautomatyzowanego podejmowania decyzji, naruszeniu ochrony danych osobowych, jeżeli to naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

6. Administrator danych co do zasady udziela informacji, o których mowa powyżej, bezpłatnie i bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania udzielenia informacji. W razie potrzeby termin ten można przedłużyć okolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Szczegółowe zasady udzielenia informacji zawierają artykuły 12, 15–22 i 34 Rozporządzenia.

7. Informacji udziela się na piśmie lub elektronicznie, na adresy podane przez osobę której dane dotyczą. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Informacje przekazują kierujący jednostkami organizacyjnymi Administratora danych. W przypadku przekazywania informacji na piśmie do rąk osoby, której dane dotyczą, należy uzyskać podpis tej osoby na dokumencie, który zawiera informacje.

VII. ZABEZPIECZENIE DANYCH OSOBOWYCH

1. POSTANOWIENIA OGÓLNE

1. Administrator danych stosuje odpowiednie środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych, w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieuprawnionym (chyba że obowiązujące przepisy prawa stanowią, że dane są jawne), uzyskaniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych uwzględnia stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia i stosuje odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Środki, o których mowa w zdaniu poprzedzającym opisano w niniejszej Polityce bezpieczeństwa danych osobowych, Polityce bezpieczeństwa informacji, Zasadach Bezpieczeństwa informacji oraz Zasadach Zarządzania Systemami Informatycznymi.

3. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, Administrator danych uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w tym wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji,nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
4. Stosowane środki techniczne i organizacyjne zapewniają w sposób ciągły poufność, integralność, dostępność i odporność systemów przetwarzania (np. odporność na ingerencję z zewnątrz z użyciem odpowiedniego oprogramowania), a także zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, np. awarii systemu informatycznego.
5. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych.
6. Administrator danych na bieżąco ocenia skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych. Środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych są w razie potrzeby poddawane przeglądom i uaktualniane.

2. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

a) POSTANOWIENIA OGÓLNE

Administrator danych tworzy odpowiednie zabezpieczenia organizacyjne w celu ochrony danych osobowych przed nieupoważnionym dostępem i rozpowszechnianiem:

1) Dane osobowe muszą być:

   a) przetwarzane zgodnie z prawem;

   b) przetwarzane przez osoby posiadające odpowiednie upoważnienia i – w razie potrzeby - uprawnienia do przetwarzania danych w systemach informatycznych, które zapoznały się z przepisami prawa dotyczącymi ochrony danych osobowych, w tym aktami prawa wewnętrznego przejętymi przez Administratora danych;

   c) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;

   d) merytorycznie poprawne i w razie potrzeby uaktualniane;

   e) adekwatne oraz ograniczone do tego, co niezbędne w stosunku do celów, w jakich są przetwarzane;

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

   g) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem

przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

2) Ochronie podlegają dane zgromadzone w jakiejkolwiek formie, w tym w dokumentach, kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, oraz w systemach informatycznych.

3) Przetwarzanie danych może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień do przetwarzania danych (w tym co do kategorii osób, których dane osoba upoważniona może przetwarzać) wynika z zakresu upoważnienia.

   Osoby posiadające ograniczone upoważnienie do przetwarzania danych, np. do danych osobowych zleceniobiorców, nie są upoważnione do przetwarzania innych danych osobowych, np. danych pracowników Administratora danych.

4) Wszystkie osoby przetwarzające dane zobowiązane są do przetwarzania danych z najwyższą starannością, wyłącznie w zakresie i celu przewidzianym upoważnieniem, niewykorzystywania danych w celach pozasłużbowych, bądź niezgodnych z upoważnieniem, zachowania danych w tajemnicy przez czas nieoznaczony, również po zakończeniu współpracy z Administratorem danych, zachowania w tajemnicy sposobów zabezpieczenia danych przez czas nieoznaczony, również po zakończeniu współpracy z Administratorem danych, ochrony danych przed udostępnieniem osobom nieupoważnionym, w szczególności wglądem, dodawaniem, zmianą, usunięciem.

5) Kierujący jednostkami organizacyjnymi Administratora danych są odpowiedzialni za przestrzeganie w podległych im jednostkach organizacyjnych przepisów powszechnie obowiązujących oraz przepisów wewnętrznych Administratora danych dotyczących ochrony danych osobowych.

   Kierujący jednostkami organizacyjnymi Administratora danych zapewniają, żeby podległe im osoby zatrudnione posiadały odpowiednie upoważnienia i – w razie potrzeby uprawnienia do przetwarzania danych w systemach informatycznych oraz dokonują niezbędnych przeszkoleń z zakresu ochrony danych osobowych, przed dopuszczeniem osoby zatrudnionej do pracy. **Odpowiedniość upoważnienia i/lub uprawnienia oznacza jego ograniczenie do przetwarzania danych osobowych wyłącznie tych kategorii osób, które jest niezbędne do wykonywania obowiązków służbowych przez osobę upoważnioną.**

   Kierujący jednostkami organizacyjnymi Administratora danych i Inspektor ochrony danych zobowiązani są do współdziałania w celu zapewnienia należytego przestrzegania przepisów dotyczących ochrony danych osobowych.

6) Przed przystąpieniem do przetwarzania danych, Pracownik ma obowiązek szczegółowego zapoznania się z niniejszą Polityką, Polityką Bezpieczeństwa Informacji oraz Zasadami Bezpieczeństwa Informacji, na dowód czego składa oświadczenie zgodnie z **załącznikiem numer 1,** w którym zobowiązuje się do przestrzegania ww. aktów prawa wewnętrznego. Obowiązek przestrzegania aktów prawa wewnętrznego, o których mowa w zdaniu poprzedzającym dotyczy także Współpracowników Uczelni (w rozumieniu PBI i zwanych dalej Współpracownikami).

7) Naruszenie Polityki bezpieczeństwa danych, Polityki Bezpieczeństwa Informacji lub Zasad Bezpieczeństwa Informacji, a w przypadku osób pełniących funkcje WBSI, ABSI, ATSI lub Właściciela InT także Zasad Zarządzania Systemami Informatycznymi może powodować odpowiedzialność służbową lub być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych albo za naruszenie dające podstawę do rozwiązania umowy cywilnoprawnej w trybie natychmiastowym, a takżeuprawniające Administratora danych do dochodzenia odszkodowania.

8) Dane osobowe są przetwarzane przez:

   a) Organy Uniwersytetu (Administratora danych);

   b) osoby upoważnione przez Administratora danych – upoważnienie odpowiednio do zakresu przetwarzanych danych osobowych i kategorii osób, których dane dotyczą;

   c) podmioty przetwarzające dane osobowe w imieniu Administratora danych lub wspólnie z nim na podstawie umów zawartych z Administratorem danych, np. przedsiębiorstwa obsługujące podróże krajowe i zagraniczne, informatycy, serwisanci programów komputerowych, obsługa prawna, tłumacze, przedsiębiorstwa kurierskie;

   d) podmioty, którym Administrator udostępnił dane osobowe, w sytuacjach przewidzianych prawem.

   Osoby/podmioty wykonujące usługi sprzątania, konserwacji, remontów, usuwania awarii nie są upoważnione do dostępu i przetwarzania danych osobowych. Umowy z tymi podmiotami powinny zawierać postanowienia o zachowaniu w tajemnicy wszelkich informacji uzyskanych w związku z realizacją usług; umowy te czy odrębne oświadczenia nie powinny jednak upoważniać do przetwarzania danych osobowych.

9) Administrator danych przetwarza dane osobowe w miejscach, w których realizuje swe statutowe zadania, stanowiących jego własność lub przez niego wskazanych, a także z wykorzystaniem tzw. rozwiązań chmurowych (obszar przetwarzania danych).

10) Wymiana danych pomiędzy lokalizacjami wchodzącymi w skład obszaru przetwarzania danych może następować pod warunkiem zabezpieczenia poufności danych.

11) Ogólne zasady zabezpieczenia obszaru przetwarzania danych osobowych:

   a) dostęp do budynków i pomieszczeń podlega kontroli dostępu na zasadach określonych aktami prawa wewnętrznego, w sposób gwarantujący możliwość dostępu wyłącznie osobom upoważnionym;

   b) w przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której przetwarzane są dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej.

12) Zakazane jest kopiowanie/wprowadzanie danych osobowych na nośniki danych i ich przetwarzanie poza obszarem przetwarzania danych (w tym w prywatnych zasobach

chmurowych lub poza systemami informatycznymi Administratora danych), z wyjątkiem ustalonych z Administratorem danych podróży służbowych lub przekazania danych podmiotowi przetwarzającemu/współadministratorowi, albo gdy w innym przypadku Inspektor ochrony danych wyrazi zgodę na przetwarzanie danych poza obszarem przetwarzania danych. Nośnikami, o których mowa w zdaniu pierwszym, są m.in. komputery i inne urządzenia przenośne, pamięć flash, dyski twarde, płyty CD/DVD, itp. Nośniki przekazywane poza obszar przetwarzania danych powinny być zabezpieczone w sposób zapewniający poufność danych osobowych, w szczególności:

a) powinny być zabezpieczone hasłem,

b) transportowane w sposób minimalizujący ryzyko kradzieży, zniszczenia, utraty,

c) niepozostawiane w samochodach, hotelach, salach konferencyjnych, chyba że zapewnione jest korzystanie z sejfu,

d) nieużywane w miejscach publicznych i środkach transportu publicznego, chybaże zapewniona jest poufność danych osobowych,

e) nieużywane poprzez podłączenie do publicznej (otwartej) sieci WI-FI.

13) Zakazane jest przesyłanie danych, w szczególności pisemnie lub w formie korespondencji e-mail, poza obszar przetwarzania danych osobowych, z wyjątkiem przesyłania podmiotom przetwarzającym/ współadministratorom danych/ podmiotom, którym udostępniono dane osobowe, przesyłania osobie, której dane dotyczą, kopii jej danych osobowych podlegających przetwarzaniu lub przesyłania organom administracji, sądom i innym instytucjom upoważnionym do otrzymywania danych osobowych na podstawie obowiązujących przepisów i pod warunkiem zabezpieczenia poufności danych.

14) Zakazane jest przechowywanie i przetwarzanie danych osobowych w prywatnych zasobach chmurowych (OneDrive, Google Drive, iCloud itp.)

15) Zakazane jest publikowanie wyników egzaminów, poprzez podanie imienia i nazwiska zdającego, chyba że obowiązujące przepisy prawa dopuszczają taką możliwość.

16) Przebywanie osób nieuprawnionych, w tym osób nieupoważnionych do przetwarzania określonych kategorii danych osobowych, w miejscach przetwarzania danych jest dopuszczalne w obecności Administratora danych lub osoby upoważnionej do przetwarzania tych danych osobowych i przy zachowaniubezpieczeństwa danych, w szczególności należy odwrócić albo zasłonić dokumenty zawierające dane osobowe, odpowiednio obrócić albo wyłączyć monitor, włączyć wygaszacz ekranu chroniony hasłem, np. poprzez użycie skrótu klawiszowego Windows + L.

17) Zakazane jest przekazywanie kluczy do pomieszczeń, szafek, biurek, szuflad, sejfów, w których znajdują się dane osobowe, osobom nieupoważnionym do przetwarzania danych osobowych albo nieupoważnionym do przetwarzania określonych kategorii danych osobowych.

18) Osoby odpowiedzialne za odbiór przesyłek pocztowych i kurierskich zabezpieczają

korespondencję adresowaną do Administratora danych i zawierającą dane osobowe zabezpieczają pocztę, która wpłynęła do Administratora danych i zawiera dane osobowe, przed dostępem osób nieupoważnionych do przetwarzania określonych kategorii danych osobowych, do momentu przekazania odpowiednim osobom.

19) Po zakończeniu przetwarzania danych osobowych w danym dniu pracy zakazane jest pozostawianie otwartych pomieszczeń, szafek, biurek, szuflad, sejfów, w których znajdują się dane osobowe oraz zakazane jest pozostawianie dokumentów i nośników z danymi osobowymi na biurkach oraz niewyłączonych komputerów.

20) W momencie zakończenia przez osoby upoważnione do przetwarzania danych wykonywania związanych z tym przetwarzaniem czynności lub opuszczenia pomieszczenia, w którym przetwarzane są dane osobowe, z innego powodu, zobowiązane są te osoby do zabezpieczenia pomieszczeń stanowiących miejsca przetwarzania danych poprzez zamknięcie prowadzących do nich drzwi lub zabezpieczenia danych poprzez umieszczenie dokumentów i elektronicznych nośników danych w miejscu, do którego nie mają dostępu osoby nieupoważnione do przetwarzania danych osobowych lub nieupoważnione do przetwarzania określonych kategorii danych osobowych, np. w szafkach, biurkach, szufladach, sejfach zamykanych na klucz.

21) Zakazane jest pozostawianie dokumentów w drukarkach, skanerach, kopiarkach.

22) Osoby/podmioty wykonujące usługi sprzątania, konserwacji, remontów, usuwania awarii nie są upoważnione do dostępu i przetwarzania danych osobowych. Administrator danych i osoby zatrudnione u Administratora danych uniemożliwiają wgląd do danych osobowych osobom/podmiotom wykonującym powyższe usługi, w szczególności poprzez umieszczenie dokumentów i elektronicznych nośników danych w szafkach, biurkach, szufladach, sejfach, zamykanych na klucz, nadzór przez osobę upoważnioną do przetwarzania danych osobowych nad wykonywaniem powyższych usług w pomieszczeniu, wylogowanie z systemu informatycznego, włączenie wygaszacza ekranu chronionego hasłem.

    Osoba zatrudniona u Administratora danych zawiadamia kierownika jednostki organizacyjnej Administratora danych, któremu podlega, o:

    a) otrzymaniu żądań dotyczących danych osobowych, w szczególności, udzielenia informacji dotyczących danych osobowych, sprostowania, uzupełnienia, usunięcia danych, ograniczenia przetwarzania, przeniesienia danych,

    b) otrzymaniu danych osobowych lub żądania dotyczącego danych osobowych niezwłocznie, nie później niż w ciągu jednego dnia roboczego od dnia otrzymania.

    Kierujący jednostką organizacyjną, w razie potrzeby we współpracy z Inspektorem ochrony danych, przygotowuje odpowiednie pisma, odpowiedzi, zawiadomienia w związku z otrzymanymi danymi osobowymi lub żądaniami dotyczącymi danych osobowych.

23) Osoba zatrudniona u Administratora danych niezwłocznie zawiadamia kierującego

jednostką organizacyjną o konieczności aktualizacji kategorii przetwarzanych danych osobowych, kategorii osób, których dane dotyczą, celów przetwarzania danych, odbiorców, terminów usunięcia poszczególnych kategorii danych. Zawiadomienie przekazywane jest niezwłocznie Inspektorowi ochrony danych celem niezwłocznego przygotowania odpowiednich aktualizacji do Rejestru czynności przetwarzania danych osobowych. Za aktualizację udzielonych upoważnień, jeśli tego wymagają, odpowiada właściwy kierownik jednostki organizacyjnej.

24) Zasady i sposób zawiadamiania o wszelkich naruszeniach ochrony danych osobowych (tj. naruszeniach bezpieczeństwa, w tym w zakresie środków technicznych i organizacyjnych służących ochronie danych osobowych i prowadzących w szczególności do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, w tym kradzieży albo zgubienia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do przetwarzanych danych) reguluje Polityka Bezpieczeństwa Informacji oraz Zarządzenie Rektora w sprawie Procedury zarządzania incydentami cyberbezpieczeństwa i naruszenia ochrony danych osobowych w Uniwersytecie Ekonomicznym we Wrocławiu (zwanej dalej także: Procedurą).

Przykładowo obowiązek zawiadomienia dotyczy:

a) ustnego ujawnienia osobie nieuprawnionej danych osobowych albo zabezpieczeń danych osobowych, w tym ujawnienia danych osobowych albo zabezpieczeń w rozmowie telefonicznej osobie, która nie została jednoznacznie zidentyfikowana,

b) zgubienia albo kradzieży dokumentu, komputera, telefonu lub innego nośnika danych zawierającego dane osobowe pracowników, studentów itp.,

c) doprowadzenia do nieuprawnionego dostępu do systemu informatycznego, pomieszczenia, komputera, na którym przetwarzane są dane osobowe, nośnika zawierającego dane osobowe, itp.,

d) stwierdzenia włamania albo próby włamania do budynku, pomieszczenia, szafki sejfu lub innego miejsca, w którym przetwarzane są dane osobowe,

e) stwierdzenia wirusa albo nieuprawnionego dostępu do systemu informatycznego,

f) stwierdzenia nietypowego zachowania się komputera lub aplikacji (resetowanie, spowolnienie pracy, zmiana wyglądu aplikacji, itp.),

g) dopuszczenia do nieuprawnionego zmodyfikowania, skopiowania albo usunięcia danych,

h) zapisania i pozostawienia w widocznym miejscu hasła do systemu informatycznego,

i) przekazania hasła innej osobie/podmiotowi, przekazania hasła na stronie internetowej lub pocztą elektroniczną,

j) braku możliwości zalogowania się do systemu informatycznego,

k) zmodyfikowania parametrów systemu informatycznego, programu

antywirusowego, firewall,

l) braku użycia niszczarki i wyrzucenia dokumentów zawierających dane osobowe,

m) wyrzucenia nośników danych bez uprzedniego usunięcia danych osobowych.

Każda osoba stwierdzająca wystąpienie naruszenia lub podejrzenia naruszenia danych osobowych informuje o tym niezwłocznie, zgodnie z Procedurą, o której mowa powyżej. Zawiadamiający udziela wszelkich wyjaśnień na żądanie Administratora lub Inspektora ochrony danych.

Inspektor ochrony danych ustala przyczyny, zakres i skutki naruszenia ochrony danych osobowych, osoby odpowiedzialne, ustala i wdraża odpowiednie środki zapobiegawcze przed dalszym naruszeniem albo naruszeniem w przyszłości oraz ustala i wdraża odpowiednie środki w celu przywrócenia prawidłowego funkcjonowania systemu ochrony danych osobowych.

Inspektor ochrony danych we współpracy z kierującym jednostką organizacyjną niezwłocznie przygotowuje odpowiednie materiały do Rejestru naruszeń ochrony danych osobowych oraz zawiadomienia o naruszeniu danych osobowych, jeżeli zachodzą podstawy do wysłania takich zawiadomień.

25) Administrator danych może zarządzić obowiązkowe cykliczne szkolenia w zakresie przetwarzania i ochrony danych osobowych.

b) INSPEKTOR OCHRONY DANYCH

1. Na podstawie art. 37 ust. 4 Rozporządzenia Administrator danych wyznacza Inspektora ochrony danych.
2. Inspektor ochrony danych nie pełni funkcji kierowniczych u Administratora danych ani nie jest zatrudniony u Administratora danych na stanowisku związanym z określaniem sposobów i celów przetwarzania danych.
3. Administrator danych publikuje dane kontaktowe Inspektora ochrony danych na stronie internetowej http://www.uew.pl
4. Administrator danych zawiadamia organ nadzorczy o danych kontaktowych Inspektora ochrony danych.
5. Inspektor ochrony danych jest należycie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych, bez względu na ich skalę, w szczególności poprzez:
   a) udział w spotkaniach kierownictwa Administratora danych dotyczących przetwarzania danych;
   b) uczestnictwo przy podejmowaniu decyzji dotyczących przetwarzania danych;
   c) członkostwo w Rektorskiej Komisji Bezpieczeństwa Informacji.
6. Administrator wspiera Inspektora ochrony danych w wypełnianiu przez niego zadań,

zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

7. Administrator zapewnia, by Inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania zadań dotyczących ochrony danych. Inspektor ochrony danych nie będzie odwoływany ani karany przez Administratora za wypełnianie swoich zadań. Inspektor ochrony danych podlega bezpośrednio Administratorowi danych.

8. Osoby, których dotyczą dane osobowe, mogą kontaktować się z Inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia.

9. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy co do wykonywania swoich zadań.

10. Do głównych zadań Inspektora ochrony danych należy:

    a) informowanie Administratora oraz pracowników, którzy przetwarzają dane, o obowiązkach spoczywających na nich na mocy niniejszej Polityki, Polityki Bezpieczeństwa Informacji, Zasad Bezpieczeństwa Informacji, Rozporządzeniaoraz innych przepisów prawa i doradzanie im w tej sprawie;

    b) monitorowanie przestrzegania niniejszej Polityki, Polityki Bezpieczeństwa Informacji, Zasad Bezpieczeństwa Informacji, Rozporządzenia i innych przepisów prawa w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

    c) współpraca z kierującymi jednostkami organizacyjnymi Administratora danych w celu przygotowania pism, odpowiedzi, zawiadomień w związku z otrzymanymi danymi osobowymi lub żądaniami dotyczącymi danych osobowych lub naruszeniem ochrony danych osobowych;

    d) prowadzenie Rejestru czynności przetwarzania danych osobowych;

    e) ustalanie przyczyny, zakresu i skutków naruszenia ochrony danych osobowych, osób odpowiedzialnych, ustalenie i wdrażanie odpowiednich środków zapobiegawczych przed dalszym naruszeniem albo naruszeniem w przyszłości,

    f) ustalanie i wdrażanie odpowiednich środków w celu przywrócenia prawidłowego funkcjonowania systemu ochrony danych osobowych,

    g) wykonywanie zadań określonych w ZBI, w tym w szczególności zadań związanych z ochroną danych osobowych jako informacji chronionych / współdziałanie z Właścicielem InT, koordynatorem odpowiedzialnym ze strony UEW za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa - zwanym „Koordynatorem KSC" oraz Menedżerem Bezpieczeństwa Teleinformatycznego w przypadku incydentów w obszarze teleinformatycznym, skutkujących lub mogących skutkować naruszeniami ochrony danych osobowych;

    h) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz

monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;

i) współpraca z organem nadzorczym;

j) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych;

k) rozwijanie wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, w szczególności poprzez udział w kursach.

11. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniemryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

c) UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH DLA OSÓB ZATRUDNIONYCH U ADMINISTRATORA DANYCH

1. Administrator danych upoważnia kierujących jednostkami organizacyjnymi do udzielania upoważnień do przetwarzania danych osobowych, określania zakresu upoważnień do przetwarzania danych osobowych oraz odwoływania upoważnień do przetwarzania danych osobowych.
2. Dyrektor Centrum Zarządzania Projektami/Centrum Obsługi Badań Naukowych (w ramach udzielonego mu przez Administratora upoważnienia, o którym mowa w ust. 1 powyżej) może udzielać dalszych upoważnień, tj. umocować kierowników projektów do udzielania upoważnień do przetwarzania danych osobowych na potrzeby realizacji projektu (w tym: do określania zakresu upoważnień do przetwarzania danych osobowych oraz odwoływania upoważnień do przetwarzania danych osobowych). Umocowania udzielone przez Dyrektora Centrum Zarządzania Projektami/Centrum Obsługi Badań Naukowych wymagają dla swej ważności formy pisemnej. O każdym udzielonym upoważnieniu kierownik projektu informuje Dyrektora Centrum właściwego dla projektu, w sposób przez niego wskazany.
3. Osoby zatrudnione zostają upoważnione do przetwarzania danych, o ile przetwarzanie danych osobowych na danym stanowisku jest konieczne.
4. Upoważnienie zawiera imię i nazwisko osoby upoważnionej i zakres upoważnienia. Integralną częścią upoważnień do przetwarzania danych jest również oświadczenie osoby upoważnionej o przyjęciu upoważnienia, zapoznaniu się z przepisami, zobowiązaniu do ich stosowania oraz o zachowaniu danych w tajemnicy, pod rygorem ponoszenia odpowiedzialności karnej i odszkodowawczej. Wzór upoważnienia wraz z oświadczeniem o zachowaniu w tajemnicy stanowi **załącznik numer 1**.
5. Upoważnienie wraz z oświadczeniem o zachowaniu w tajemnicy sporządza się w dwóch egzemplarzach. Jeden egzemplarz upoważnienia przechowuje się w dokumentach zatrudnienia upoważnionego, drugi wręcza się osobie upoważnionej. Powyższe postanowienia stosuje się również do zmiany i anulowania upoważnienia.
6. W przypadku Współpracowników upoważnienie do przetwarzania danych osobowych w zakresie niezbędnym dla realizacji umowy może wynikać wprost z przyjętego właściwym

zarządzeniem Rektora wzoru umowy, bez potrzeby stosowania odrębnego dokumentu upoważnienia.

7. **Kierujący jednostkami organizacyjnymi prowadzą rejestry wszystkich udzielonych upoważnień przy czym rejestry prowadzone przez Dyrektora Centrum Zarządzania Projektami i Dyrektora Centrum Badań Naukowych obejmują także upoważnienia udzielone przez kierowników projektów**. W ramach obowiązku prowadzenia rejestru mieści się także obowiązek bieżącej aktualizacji upoważnień oraz samego rejestru, jak również obowiązek obligatoryjnego, corocznego przeglądu udzielonych upoważnień w terminie do 31 maja każdego roku.
8. Zasady przyznawania, odbierania i modyfikowania uprawnień dostępowych do systemów informatycznych, w tym w obrębie infrastruktury teleinformatycznej, w związku z udzielonymi upoważnieniami określają Zasady Zarządzania Systemami Informatycznymi oraz Zasady Bezpieczeństwa Informacji. Uprawnienia, o których mowa w zdaniu poprzedzającym, przyznawane są adekwatnie do potrzeb wynikających z wykonywanych obowiązków i stosownie do udzielonych upoważnień.
9. Administratorowi danych przysługuje w każdym czasie prawo kontroli udzielanych upoważnień, a ponadto prawo do ich zmiany lub odwołania. Prawo kontroli, o którym mowa w zdaniu poprzedzającym przysługuje także Inspektorowi ochrony danych.

d) PRZEKAZYWANIE NA TERENIE POLSKI I POZOSTAŁYCH KRAJÓW UE DANYCH OSOBOWYCH PODMIOTOM PRZETWARZAJĄCYM DANE OSOBOWE

1. Administrator danych powierzy przetwarzanie danych osobowych osobom, podmiotom, organom, instytucjom na terenie Polski i pozostałych krajów Unii Europejskiej, wyłącznie gdy:

   a) odbiorcą danych osobowych jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem polskim, np. publiczne uczelnie partnerskie, instytucja obsługująca program ERASMUS, Zakład Ubezpieczeń Społecznych, Urząd Skarbowy, Urząd Statystyczny, Policja, Prokuratura, Ministerstwo Nauki i Szkolnictwa Wyższego, Najwyższa Izba Kontroli, Powiatowy Urząd Pracy,

   b) odbiorcą jest podmiot przetwarzający, niebędący organem publicznym, jeżeli została zawarta z tym podmiotem umowa, która określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora danych i podmiotu przetwarzającego dane w imieniu Administratora danych.

2. Podmioty przetwarzające mogą przetwarzać dane osobowe wyłącznie w zakresie i celu określonym w umowie i zobowiązane są przed rozpoczęciem przetwarzania danych zapewnić odpowiednie środki techniczne i organizacyjne, żeby przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.

3. Wzór umowy o powierzenie przetwarzania danych osobowych (w przypadku braku zawarcia innej umowy) stanowi **załącznik nr 2**.

4. W zakresie przestrzegania przepisów o ochronie danych osobowych podmiot przetwarzający ponosi odpowiedzialność jak Administrator danych.
5. Jednostka organizacyjna Administratora danych odpowiedzialna za rejestrację umowy w Centralnym Rejestrze Umów UEW informuje Inspektora ochrony danych o zawarciu umowy z podmiotem przetwarzającym (i jej zmianie) w celu aktualizacji Rejestru czynności przetwarzania danych osobowych. Obowiązek informacyjny, o którym mowa w zdaniu poprzedzającym dotyczy także umów o współadministrowanie danymi.
6. Osoby zatrudnione u Administratora danych zobowiązane są przekazywać dane osobowe wyłącznie odbiorcom wskazanym przez kierującego jednostką organizacyjną, wyłącznie w zakresie przez niego wskazanym oraz na adresykontaktowe przez niego wskazane albo z nim uzgodnione. Dane osobowe w formie papierowej będą przekazywane w sposób uniemożliwiający wgląd osób nieupoważnionych, w szczególności w nieprzezroczystych, trwale zamkniętych kopertach.
7. Zakazane jest przekazanie danych osobowych do odbiorcy przez osoby zatrudnione u Administratora danych bez otrzymania informacji, o których mowa w punkcie 6.
8. Osoby zatrudnione u Administratora danych informują kierującego właściwą jednostką organizacyjną o konieczności przekazania danych osobowych do odbiorcy, który nie został wskazany przez Administratora danych.

e) PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTWA TRZECIEGO (POZA EUROPEJSKI OBSZAR GOSPODARCZY) PODMIOTOM PRZETWARZAJĄCYM DANE OSOBOWE

1. Przekazywanie danych osobowych do państwa trzeciego (nienależącego do Europejskiego Obszaru Gospodarczego) lub organizacji międzynarodowej wymaga uprzedniego ustalenia czy spełnione są warunki przekazania, określone w Rozporządzeniu, w tym czy nie zostanie naruszony stopień ochrony osób fizycznych zagwarantowany w Rozporządzeniu.
2. Administrator danych:
    a) w pierwszej kolejności ustala czy Komisja Europejska stwierdziła w drodze decyzji, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

    Decyzje przyjęte przez Komisję na mocy dyrektywy 95/46/WE, którą uchyla Rozporządzenie, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

    Przekazanie danych przez Administratora do Państwa trzeciego lub organizacji międzynarodowej może nastąpić do:

- organu publicznego, np. do publicznej uczelni partnerskiej, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub państwa członkowskiego, albo

- podmiotu przetwarzającego, niebędącego organem publicznym, jeżeli została zawarta z tym podmiotem umowa zgodnie z **załącznikiem 2**.

b) W razie braku decyzji Komisji Europejskiej Administrator danych może przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia,i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

W tym celu Administrator danych zawiera z podmiotem odbierającym dane w państwie trzecim, niezależnie od tego czy jest organem publicznym czy innym podmiotem, **umowę zawierającą co najmniej wszystkie klauzule ochrony danych przyjęte przez Komisję Europejską** (opublikowane zestawy tzw. modelowych klauzul umownych) **albo stosuje inne odpowiednie zabezpieczenia opisane w artykule 46 Rozporządzenia**.

Zastosowane przez Administratora danych zabezpieczenia powinny zapewniać dostępność egzekwowalnych praw osoby, której dane dotyczą, i skutecznych środków ochrony prawnej - w tym prawa do skutecznych administracyjnych lub sądowych środków zaskarżenia i do żądania odszkodowania - w Unii Europejskiej lub w państwie trzecim.

Zgodnie z zasadą ogólną, stosowane przez Administratora danych wzory umów, klauzul informacyjnych i oświadczeń zawierają postanowienia, że dane osobowe nie będą przekazane do Państwa trzeciego w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679. W przypadku gdy Administrator danych zamierza mimo to przekazać dane osobowe do Państwa trzeciego należy poinformować osobę, której dane dotyczą, o:

a) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

b) stwierdzeniu lub braku stwierdzenia przez Komisję Europejską w drodze decyzji istnienia odpowiedniego stopnia ochrony w państwie trzecim lub organizacji międzynarodowej;

c) wzmiankę o zastosowanych zabezpieczeniach ochrony danych osobowych oraz o tym, gdzie i jak można uzyskać informację na ich temat.

3. **W razie braku** decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń, o których mowa w ust. 2, dane osobowe **niemogą być przekazywane do państwa trzeciego lub organizacji międzynarodowej**, nawet jeżeli osoba, której dane dotyczą, została poinformowana o ewentualnym ryzyku związanym z przekazaniem danych i wyraziła na takie przekazanie zgodę.

4. Jednostka organizacyjna Administratora danych odpowiedzialna za rejestrację umowy w Centralnym Rejestrze Umów UEW informuje Inspektora ochrony danych o zawarciu umowy z podmiotem przetwarzającym w celu aktualizacji Rejestru czynności przetwarzania danych osobowych.
5. Osoby zatrudnione u Administratora danych zobowiązane są przekazywać dane osobowe wyłącznie odbiorcom w państwach trzecich albo organizacjom międzynarodowym wskazanym przez Kierownika jednostki organizacyjnej, wyłącznie w zakresie przez niego wskazanym oraz na adresy kontaktowe przez niego wskazane albo z nim uzgodnione. Dane osobowe w formie papierowej będą przekazywane w sposób uniemożliwiający wgląd osób nieupoważnionych, w szczególności w nieprzezroczystych, trwale zamkniętych kopertach
6. Zakazane jest przekazanie danych osobowych do odbiorcy z państwa trzeciego przez osoby zatrudnione u Administratora danych bez otrzymania informacji, o których mowa w punkcie 5.
7. Osoby zatrudnione u Administratora danych informują właściwego kierownika jednostki organizacyjnej o konieczności przekazania danych osobowych do odbiorcy z państwa trzeciego, który nie został wskazany przez Administratora danych.

f) REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych tworzy Rejestr czynności przetwarzania danych osobowych zgodnie z **załącznikiem numer 3**.
2. Rejestr czynności przetwarzania danych osobowych prowadzi i aktualizuje Inspektor ochrony danych, po uzyskaniu od kierujących jednostkami organizacyjnymi informacji, o których mowa w ust. 3.
3. Rejestr czynności przetwarzania danych osobowych zawiera:
   a) kategorie danych osobowych;
   b) opis kategorii osób, których dane dotyczą;
   c) cele przetwarzania danych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich (poza Europejskim Obszarem Gospodarczym) lub w organizacjach międzynarodowych;
   e) informacje dotyczące przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
   f) planowane terminy usunięcia poszczególnych kategorii danych,
   g) dane dotyczące współadministratora danych.
4. W przypadku zmiany danych, o których mowa pkt 3 należy zmianę odnotować w

Rejestrze. Przykładowo, jeżeli nastąpi przekazanie danych osobowych do Państwa trzeciego albo organizacji międzynarodowej, należy odnotować w Rejestrze nazwę tego Państwa albo organizacji międzynarodowej i datę przekazanie danych oraz dane podmiotu przetwarzającego.

5. Rejestr czynności przetwarzania danych osobowych prowadzony jest w postaci elektronicznej.
6. **Rejestr nie jest jawny**. Administrator danych osobowych udostępnia rejestr na żądanie organu nadzorującego przetwarzanie danych osobowych zgodnie z przepisami o ochronie danych osobowych.

g) REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

1. Administrator danych tworzy Rejestr naruszeń ochrony danych osobowych zgodnie z **załącznikiem numer 4.**
2. Rejestr naruszeń ochrony danych osobowych prowadzi Inspektor ochrony danych.
3. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
4. Rejestr naruszeń ochrony danych osobowych zawiera:
   a) okoliczności naruszenia ochrony danych osobowych;
   b) kategorie i przybliżoną liczbę osób, których dane dotyczą;
   c) kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczynaruszenie;
   d) skutki naruszenia ochrony danych osobowych;
   e) podjęte działania zaradcze.
5. Naruszenie ochrony danych osobowych może powodować w szczególności następujące skutki: utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, naruszenie dobrego imienia lub wszelkie inne znaczne szkody gospodarcze lub społeczne.
6. Inspektor ochrony danych dokumentuje w Rejestrze wszelkie naruszenia ochrony danych osobowych.
7. Administrator danych zawiadamia organ nadzorujący o naruszeniu ochrony danych osobowych bez zbędnej zwłoki (w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
8. Administrator danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli to naruszenie może powodować wysokie

ryzyko naruszenia praw lub wolności tej osoby.

9. Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, w następujących przypadkach:

   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony iśrodki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w

      szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

   b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

   c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

10. Rejestr naruszeń ochrony danych osobowych prowadzony jest w postaci elektronicznej.

11. Rejestr nie jest jawny. Administrator danych osobowych udostępnia Rejestr na żądanie organu nadzorującego przetwarzanie danych osobowych zgodnie z przepisami o ochronie danych osobowych.

3. ŚRODKI TECHNICZNE OCHRONY DANYCH

Administrator danych tworzy i stosuje odpowiednie zabezpieczania techniczne w celu ochrony danych przed nieupoważnionym dostępem i przetwarzaniem:

1. Miejsca przetwarzania danych osobowych zabezpiecza się przed dostępem do nich osób nieuprawnionych w każdym czasie, w szczególności na czas nieobecności w tych miejscach osób upoważnionych do przetwarzania danych.

2. Wydrukowane dokumenty oraz nośniki danych zawierające dane osobowe są przekazywane osobom upoważnionym do przetwarzania danych osobowych w sposób, który uniemożliwia zapoznanie się z ich treścią przez osoby nieupoważnione, np. w nieprzezroczystych, trwale zamkniętych kopertach.

3. Budynki, w których przetwarzane są dane osobowe, zabezpieczone jest monitoringiem.

4. Kopie dokumentów, które są zbędne dla przetwarzania danych, osoba upoważniona niezwłocznie, nie później niż w ciągu 3 dni, niszczy mechanicznie w niszczarce dokumentów.

5. Dane osobowe, które są zbędne dla przetwarzania danych, osoba upoważniona niezwłocznie, nie później niż w ciągu 3 dni, usuwa z systemu informatycznego lub elektronicznego nośnika danych, a jeżeli to jest niemożliwe, przekazuje Inspektorowi ochrony danych w celu uszkodzenia przez informatyka elektronicznego nośnika danych w sposób uniemożliwiający odczytanie i odzyskanie danych osobowych.

4. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH W ZAKRESIESYSTEMÓW INFORMATYCZNYCH

Administrator danych tworzy i stosuje odpowiednie środki techniczne i organizacyjne zarządzania systemami informatycznymi, w których przetwarzane są dane osobowe na zasadach określonych w Polityce Bezpieczeństwa Informacji, Zasadach Bezpieczeństwa Informacji oraz Zasadach Zarządzania Systemami Informatycznymi. Dotyczy to w szczególności: procedury nadawania i usuwania uprawnień w systemach informatycznych, stosowanych metod i środków uwierzytelniania, procedur rozpoczynania, zawieszania i kończenia pracy przez użytkowników systemów, komputerów, komputerów przenośnych oraz innych urządzeń, jak również stosowanych przez Administratora środków ochrony (w tym procedur tworzenia kopii zapasowych oraz stosowanych zabezpieczeń przed dostępem osób nieupoważnionych do danych osobowych przetwarzanych w systemach informatycznych) oraz postępowania w razie naruszenia zasad bezpieczeństwa danych.

IV. ZAŁĄCZNIKI

Załącznikami do niniejszej Polityki są:

Załącznik nr 1	Wzór upoważnienia i oświadczenia o zachowaniu danych w tajemnicy;
Załącznik nr 2	Wzór umowy o powierzenie przetwarzania danych osobowych;
Załącznik nr 3	Rejestr czynności przetwarzania danych osobowych;
Załącznik nr 4	Rejestr naruszeń ochrony danych osobowych.