POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Uniwersytet Ekonomiczny we Wrocławiu

Wrocław 2018

SPIS TREŚCI

I. PRZEDMIOT POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Polityka bezpieczeństwa danych osobowych obejmuje całokształt uregulowań dotyczących przetwarzania i ochrony danych osobowych na Uniwersytecie Ekonomicznym we Wrocławiu (zwanych dalej również „danymi").

Polityka bezpieczeństwa danych osobowych stanowi realizację wymogów 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").

II. DEFINICJE

Użyte w dokumencie pojęcia oznaczają:

1. **Administrator danych – Uniwersytet Ekonomiczny we Wrocławiu**, ul. Komandorska 118/120, 53-345 Wrocław, NIP: 896-000-69-97, tel. +48 71 36 80 100, fax +48 71 36 72 778, e-mail: kontakt@ue.wroc.pl.
   Administrator danych decyduje o celach i środkach przetwarzania danych osobowych.
2. **Administrator sieci lokalnej** – informatyk nadzorujący pracę sieci komputerowej, do jego zadań należy: konfiguracja urządzeń sieciowych, podłączanie urządzeń końcowych do sieci i nadawanie im numerów IP, monitorowanie pracy sieci i zapewnienie jej bezpieczeństwa;
3. **Administrator systemu** (oprogramowania) – osoba nadająca uprawnienia użytkownikom do poszczególnych funkcji poszczególnych programów;
4. **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.

5. **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;
6. **Jednostka organizacyjna** – każdy element struktury organizacyjnej Administratora danych (np.: dziekanaty, instytuty, katedry, działy, sekcje, biura);
7. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
8. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
9. **Ograniczenie przetwarzania –** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania, w szczególności zgodnie z artykułem 18 Rozporządzenia.
10. **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;
11. **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
12. **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 odbiorcę uznaje się w szczególności osoby zatrudnione u Administratora danych, które są upoważnione do przetwarzania danych, a także podmioty przetwarzające, takie jak np. przedsiębiorstwa obsługujące podróże krajowe i zagraniczne, informatyków, serwisantów programów komputerowych, obsługę prawną, tłumaczy, przedsiębiorstwa kurierskie.

13. **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;
14. **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;
15. **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;
16. **Usuwanie danych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
17. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych, literowo-cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
18. **Hasło** – ciąg znaków literowych, cyfrowych, literowo-cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

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. Administrator danych przetwarza dane osobowe następujących osób fizycznych:
   a) studentów (członków rodzin studentów, kandydatów)
   b) doktorantów (członków rodzin doktorantów, kandydatów);
   c) słuchaczy studiów podyplomowych i szkoleń (pracodawców słuchaczy), kandydatów;
   d) absolwentów;
   e) autorów i recenzentów,
   f) zagranicznych pracowników naukowych;
   g) gości domów studenckich;
   h) osób korzystających z Biblioteki;
   i) osób korzystających z Księgarni
   j) osób zatrudnionych (członków rodzin);
   k) kandydatów na pracowników, zleceniobiorców, wykonawców;
   l) wolontariuszy;
   m) dostawców, usługobiorców (przyszłych dostawców, usługobiorców);
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, 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", 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 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 słuchaczy studiów podyplomowych i szkoleń (pracodawców słuchaczy) 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 (artykuł 6 ust. 1 pkt „c", „e" Rozporządzenia);

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 zagranicznych pracowników naukowych 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 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 i osób zatrudnionych na podstawie umów cywilnoprawnych (odpowiednio członków rodzin) przez

Administratora danych jest niezbędne do wykonania umowy, udzielania dodatkowych świadczeń nieobjętych umową, np. pomocy materialnej, 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", 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 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);

m) przetwarzanie danych osobowych dostawców, usługobiorców (przyszłych dostawców, usługobiorców) 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. Administrator przetwarza następujące kategorie osób fizycznych i kategorie danych osobowych:

a) Studentów (odpowiednio członków rodzin studentów, kandydatów): imię i nazwisko, nazwisko poprzednie, płeć, data i miejscowość i kraj urodzenia, narodowość, obywatelstwo, rodzaj i nr dowodu tożsamości, nr PESEL a w przypadku jego braku – numer dokumentu potwierdzającego tożsamość oraz kraj wydania dokumentu tożsamości, pozostałe dane zawarte w dowodzie tożsamości, nr telefonu kontaktowego komórkowy i stacjonarny, adres e-mail prywatny i uczelniany, adres zameldowania, adres zamieszkania, adres do korespondencji, miejsce zamieszkania przed rozpoczęciem studiów: wieś lub miasto; Oddział Narodowego Funduszu Zdrowia, nr rachunku bankowego, wybrane języki obce, informacje dotyczące powszechnego obowiązku służby wojskowej, zdjęcie, rok ukończenia szkoły, w której otrzymano świadectwo dojrzałości, typ szkoły, adres korespondencyjny szkoły, kraj zdawania matury, rodzaj matury, uczestnictwo i osiągnięcia w olimpiadach szczebla centralnego, przebieg studiów i wykształcenie, tytuł zawodowy, rodzaj niepełnosprawności i datę ważności badań lekarskich, imiona rodziców,

organ wydający świadectwo maturalne, informacje o dokumencie stanowiącym podstawę ubiegania się o przyjęcie na studia, przebieg studiów, nr dyplomu, informacje w przedmiocie przyznanych świadczeń pomocy materialnej, dane, które były podstawą do przyznania świadczeń, 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 i sytuację rodzinną, zdjęcie, rodzaj niepełnosprawności, w przypadku cudzoziemców: kraj pochodzenia, informacje o podjęciu i odbywaniu studiów na zasadach obowiązujących obywateli polskich, informacje o podstawie przyjęcia na studia, 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.

b) Doktorantów (odpowiednio członków rodzin doktorantów, kandydatów): imię i nazwisko, numer PESEL, a w przypadku jego braku – numer dokumentu potwierdzającego tożsamość oraz kraj wydania dokumentu tożsamości, obywatelstwo, rok urodzenia, płeć, obszar wiedzy, dziedziny nauki i dyscypliny naukowej albo dziedziny sztuki i dyscypliny artystycznej oraz nazwy studiów doktoranckich, daty rozpoczęcia studiów doktoranckich i przebieg kształcenia, informacje w przedmiocie przyznanych świadczeń pomocy materialnej, dane, które były podstawą do przyznania świadczeń, informacje o przyznanym stypendium doktoranckim, informacje o pozostawaniu w stosunku pracy z uczelnią, w której odbywa stacjonarne studia doktoranckie, w przypadku cudzoziemców: kraj pochodzenia, informacje o podjęciu i odbywaniu studiów na zasadach obowiązujących obywateli polskich, informacje o podstawie przyjęcia na studia, 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.

c) Słuchaczy studiów podyplomowych i szkoleń (pracodawców słuchaczy), kandydatów: imię i nazwisko, imiona rodziców, PESEL, data i miejsce urodzenia, adres zamieszkania, nr telefonu kontaktowego, adres e-mail, wykształcenie, tytuł/stopień zawodowy, miejsce pracy, stanowisko, staż pracy (lata) dane dotyczące pracodawcy, dane dotyczące odpłatności za studia/szkolenie, przebieg studiów, szkolenia.

d) Absolwentów: imię i nazwisko, adres do korespondencji, adres e-mail.

e) Autorów, recenzentów: imię i nazwisko, PESEL, adres zamieszkania, numery ewidencyjne, nr telefonu kontaktowego, adres e-mail, dane dotyczące publikacji, recenzji

f) Zagranicznych pracowników naukowych: imię, nazwisko, data urodzenia, numer dokumentu tożsamości, adres zamieszkania, telefon, e-mail, nazwa uczelni (katedry, wydziału);

g) Gości domów studenckich: imię, nazwisko, Pesel, numer dokumentu tożsamości, adres zamieszkania, telefon, e-mail.

h) Osób korzystających z Biblioteki: imię i nazwisko, adres zamieszkania, adres e-mail, numer telefonu, miejsce pracy, nazwę uczelni, formę i kierunek studiów, rok studiów, numer albumu, nazwę i numer, dokumentu tożsamości, PESEL, loginy, hasła.

i) Osób korzystających z Księgarni: imię, nazwisko, firma, adres zamieszkania, adres e-mail, numer telefonu, dane dotyczące zamówienia, loginy, hasła.

j) Osób zatrudnionych (członków rodziny): imię, nazwisko, firmy, 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, uprawnieniach, umiejętnościach, informacje dotyczące powszechnego obowiązku służby wojskowej, 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.

k) Kandydatów na pracowników, zleceniobiorców, wykonawców: imię, nazwisko, dane teleadresowe, numery ewidencyjne, informacje o zatrudnieniu, wykształceniu, wizerunek na zdjęciach załączonych do CV.

l) Wolontariuszy: imię, nazwisko, dane teleadresowe, wykształcenie.

m) Dostawców, usługobiorców (przyszłych dostawców, usługobiorców): 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 jest dozwolone 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 słuchaczy studiów podyplomowych i szkoleń (pracodawców słuchaczy) 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 zagranicznych pracowników naukowych 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 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 umową, wynikającego z powszechnie obowiązujących przepisów prawa. Dane osobowe kandydatów na wolontariuszy, z którymi nie została zawarta umowa, są przechowywane w bazie danych przez okres nie dłuższy niż 3 miesiące.
18. Dane osobowe dostawców, 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 przetwarzania 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, słuchaczem, autorem, pracownikiem, dostawcą, usługobiorcą, itp., w szczególności podczas pierwszego kontaktu z kandydatem na studenta, pracownika, z przyszłym dostawcą,

usługobiorcą uzyskuje 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.

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. W trym przypadku cofnięcie zgody na przetwarzanie danych jest niedopuszczalne.

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, fax, 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.

24. Wycofanie zgody na przetwarzanie danych osobowych kandydata na studenta, doktoranta, słuchacza (pracodawcy słuchacza), 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 jednak zwiększenia zakresu przetwarzanych danych lub zmiany celu przetwarzania danych, w porównaniu do stanu w momencie zawarcia umowy, np. w przypadku przetwarzania danych dotyczących udzielenia zapomóg/stypendiów, osoba, której dane dotyczą, powinna wyrazić zgodę na przetwarzanie danych w zwiększonym zakresie lub w innym celu niż pierwotny. Wycofanie zgody na przetwarzanie dodatkowych danych osobowych zawartych we wniosku o zapomogę/stypendium uniemożliwia dalsze rozpoznawanie wniosku, który w takiej sytuacji pozostawia się bez rozpoznania.

V. PROFILOWANIE OSOBY FIZYCZNEJ

1. Administrator danych korzysta na swoich stronach internetowych z plików pozwalających, przy wykorzystaniu danych osobowych, na profilowanie osoby fizycznej (w szczególności **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 punkcie 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 nie podlegania decyzji, która opiera się wyłącznie 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) 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;
   c) kategoriach odbiorców danych osobowych;
   d) istnieniu albo braku istnienia wymogu podania danych osobowych oraz konsekwencjach niepodania danych osobowych;
   e) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej i zabezpieczeniach danych osobowych;
   f) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
   g) 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;
   h) prawie cofnięcia w dowolnym momencie zgody na przetwarzania danych osobowych, w przypadku jej udzielenia;
   i) stosowaniu zautomatyzowanego przetwarzania danych osobowych (profilowanie);
   j) 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;
   k) 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 wzoru stosowanego przez Administratora danych (**załączniki nr 1.1, 1.2, 1.4, 1.5)**.

W przypadku zastosowania zgód udzielanych na stronie internetowej Administratora danych podczas rekrutacji na studia, odpowiednie oświadczenia o udzieleniu zgody na przetwarzanie danych powinny być zawarte również w formularzach zgłoszeniowych, które wypełnia, podpisuje i składa student, słuchacz (pracodawca słuchacza) – **załącznik nr 1.3**.

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 czy zapomogi, należy uzyskać zgodę na przetwarzanie danych osobowych. Wzór podania o przyznanie miejsca w domu studenckim stanowi **załącznik nr 1.7**.

b) zawieraniu umowy ze studentem, słuchaczem (pracodawcą słuchacza), 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 (**załączniki 2.1 – 2.7**),

W tym przypadku zmienia się bowiem w szczególności podstawa prawna przetwarzania danych osobowych, cel przetwarzania danych osobowych oraz okres przechowywania danych osobowych, co powoduje, że Administrator danych powinien przekazać nowe informacje osobie, której dane dotyczą.

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 (**załączniki 3.1, 3.2**).

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.

   Administrator nie jest zobowiązanych 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, np. przez przepisy prawa dotyczące ubiegania się o stypendium czy zapomogę, na podstawie których następuje podanie przez wnioskodawcę danych innych osób, w szczególności członków rodziny.

4. Informacje, o których mowa w ust. 1, będą przekazywane w formie pisemnej lub elektronicznej. Informacje przekazują albo zamieszczają w treści umów sekretariaty jednostek lub komórek organizacyjnych Administratora danych.

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. Przykładowe wzory zgód, postanowień i oświadczeń do umów ze studentami, słuchaczami, umów o pracę, zlecenia, o dzieło, umów z dostawcami, usługobiorcami oraz informacji dla kandydatów, dostawców, zleceniobiorców, stanowią **załączniki nr 1.1 – 1.7, 2.1 – 2.7, 3.1 – 3.2**.

   Powyższe załączniki należy stosować odpowiednio również do innych postępowań prowadzonych przez Administratora danych albo innych umów zawieranych przez Administratora danych.
6. 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.
7. 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 o kolejne 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.
8. 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 sekretariaty jednostek lub komórek organizacyjnych Administratora danych. W przypadku przekazywania informacji na piśmie do rąk

osoby, której dane dotyczą, należy uzyskać podpis tej osoby na dokumencie, który zawiera informacje.

9. Pozostałe obowiązki informacyjne Administratora danych określa punkt VII ppkt 2 „f".

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 opisane w niniejszej Polityce odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
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 zabezpieczania 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, które zapoznały się z przepisami prawa dotyczącymi ochrony danych osobowych oraz niniejszą Polityką;
   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 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) Kierownicy jednostek lub komórek organizacyjnych Administratora danych są odpowiedzialni za przestrzeganie w podległych im jednostkach i komórkach organizacyjnych przepisów powszechnie obowiązujących oraz przepisów wewnętrznych Administratora danych dotyczących ochrony danych osobowych.

Kierownicy jednostek lub komórek organizacyjnych Administratora danych zapewniają, żeby podległe mu osoby zatrudnione posiadały odpowiednie upoważnienia do przetwarzania danych oraz dokonują niezbędnych przeszkoleń z zakresu ochrony danych osobowych, przed dopuszczeniem osoby zatrudnionej do pracy.

Kierownicy jednostek lub komórek organizacyjnych Administratora danych i Inspektor ochrony danych zobowiązani są do współdziałania w celu zapewnienia należytego przestrzegania przepisów dotyczących ochrony danych osobowych.

6) Osoba zatrudniona u Administratora danych (bez względu na formę prawną zatrudnienia), przed przystąpieniem do przetwarzania danych, ma obowiązek szczegółowego zapoznania się z Polityką bezpieczeństwa danych osobowych wraz ze wszystkimi jej załącznikami. Po zapoznaniu się z treścią Polityki bezpieczeństwa danych osobowych osoba zatrudniona składa oświadczenie zgodnie z **załącznikiem numer 5.2**.
7) Naruszenie Polityki bezpieczeństwa danych może być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych albo za naruszenie dające podstawę do rozwiązania umowy cywilnoprawnej w trybie natychmiastowym, a także uprawniające Administratora danych do dochodzenia odszkodowania. Naruszenie Polityki bezpieczeństwa danych może powodować odpowiedzialność służbową.
8) Dane osobowe są przetwarzane przez:
   a) Organy Uniwersytetu (Administratora danych);
   b) osoby upoważnione przez Administratora danych z działu administracji (np. Dziekanaty, Archiwum, Dział BHP, Biblioteka, Księgarnia, Biuro Karier, Centrum Kształcenia Ustawicznego, Centrum Współpracy Międzynarodowej, Sekcja Obsługi Projektów Rozwojowych, Dział Domów Studenckich, Dział Pomocy Materialnej dla Studentów i Doktorantów, Dział Polityki i Zarządzania Kadrami, Dział Nauczania, Dział Planowania i Rachuby Płac, Dział Księgowości Ogólnej, Biuro Rekrutacji, Studium Języków Obcych, Studium Wychowania Fizycznego i Sportu, Ekonomiczny Uniwersytet Dziecięcy i Akademia Młodego Ekonomisty, Uniwersytet III Wieku, Wydawnictwo – upoważnienie pełne albo ograniczone odpowiednio do zakresu przetwarzanych danych osobowych;
   c) podmioty przetwarzające dane osobowe w imieniu Administratora danych na podstawie umów zawartych z Administratorem danych, np. przedsiębiorstwa obsługujące podróże krajowe i zagraniczne, informatycy, serwisanci programów komputerowych, obsługa prawna, tłumacze, przedsiębiorstwa kurierskie.

      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 określa następujący obszar, w którym przetwarzane są dane osobowe:
   a) siedziba Administratora danych: ul. Komandorska 118/120, 53-345 Wrocław;
   b) ul. Nowowiejska 3, 58-500 Jelenia Góra;
   ul. Jana Pawła II 38c, 59-700 Bolesławiec.

   Wykaz budynków tworzących obszar, w którym przetwarzane są dane osobowe, prowadzi Inspektor ochrony 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;
   b) kontrola dostępu polega na ewidencjonowaniu wszystkich przypadków pobrania i zwrotu kluczy od budynków i pomieszczeń. W ewidencji zapisuje się imię i nazwisko osoby pobierającej lub zdającej klucze, numer lub inne oznaczenie budynku lub pomieszczenia oraz godzinę pobrania i zdania kluczy;
   c) klucze do budynków lub pomieszczeń, w których przetwarzane są dane osobowe wydawane mogą być wyłącznie osobom upoważnionym do przetwarzania danych osobowych lub innym osobom upoważnionym do dostępu do tych budynków lub pomieszczeń na innych zasadach;
   d) Inspektor ochrony danych przekazuje personelowi przechowującemu klucze w formie pisemnej aktualny wykaz pomieszczeń, do których dostęp jest ograniczony ze względu na przetwarzanie danych osobowych oraz wykaz osób upoważnionych do pobierania kluczy do tych pomieszczeń;
   e) osoby dysponujące zbiorami danych osobowych są zobowiązane do niezwłocznego informowania Inspektora ochrony danych o zmianach personalnych oraz o zmianie lokalizacji miejsc przetwarzania danych osobowych;
   f) 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, z wyjątkiem ustalonych z Administratorem danych podróży służbowych lub przekazania danych podmiotowi przetwarzającemu 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, chyba że 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 lub 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 danych osobowych w chmurze obliczeniowej (na serwerach zewnętrznych), za wyjątkiem usługi Microsoft Office365, realizowanej na podstawie umowy pomiędzy UEW a Microsoft, chyba że jest to niezbędne do realizacji umowy z podmiotem przetwarzającym i pod warunkiem zabezpieczenia poufności danych.
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 zachowaniu bezpieczeństwa 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) Sekretariaty jednostek lub komórek organizacyjnych Administratora danych 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 przy użyciu zamka 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. Klucze należy przekazać do miejsca chronienia odnotowując czas zdania.
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.
23) Osoba zatrudniona u Administratora danych niezwłocznie zawiadamia sekretariat jednostki lub komórki organizacyjnej Administratora danych, której podlega, o otrzymaniu danych osobowych, w szczególności na służbowy adres e-mail, od osób, które nie są zatrudnione u Administratora danych, w tym o otrzymaniu danych osobowych od kandydatów na pracowników, zleceniobiorców.

    Osoba zatrudniona u Administratora danych zawiadamia sekretariat jednostki lub komórki organizacyjnej Administratora danych, której podlega, o otrzymaniu żądań dotyczących danych osobowych, w szczególności, udzielenia informacji dotyczących danych osobowych, sprostowania, uzupełnienia, usunięcia danych, ograniczenia przetwarzania, przeniesienia danych.

    Osoba zatrudniona zawiadamia sekretariat jednostki lub komórki organizacyjnej Administratora danych, której podlega, o otrzymaniu danych osobowych lub żądania dotyczącego danych osobowych niezwłocznie, nie później niż w ciągu jednego dnia roboczego od dnia otrzymania.

Sekretariat we współpracy z Inspektorem ochrony danych przygotowuje odpowiednie pisma, odpowiedzi, zawiadomienia w związku z otrzymanymi danymi osobowymi lub żądaniami dotyczącymi danych osobowych.

24) Osoba zatrudniona u Administratora danych niezwłocznie zawiadamia sekretariat Administratora danych o konieczności aktualizacji kategorii przetwarzanych danych osobowych, kategorii osób, których dane dotyczą, celów przetwarzania danych, odbiorców, terminów usunięcia poszczególnych kategorii danych.

Sekretariat we współpracy z Inspektorem ochrony danych niezwłocznie przygotowuje odpowiednie aktualizacje do Rejestru czynności przetwarzania danych osobowych.

25) Osoba zatrudniona u Administratora danych zawiadamia sekretariat jednostki lub komórki organizacyjnej Administratora danych, której podlega, o wszelkich naruszeniach ochrony danych osobowych, tj. naruszeniach bezpieczeństwa, w tym naruszeniach opisanych w niniejszej Polityce środków technicznych i organizacyjnych, prowadzących w szczególności do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, w tym kradzieży albo zgubienia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

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, współpracowników, klientów,
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) samodzielnego pobierania i instalowania oprogramowania,
m) braku użycia niszczarki i wyrzucenia dokumentów zawierających dane osobowe,
n) wyrzucenia nośników danych bez uprzedniego usunięcia danych osobowych.

Osoba zatrudniona zawiadamia sekretariat jednostki lub komórki organizacyjnej Administratora danych, której podlega, o naruszeniu niezwłocznie, nie później niż w ciągu jednego dnia roboczego od dnia wykrycia naruszenia, oraz udziela wszelkich wyjaśnień na żądanie Administratora danych i innych osób.

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

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

26) 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. Dane Inspektora ochrony danych zawiera **załącznik nr 4**.
3. 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.
4. Administrator danych publikuje dane kontaktowe Inspektora ochrony danych na stronie internetowej http://www.ue.wroc.pl/
5. Administrator danych zawiadamia organ nadzorczy o danych kontaktowych Inspektora ochrony danych.

6. 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.
7. 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.
8. 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.
9. 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.
10. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy co do wykonywania swoich zadań.
11. Do głównych zadań Inspektora ochrony danych należy:
    a) udzielanie upoważnień do przetwarzania danych osobowych, określanie zakresu upoważnień do przetwarzania danych osobowych, uchylanie upoważnień do przetwarzania danych osobowych, udzielanie upoważnień do pomieszczeń serwera;
    b) informowanie Administratora oraz pracowników, którzy przetwarzają dane, o obowiązkach spoczywających na nich na mocy niniejszej Polityki, Rozporządzenia oraz innych przepisów prawa i doradzanie im w tej sprawie;
    c) organizowanie przetwarzania danych u Administratora danych w sposób zgodny z Rozporządzeniem;
    d) monitorowanie przestrzegania niniejszej Polityki, Rozporządzenia i innych przepisów prawa, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    e) współpraca z sekretariatami Administratora danych w celu przygotowania pism, odpowiedzi, zawiadomień w związku z otrzymanymi danymi osobowymi lub żądaniami dotyczącymi danych osobowych lub naruszeniem ochrony danych osobowych;
    f) prowadzenie Rejestru czynności przetwarzania danych osobowych i Rejestru naruszeń ochrony danych;
    g) ustalanie przyczyny, zakresu i skutków naruszenia ochrony danych osobowych, osób odpowiedzialnych, ustalenie i wrażenie odpowiednich środki zapobiegawczych przed dalszym naruszeniem albo naruszeniem w przyszłości,

ustalanie i wdrażanie odpowiednich środki w celu przywrócenia prawidłowego funkcjonowania systemu ochrony danych osobowych.

h) wyrażanie zgody na kopiowanie/wprowadzanie danych osobowych na nośniki danych i ich przetwarzanie poza obszarem przetwarzania danych na zasadach określonych w niniejszej Polityce;
i) wyrażanie zgód na pobieranie, instalowanie lub przechowywanie na komputerze programów niezakupionych przez Administratora danych;
j) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;
k) współpraca z organem nadzorczym;
l) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych;
m) rozwijanie wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, w szczególności poprzez udział w kursach.

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

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

1. Administrator danych upoważnia Inspektora ochrony danych do udzielania upoważnień do przetwarzania danych osobowych, określania zakresu upoważnień do przetwarzania danych osobowych, uchylania upoważnień do przetwarzania danych osobowych, udzielania upoważnień do pomieszczeń serwera.
2. Inspektor ochrony danych upoważnia kierowników jednostek i komórek organizacyjnych Administratora danych, jeżeli przetwarzanie danych osobowych przez te osoby jest konieczne.
3. Kierownik jednostki lub komórki organizacyjnej składa do Inspektora ochrony danych wniosek o udzielenie, zmianę, uchylenie upoważnienia. Zmiana albo uchylenie upoważnienia może być spowodowane przez np. zmianę stanowiska pracy, rozwiązanie stosunku pracy. Wzór wniosku stanowi **załącznik nr 5.1**.
4. Inspektor ochrony danych upoważnia zatrudnione osoby (bez względu na formę prawną zatrudnienia) do przetwarzania danych, o ile przetwarzanie danych osobowych na danym stanowisku jest konieczne.
5. Inspektor ochrony danych udzielając upoważnień pełnych lub ograniczonych do przetwarzania danych osobowych stosuje zasadę „minimalnych uprawnień", tj. nadawania jedynie upoważnień koniecznych to przetwarzania niezbędnych danych osobowych na danym stanowisku.

6. Inspektor ochrony danych przekazuje kopię upoważnienia Kierownikowi jednostki lub komórki organizacyjnej oraz Administratorowi Systemu.
7. Za niezwłoczne zarejestrowanie uprawnień dostępu do systemu informatycznego (nadając identyfikator i wnioskowane uprawnienia), zmiany uprawnień, uchylenia uprawnień odpowiedzialny jest Administrator danego systemu, na podstawie okazanego przez Inspektora ochrony danych upoważnienia udzielonego określonej osobie, zmiany upoważnienia, uchylenia upoważnienia.
8. 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 i Polityką bezpieczeństwa danych osobowych, zobowiązaniu do ich stosowania oraz o zachowaniu danych w tajemnicy, pod rygorem ponoszenia odpowiedzialności karnej i odszkodowawczej.
9. Tworzy się następujące rodzaje upoważnień:
   a) upoważnienie do przetwarzania danych osobowych – do dostępu do określonej kategorii danych osobowych oraz określonego zakresu przetwarzania, stosownie do treści upoważnienia;
   b) upoważnienie dla Inspektora ochrony danych – do udzielania upoważnień do przetwarzania danych osobowych, określania zakresu upoważnień do przetwarzania danych osobowych, uchylania upoważnień do przetwarzania danych osobowych, udzielania upoważnień do pomieszczeń serwera;
   c) upoważnienie do dostępu do pomieszczenia serwera.
10. Wzory upoważnień wraz z oświadczeniem o zachowaniu w tajemnicy stanowią **załączniki numer 5.2 - 5.4**. Wzór oświadczenia o uchyleniu upoważnienia stanowi **załącznik nr 5.5**. W przypadku zaistnienia podstaw, Kierownik jednostki lub komórki organizacyjnej niezwłocznie składa do Inspektora ochrony danych wniosek o zmianę albo uchylenie upoważnienia. Kierownik Działu Kadr niezwłocznie zgłasza Inspektorowi ochrony danych fakt rozwiązania umowy z osobą zatrudnioną albo zmiany stanowiska.
11. Upoważnienie wraz z oświadczeniem o zachowaniu w tajemnicy sporządza się w dwóch egzemplarzach. Jeden egzemplarz upoważnienia przechowuje Inspektor ochrony danych, drugi wręcza się osobie upoważnionej. Powyższe postanowienia stosuje się również do zmiany i anulowania upoważnienia.
12. Kierownik jednostki lub komórki organizacyjnej przechowuje kopię upoważnienia, zmiany, uchylenia upoważnienia.
13. Administrator systemu przechowuje kopię upoważnienia, zmiany, uchylenia upoważnienia. Administrator danego systemu odnotowuje identyfikator użytkownika, datę zarejestrowania w systemie, datę usunięcia z systemu.
14. Warunkiem udzielenia ważnego i skutecznego upoważnienia lub zmiany upoważnienia jest podpisanie go przez osobę udzielającą upoważnienia oraz przyjęcie upoważnienia

przez osobę otrzymującą upoważnienie i podpisanie oświadczenia o zachowaniu w tajemnicy.

15. Administratorowi danych oraz Inspektorowi ochrony danych przysługuje w każdym czasie prawo kontroli udzielanych upoważnień oraz ich zmiany lub uchylania.

c) PRZEKAZYWANIE NA TERENIE POLSKI I POZOSTAŁYCH KRAJÓW UNII EUROPEJSKIEJ 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 aneksu dotyczącego danych osobowych do umowy z podmiotem przetwarzającym np. do umowy zlecenia, oraz wzór umowy o przekazanie danych osobowych (w przypadku braku zawarcia innej umowy) stanowią załączniki **załącznik nr 6.1 i 6.2**. Administrator danych wprowadzi postanowienia, o których mowa we wzorze aneksu, do umów z podmiotami przetwarzającymi, chyba że strony umowy zgodzą się stosowanie innych postanowień zapewniających równoważny poziom ochrony danych.
4. W zakresie przestrzegania przepisów o ochronie danych osobowych podmiot przetwarzający ponosi odpowiedzialność jak Administrator danych.
5. Sekretariat jednostki lub komórki organizacyjnej Administratora danych informuje Inspektora ochrony danych o zawarciu umowy z podmiotem przetwarzającym w celu aktualizacji Rejestru czynności przetwarzania danych osobowych.

6. Osoby zatrudnione u Administratora danych zobowiązane są przekazywać dane osobowe wyłącznie odbiorcom wskazanym przez Kierownika komórki lub jednostki organizacyjnej, wyłącznie w zakresie wskazanym przez Kierownika oraz na adresy kontaktowe wskazane przez Kierownika albo uzgodnione z Kierownikiem. 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 sekretariat komórki lub jednostki organizacyjnej o konieczności przekazania danych osobowych do odbiorcy, który nie został wskazany przez Administratora danych.

d) PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTWA TRZECIEGO (POZA UNIĘ EUROPEJSKĄ) PODMIOTOM PRZETWARZAJĄCYM DANE OSOBOWE

1. Przekazywanie danych osobowych do państwa trzeciego (nienależącego do Unii Europejskiej) 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, niebędący organem publicznym, jeżeli została zawarta z tym podmiotem umowa zgodnie z **załącznikiem 6.1 albo 6.2**.

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.

Wzory umów i oświadczeń, o których mowa w załącznikach nr 2.1 – 2.7, np. umów z pracownikami, studentami, 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 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 **nie mogą 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. Sekretariat jednostki lub komórki organizacyjnej Administratora danych 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 komórki lub jednostki organizacyjnej, wyłącznie w zakresie wskazanym przez Kierownika oraz na adresy kontaktowe wskazane przez Kierownika albo uzgodnione z Kierownikiem. 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 sekretariat komórki lub jednostki organizacyjnej o konieczności przekazania danych osobowych do odbiorcy z państwa trzeciego, który nie został wskazany przez Administratora danych.

e) REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych tworzy Rejestr czynności przetwarzania danych osobowych zgodnie z **załącznikiem numer 7**.
2. Rejestr czynności przetwarzania danych osobowych prowadzi Inspektor ochrony danych.
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 Unię Europejską) 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.
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.

f) REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

1. Administrator danych tworzy Rejestr naruszeń ochrony danych osobowych zgodnie z **załącznikiem numer 8.**
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 dotyczy naruszenie;
   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. Wzór zawiadomienia stanowi **załącznik nr 9.**
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 osób fizycznych. Wzór zawiadomienia stanowi **załącznik nr 10.**
9. Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, w następujących przypadkach:
   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki 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.

2. ŚRODKI TECHNICZNE OCHRONY DANYCH

Administrator danych tworzy 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.

3. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH W ZAKRESIE SYSTEMU INFORMATYCZNEGO

1. Dane osobowe mogą być przetwarzane przy użyciu komputerów stacjonarnych oraz komputerów i innych urządzeń przenośnych i przy wykorzystaniu systemu informatycznego.

2. Uwzględniając, że przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.
3. Dane osobowe przetwarzane w systemach informatycznych mogą być przetwarzane wyłącznie w aplikacjach (programach) systemów dostosowanych do merytorycznych potrzeb jednostki organizacyjnej Administratora danych, w której zbiór danych osobowych jest przetwarzany.
4. Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe, powinien posiadać prawa ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań. Zasada obowiązuje także administratorów systemów.
5. Za rejestrowanie uprawnień dostępu do systemu informatycznego odpowiedzialny jest Administrator danego systemu. Po zakończeniu współpracy osoby przetwarzającej dane z Administratorem danych Administrator systemu uniemożliwia tej osobie dostęp do systemu informatycznego poprzez odpowiednie rozwiązania informatyczne.
6. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika i hasła. Użytkownik nie może korzystać z automatycznych procesów logowania.
7. Identyfikatora użytkownika i hasła, w tym haseł archiwalnych, nie można zapisywać / pozostawiać w miejscu, do którego dostęp mają osoby nieuprawnione, w tym nie można ujawniać innym osobom upoważnionym do przetwarzania danych osobowych, nawet po utracie ważności przez hasło.
8. Identyfikator użytkownika ustala Administrator danego systemu.
9. Następuje okresowa zmiana hasła.
10. W przypadku korzystania z komputera podłączonego do sieci Internet zakazane jest wyrażanie zgody na zapamiętywanie identyfikatorów i haseł w systemie komputera lub w przeglądarce.
11. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być przydzielony innej osobie.
12. W momencie zakończenia przez osoby upoważnione do przetwarzania danych wykonywania czynności związanych z tym przetwarzaniem lub opuszczenia pomieszczenia z innego powodu, zobowiązane są one do zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym poprzez wylogowanie się z tego systemu albo włączenie wygaszacza ekranu chronionego hasłem. W momencie zakończenia pracy osoby upoważnione do przetwarzania danych zobowiązane są wyłączyć komputer.
13. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane osobom nieupoważnionym. W razie potrzeby osoba przetwarzająca dane osobowe uniemożliwia wgląd w przetwarzane

dane osobom nieupoważnionym poprzez włączenie wygaszacza ekranu chronionego hasłem, np. poprzez użycie skrótu klawiszowego windows + L.

14. Zainstalowano wygaszacze ekranów chronione hasłem na stanowiskach komputerowych, na których przetwarzane są dane osobowe, z określonym czasem ich aktywacji.
15. Serwer, na którym przechowywane są dane osobowe, znajduje się w odrębnym, zamykanym pomieszczeniu w celu ochrony przed dostępem osób nieupoważnionych.
16. Aktywność użytkowników systemu komputerowego jest logowana.
17. Oprogramowanie stosowane na stanowiskach komputerowych musi być legalne i posiadać ważne licencje, a także musi być na bieżąco aktualizowane. Niezbędne jest zainstalowanie wszystkich aktualizacji proponowanych przez producenta dla danego systemu operacyjnego. Należy włączyć opcję automatycznej aktualizacji systemu operacyjnego.
18. Zakazane jest pobieranie, instalowanie lub przechowywanie na komputerze programów niezakupionych przez Administratora danych. Zgodę na pobieranie, instalowanie lub przechowywanie na komputerze programów niezakupionych przez Administratora danych wyraża Inspektor ochrony danych w uzgodnieniu z Administratorem systemu lub informatykiem.
19. Ściąganie z sieci Internet lub otwieranie plików wykonywalnych (.exe) może się odbywać wyłącznie za każdorazową zgodą Inspektora ochrony danych.
20. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania miejscem przetwarzania danych.
21. Dane powinny być przenoszone przy wykorzystaniu sieci informatycznej Administratora danych. Dane mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
22. Zastosowano środki ochrony systemu informatycznego w postaci: programu antywirusowego oraz programu ochrony dostępu do sieci (firewall). Zakazane jest wyłączanie, blokowanie, odinstalowywanie tego oprogramowania. W przypadku niezbędnego korzystania z komputera osobistego za zastosowanie środków ochrony systemu informatycznego w postaci programu antywirusowego odpowiada użytkownik.
23. Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu poczty elektronicznej odbiorcy dokumentu.
24. W przypadku przesyłania informacji wrażliwych wewnątrz uczelni bądź poza uczelnię należy wykorzystywać mechanizmy kryptograficzne.
25. Zaleca się, aby użytkownik zawarł w korespondencji elektronicznej prośbę o potwierdzenie otrzymania i zapoznania się z informacją.

26. Zakazane jest odbieranie od nieznanych nadawców wiadomości poczty elektronicznej i załączników, których tytuł może sugerować, że zawierają wirusy lub inne programy niebezpieczne dla systemu informatycznego.
27. W przypadku stwierdzenia pojawienia się wirusa, użytkownik winien powiadomić Inspektora ochrony danych, który zleci informatykowi usunięcie zagrożenia i stwierdzi, czy wirus spowodował w zakresie danych osobowych nieuprawniony dostęp, utratę, itp.
28. Szczegółowe środki techniczne i organizacyjne zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe, zawiera dokument „Instrukcja zarządzania systemem informatycznym" (**załącznik numer 11**).

4. POSTANOWIENIA KOŃCOWE

Polityka bezpieczeństwa danych osobowych wchodzi w życie z dniem 25 maja 2018 r.

5. ZAŁĄCZNIKI

Załącznikami do niniejszej Polityki są:

- Załącznik nr 1.1 – 1.7	Przykładowe wzory zgód na przetwarzanie danych osobowych;
- Załącznik nr 2.1 – 2.7	Przykładowe wzory oświadczeń do umów oraz wzory umów z klauzulami dotyczącymi ochrony danych osobowych;
- Załącznik nr 3.1, 3.2	Informacje dla kandydatów na pracowników, przyszłych dostawców, usługobiorców;
- Załącznik nr 4	Dane Inspektora ochrony danych
- Załącznik nr 5.1 – 5.5	Wzór wniosku o upoważnienie do przetwarzania danych. Wzory upoważnień i oświadczeń o zachowaniu danych w tajemnicy, wzór oświadczenia o uchyleniu upoważnienia;
- Załącznik nr 6.1, 6.2	Wzór postanowień do umów z podmiotami przetwarzającymi dane osobowe, wzór umowy o powierzenie przetwarzania danych osobowych;
Załącznik nr 7	Rejestr czynności przetwarzania danych osobowych;
- Załącznik nr 8	Rejestr naruszeń ochrony danych osobowych;
- Załącznik nr 9	Zgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych;
- Załącznik nr 10	Zawiadomienie o naruszeniu ochrony danych osobowych
- Załącznik nr 11	Instrukcja zarządzania systemem informatycznym

Wrocław, dn. 25 maja 2018 r.

Zatwierdził:

.....

REKTOR