Uniwersytet Gdański

POLITYKA OCHRONY DANYCH OSOBOWYCH W UNIWERSYTECIE GDAŃSKIM

Spis treści

I. PODSTAWA PRAWNA

§ 1.

Dane osobowe w Uniwersytecie Gdańskim przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, w szczególności przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zwanego Ogólnym Rozporządzeniem o Ochronie Danych, a także innych aktów prawnych, które znajdują zastosowanie do przetwarzania danych osobowych i ochrony prywatności.

§ 2.

Dane osobowe w Uniwersytecie Gdańskim przetwarzane są w celu realizacji obowiązków oraz uprawnień określonych przepisami prawa (w tym statutowych celów szkoły wyższej), a w szczególności:

1) dla zabezpieczenia prawidłowego toku realizacji zadań dydaktycznych, naukowych, badawczych i organizacyjnych Uczelni wynikających z przepisów ustawy z dnia 20 lipca 2018 roku – Prawo o szkolnictwie wyższym i nauce (t.j. Dz.U. z 2021 r. poz. 478 ze zm.).
2) dla zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni polityki personalnej oraz bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia nawiązywanych przez Uczelnię,
3) dla realizacji innych celów i zadań Uniwersytetu Gdańskiego,

z poszanowaniem praw i wolności osób, których dane osobowe Uczelnia przetwarza.

II. SŁOWNIK POJĘĆ

§ 3.

Użyte w niniejszym dokumencie określenia oznaczają:

1) **Inspektor Ochrony Danych (IOD)** – osobę wyznaczoną przez Administratora, nadzorującą przestrzeganie zasad ochrony przetwarzania danych osobowych w Uczelni. Zadania, uprawnienia i obowiązki wynikające ze stosowania Polityka Ochrony Danych Osobowych odnoszą się również do wyznaczonego przez Administratora Z-cy IOD;
2) **Administrator** – Uniwersytet Gdański reprezentowany przez Rektora;
3) **Administrator Systemu Informatycznego (ASI)** – pracowników jednostek organizacyjnych podległych bezpośrednio Dyrektorowi Centrum Informatycznego lub innych wyznaczonych pracowników Uczelni powołanych przez LADO odpowiedzialnych za zarządzanie oraz utrzymanie systemu przetwarzającego dane osobowe;
4) **Czynność przetwarzania** - zespół powiązanych ze sobą operacji na danych, które można określić w sposób zbiorczy, w związku z celem w jakim te czynności są podejmowane;
5) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6) **Dane osobowe szczególne** - dane osobowe ujawniające 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;
7) **Dane osobowe zwykłe –** wszystkie dane osobowe nie stanowiące danych osobowych szczególnych;
8) **Hasło** – ciąg znaków literowych, cyfrowych lub innych specjalnych znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

9) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
10) **Incydent –** naruszenie ochrony danych osobowych;
11) **Integralność danych** – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
12) **Jednostka organizacyjna** – wyodrębnioną część struktury organizacyjnej Uczelni;
13) **Koordynator Ochrony Danych Osobowych (KODO)** – osobę wyznaczoną przez LADO koordynującą procesy w obszarze ochrony danych osobowych;
14) **Lokalny Administrator Danych Osobowych (LADO)** – osobę, której powierzono obowiązki i uprawnienia Administratora;
15) **Miejsce przetwarzania danych osobowych** – obszar gdzie wykonywane są jakiekolwiek operacje na danych osobowych w ramach jednostki organizacyjnej Administratora;
16) **Naruszenie ochrony danych osobowych** - przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
17) **Osoba upoważniona** – osobę, która upoważniona została w formie pisemnej przez Administratora do przetwarzania danych osobowych;
18) **Podmiot przetwarzający –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
19) **Poufność danych** – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
20) **Proces przetwarzania danych** – zespół czynności przetwarzania danych osobowych;
21) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak, zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
22) **Rozliczalność** – właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
23) **Rozporządzenie** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO);
24) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
25) **Uczelnia lub UG** – Uniwersytet Gdański;
26) **Upoważnienie** – uprawnienie do przetwarzania danych osobowych wydane w formie pisemnej (elektronicznej lub papierowej);
27) **Użytkownik** – osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym, której został przydzielony dostęp do systemu przez ASI;
28) **Współadministrowanie** – sytuacja w której co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych;
29) **Zabezpieczenie danych osobowych** – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
30) **Zdarzenie** – informacja lub okoliczność dająca podejrzenie naruszenia ochrony danych osobowych na podstawie, której dokonuje się oceny ryzyka naruszenia praw i wolności. W przypadku stwierdzenia braku zagrożenia dla praw i wolności zdarzenie nie stanowi naruszenia tych praw.

III. CEL WPROWADZENIA POLITYKI OCHRONY DANYCH OSOBOWYCH

§ 4.

1. Polityka Ochrony Danych Osobowych, zwana dalej Polityką stanowi zbiór zasad obowiązujących przy przetwarzaniu danych osobowych w Uniwersytecie Gdańskim.
2. Celem Polityki jest:
   1) zapewnienie właściwego poziomu bezpieczeństwa danych osobowych w Uczelni poprzez wdrożenie odpowiedniego systemu ich ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi;
   2) podniesienie poziomu świadomości pracowników Uczelni co do istoty problemu bezpieczeństwa danych osobowych.

IV. ZAKRES STOSOWANIA POLITYKI

§ 5.

1. Polityka ma zastosowanie w stosunku do wszystkich postaci informacji zawierających dane osobowe: dokumentów papierowych, zapisów elektronicznych i innych będących własnością Uczelni lub administrowanych przez Uczelnię.
2. Politykę stosuje się do danych osobowych przetwarzanych:
   1) tradycyjnie, w dokumentach papierowych, a w szczególności w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych;
   2) w systemach informatycznych.

§ 6.

1. Procedury określone w niniejszym dokumencie obowiązują wszystkich pracowników administracyjnych i naukowych Uczelni, jak również wszystkie osoby trzecie mające dostęp do danych osobowych przetwarzanych w Uniwersytecie Gdańskim.
2. Ochrona danych osobowych wynikająca z Polityki jest realizowana na każdym etapie przetwarzania informacji.

V. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Zarządzanie danymi osobowymi i zakresy odpowiedzialności

§ 7.

Administratorem przetwarzanych w Uczelni danych osobowych w rozumieniu rozporządzenia jest Uniwersytet Gdański reprezentowany przez Rektora. W trakcie nieobecności Rektora funkcję Administratora pełni zastępujący go Prorektor.

§ 8.

1. Obowiązki wynikające z rozporządzenia Rektor powierza **Lokalnym Administratorom Danych Osobowych (LADO)**, którymi są:
   1) Dziekan Wydziału – w zakresie danych osobowych przetwarzanych w ramach wydziałów oraz osób i jednostek współpracujących;
   2) Kanclerz – w zakresie danych osobowych przetwarzanych w ramach jednostek Administracji Centralnej Uczelni;

3) Dyrektorzy/kierownicy pozostałych jednostek organizacyjnych badawczych, badawczo-rozwojowych, dydaktycznych oraz prowadzonych wspólnie z innymi podmiotami, określonych w Regulaminie Organizacyjnym UG – w zakresie danych osobowych przetwarzanych w ramach tych jednostek oraz osób i podmiotów współpracujących. W wyjątkowych przypadkach funkcję LADO pełnioną przez ww. osoby może pełnić Kanclerz UG. Decyzje w tym zakresie podejmuje Administrator.

2. LADO mogą wyznaczać swoich zastępców, którzy realizują obowiązki wynikające z § 9.
3. LADO, który wyznaczył swojego zastępcę jest zobowiązany niezwłocznie o tym fakcie poinformować Administratora.
4. Nadzór nad realizacją zadań nałożonych na LADO sprawuje Rektor.

§ 9.

1. Lokalni Administratorzy Danych Osobowych są zobowiązani do przestrzegania przepisów dotyczących ochrony danych osobowych w podległym im obszarach, w szczególności poprzez:
   1) zapewnienie właściwych warunków organizacyjnych i technicznych, gwarantujących ochronę danych osobowych przetwarzanych w podległych im obszarach oraz ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   2) dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnienie, aby dane te były:
      a) przetwarzane zgodnie z prawem,
      b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddane dalszemu przetwarzaniu niezgodnemu z tymi celami,
      c) merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane,
      d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
   3) dopuszczanie do przetwarzania danych wyłącznie osób posiadających stosowne upoważnienie;
   4) wdrożenie, a następnie nadzorowanie przestrzegania przez pracowników przepisów wewnętrznych obowiązujących w tym zakresie, tj. Polityki oraz Polityki bezpieczeństwa teleinformatycznego;
   5) wykonywanie zaleceń IOD w zakresie ochrony danych osobowych;
   6) uwzględnianie zaleceń Dyrektora Centrum Informatycznego w zakresie zabezpieczeń systemów informatycznych, w tym akceptowanie, niezbędnych dla zgodności z prawem, modyfikacji stosowanych systemów informatycznych;
   7) sprawowanie kontroli nad przetwarzaniem danych osobowych.
2. LADO sprawują nadzór nad realizacją zadań nałożonych na kierowników jednostek w podległych im obszarach.
3. LADO lub osoba przez niego upoważniona we współpracy z Dyrektorem Centrum Informatycznego sprawuje nadzór nad realizacją zadań nałożonych na ASI, jemu podlegających.

§ 10.

1. Rektor wyznacza **Inspektora Ochrony Danych (IOD)** oraz jego zastępcę, którzy nadzorują przestrzeganie zasad ochrony danych osobowych.
2. W zakresie obowiązków wynikających z niniejszej Polityki, IOD podlega bezpośrednio Rektorowi.
3. IOD wykonuje swoje zadania we współpracy z Lokalnymi Administratorami Danych Osobowych (LADO) i osobą nadzorującą obszar IT, Administratorami Systemów Informatycznych (ASI) oraz z pomocą Dyrektora Centrum Informatycznego lub osobą przez niego upoważnioną.

4. Do zadań IOD należy, w szczególności:
   1) zapewnienie przestrzegania przepisów o ochronie danych osobowych w Uniwersytecie Gdańskim, w tym również udzielanie zaleceń odnośnie ochrony danych osobowych oraz monitorowanie ich wykonania;
   2) podejmowanie działań monitorujących i kontrolnych w jednostkach organizacyjnych Uczelni, lub podmiotach, którym Uczelnia powierzyła przetwarzanie danych osobowych, a w przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych wnioskowanie o niezwłoczne ich usunięcie;
   3) prowadzenie centralnej ewidencji osób upoważnionych do przetwarzania danych osobowych, a także nadzorowanie przyznawania i odwoływania uprawnień w tym zakresie;
   4) prowadzenie centralnego rejestru czynności przetwarzania danych osobowych oraz – gdy ma to zastosowanie - rejestru kategorii czynności przetwarzania dokonywanych w imieniu Administratora, a także innych ewidencji związanych z ochroną danych osobowych;
   5) koordynowanie procesu przyznawania/zmiany/odwoływania uprawnień do przetwarzania danych osobowych w ramach jednostek Administracji Centralnej zgodnie z procedurami określonymi w niniejszej Polityce;
   6) współpracowanie z organem nadzorczym, w tym monitorowanie jego zaleceń w zakresie ochrony danych osobowych i implementowanie ich w Uczelni;
   7) informowanie Administratora, podmiotu przetwarzającego oraz pracowników o obowiązkach spoczywających na nich na mocy rozporządzenia i doradzanie im w tym zakresie;
   8) reagowanie na zdarzenia i incydenty ochrony danych osobowych w Uczelni;
   9) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem praw przysługujących im na mocy rozporządzenia.

§ 11.

1. **Koordynatora Ochrony Danych Osobowych (KODO) oraz jego zastępców,** w podległej jednostce, wyznacza LADO.
2. Do zadań KODO należy:
   1) koordynowanie procesu przyznawania/zmiany/odwoływania uprawnień do przetwarzania danych osobowych w ramach poszczególnych wydziałów / jednostek ogólnouniwersyteckich zgodnie z procedurami określonymi w niniejszej Polityce, w tym w szczególności:
      a) sprawdzenie poprawności wypełnienia wniosku o nadanie/ zmianę/ odwołanie uprawnień do przetwarzania danych osobowych,
      b) weryfikacja zasadności przyznania stosownych uprawnień oraz spełnienia wymogów formalnych niezbędnych do ich uzyskania;
   2) wspomaganie pracowników jednostki organizacyjnej w realizacji zadań związanych z ochroną danych osobowych, w tym w wypełnieniu obowiązku informacyjnego;
   3) koordynowanie działań związanych z naruszeniami ochrony danych osobowych w obszarze podległym LADO;
   4) wykonywanie innych zadań w obszarze przetwarzania danych osobowych na polecenie LADO lub IOD.
3. W zakresie obowiązków wynikających z niniejszej Polityki, KODO współpracuje bezpośrednio z Lokalnym Administratorem Danych Osobowych (LADO), Inspektorem Ochrony Danych (IOD) oraz Administratorami Systemów Informatycznych (ASI).
4. Nadzór nad realizacją zadań nałożonych na KODO sprawują LADO.

§ 12.

Komendant Straży Uniwersyteckiej odpowiada za bezpieczeństwo fizyczne osób i mienia na terenie Uczelni, w tym w szczególności za:

1) kontrolę i monitorowanie ruchu osobowego w budynkach chronionych przez Straż Uniwersytecką,
2) nadzór nad wydawaniem kluczy do pomieszczeń i prowadzeniem ksiąg ewidencyjnych w obiektach UG chronionych przez SU;
3) rekomendowanie działań organizacyjnych, zabezpieczeń mechanicznych i elektronicznych w celu podniesienia poziomu bezpieczeństwa obiektów UG;
4) nadzór nad systemami monitoringu wizyjnego oraz systemami alarmowymi w budynkach chronionych przez Straż Uniwersytecką;
5) zapewnienie ciągłości zabezpieczenia obiektów, w tym planowanie służb oraz dostosowanie czasu pracy i zadań do bieżących potrzeb.

§ 13.

1. **Dyrektor Centrum Informatycznego** lub osoba przez niego upoważniona:
   1) we współpracy z LADO zapewnia bezpieczeństwo danych osobowych w systemach informatycznych, w tym w szczególności poprzez zachowanie poufności, integralności, dostępności i rozliczalności przetwarzanych danych;
   2) określa strategię zabezpieczenia systemów informatycznych Uczelni służących do przetwarzania danych osobowych;
   3) uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych określa potrzeby w zakresie zabezpieczenia systemów informatycznych, zapewniające stopień bezpieczeństwa odpowiadający temu ryzyku;
   4) przygotowuje wspólnie z IOD wytyczne i zalecenia w zakresie zgodności zabezpieczeń systemów informatycznych i aplikacji, w których przetwarzane są dane osobowe z obowiązującymi przepisami i wytycznymi organu nadzorczego w tym zakresie;
   5) wspiera szkolenia w zakresie przestrzegania zasad bezpieczeństwa danych osobowych w systemach informatycznych;
   6) prowadzi centralny rejestr uprawnień do systemów informatycznych, w których przetwarza się dane osobowe;
   7) Prowadzi wykaz ASI;
   8) jest odpowiedzialny za opracowanie, nowelizowanie i wdrożenie Polityki bezpieczeństwa teleinformatycznego.
2. Dyrektor Centrum Informatycznego lub osoba przez niego upoważniona we współpracy z LADO sprawuje nadzór nad realizacją zadań nałożonych na ASI.

§ 14.

1. **Administratorzy Systemów Informatycznych (ASI)** odpowiadają w szczególności za:
   1) czynności związane z bieżącą aktualizacją i utrzymaniem ciągłości działania systemów informatycznych;
   2) przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych, w których przetwarzane są dane osobowe, w tym stosowanie wszelkich dostępnych mechanizmów ochrony celem właściwego ich zabezpieczenia;
   3) przydzielanie użytkownikom dostępu do systemów informatycznych a także blokowanie tego dostępu w przypadku cofnięcia uprawnień lub rozwiązania stosunku pracy;
   4) prowadzenie i aktualizację wykazu osób upoważnionych do przetwarzania danych osobowych w administrowanych przez nich systemach;

5) szkolenie użytkowników z obsługi i bezpiecznej eksploatacji systemów;
6) opracowanie i aktualizację szczegółowej instrukcji zarządzania dla każdego z administrowanych przez siebie systemów przetwarzania danych, zgodnie z wytycznymi określonymi w ramowej Polityce bezpieczeństwa teleinformatycznego;
7) informowanie IOD o wszelkich naruszeniach ochrony danych osobowych w przetwarzanych systemach informatycznych, a także współdziałanie przy usuwaniu skutków tych naruszeń;
8) usuwanie danych osobowych z administrowanych systemów informatycznych;
9) ma obowiązek zweryfikowania czy pracownik jakiemu nadaje/zmienia uprawnienia posiada upoważnienie do przetwarzania danych osobowych.

2. Administratora Systemu Informatycznego powołuje Lokalny Administrator Danych Osobowych w porozumieniu z Dyrektorem Centrum Informatycznego oraz właściwym kierownikiem jednostki organizacyjnej.

§ 15.

1. **Kierowników jednostek organizacyjnych** zobowiązuje się, w szczególności do:
   1) zapewnienia zgodności przetwarzania danych osobowych w podległych im jednostkach, z obowiązującymi przepisami w tym zakresie, ze szczególnym uwzględnieniem przepisów wewnętrznych, tj. Polityki oraz Polityki bezpieczeństwa teleinformatycznego;
   2) ograniczenia dostępu do przetwarzania danych osobowych w podległej jednostce wyłącznie do osób posiadających stosowne upoważnienie nadane przez Administratora;
   3) zarządzania uprawnieniami pracowników do przetwarzania danych osobowych w podległej jednostce, w tym wnioskowania o nadanie, zmianę, odwołanie oraz weryfikację uprawnień;
   4) zapoznawania podległych im pracowników zatrudnionych przy przetwarzaniu danych osobowych z obowiązującymi przepisami w tym zakresie;
   5) wykonywania zaleceń IOD w zakresie ochrony danych osobowych.
2. Kierownicy jednostek sprawują nadzór nad przestrzeganiem przez podległych im pracowników przepisów w zakresie ochrony danych osobowych.

§ 16.

Osoby uprawnione do przetwarzania danych osobowych w Uczelni są zobowiązane:
1) przetwarzać dane osobowe wyłącznie w zakresie upoważnienia zgodnie z powierzonymi obowiązkami pracowniczymi i poleceniami pracodawcy jako Administratora danych;
2) zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczeń zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu;
3) zapoznać się z przepisami prawa w zakresie ochrony danych osobowych, ze szczególnym uwzględnieniem Polityki oraz Polityki bezpieczeństwa teleinformatycznego;
4) stosować określone przez IOD wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych;
5) korzystać z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w Polityce bezpieczeństwa teleinformatycznego;
6) chronić dane osobowe przed dostępem osób nieuprawnionych, zabezpieczać je przed uszkodzeniem, zniszczeniem i nielegalnym ujawnieniem;
7) niezwłocznie informować LADO oraz IOD o zdarzeniach i incydentach.

2. Przyznawanie i odwoływanie uprawnień do przetwarzania danych osobowych

§ 17.

1. Za przyznawanie i odwoływanie uprawnień do przetwarzania danych osobowych odpowiada Administrator.
2. Administrator przyznaje/zmienia i odwołuje uprawnienia do przetwarzania danych osobowych LADO.
3. Właściwy LADO przyznaje/zmienia i odwołuje uprawnienia do przetwarzania danych osobowych w ramach Administracji Centralnej i pozostałych jednostek organizacyjnych, określonych w Regulaminie Organizacyjnym UG.
4. W przypadku wyznaczenia pracownika podległego LADO do pełnienia dodatkowej funkcji, Administrator upoważnia właściwego LADO do przyznawania, zmiany i odwołania dodatkowych uprawnień związanych z pełnioną przez pracownika funkcją.
5. W przypadku nadawania uprawnień studentom lub doktorantom pełniącym określone funkcje lub uczestniczących w realizacji zadań dydaktycznych, naukowych lub rozwojowych, uprawnienia przyznaje właściwy LADO.

§ 18.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie Administratora lub właściwego LADO. Pracownicy UG z chwilą odbycia przeszkolenia w obszarze ochrony danych osobowych nabywają uprawnienia do przetwarzania zwykłych danych osobowych, w zakresie obowiązków określonych przez przełożonego. W przypadku nowo zatrudnionych pracowników, uprawnienie do przetwarzania danych osobowych dot. realizacji korespondencji elektronicznej (poczta elektroniczna oraz EZD standard) oraz korespondencji tradycyjnej, nabywają oni z chwilą zatrudnienia, a przeszkolenie o jakim mowa powyżej muszą odbyć w terminie do 7 dni od zatrudnienia. W zakresie przetwarzania danych osobowych szczególnych, upoważnienie musi być wydane do każdej czynności, w ramach której przetwarzane są te dane, oraz każdorazowo w przypadku zaistnienia jakichkolwiek zmian. Upoważnienie wydaje się w formie pisemnej.
2. Zakres dostępu do danych osobowych oraz do systemów informatycznych określa i akceptuje przełożony pracownika na podstawie zakresu obowiązków, powołań i/lub posiadanych pełnomocnictw bądź osoba nadzorująca w przypadku doktorantów, studentów lub innych osób na podstawie umów cywilnoprawnych, porozumień lub innych dokumentów formalnoprawnych.
3. ASI nadając uprawnienia do systemów informatycznych, w których przetwarzane są dane osobowe, ma obowiązek zweryfikowania czy pracownik posiada upoważnienie do ich przetwarzania.
4. Centrum Informatyczne prowadzi rejestr nadanych dostępów do systemów informatycznych.
5. Procedowanie wniosku o nadanie/zmianę lub odwołanie uprawnień odbywa się zgodnie z *Instrukcją nadawania, zmiany i odwołania uprawnień do przetwarzania danych osobowych*, stanowiącą **załącznik nr 1** do Polityki.
6. Procedowanie wniosku o nadanie/zmianę lub odwołanie uprawnień odbywa się w formie elektronicznej za pomocą dedykowanego systemu informatycznego dostępnego w Portalu Pracownika W wyjątkowych przypadkach dopuszcza się procedowanie wniosków w innej formie niż ww., w tym w formie papierowej w zakresie czynności lub osób nieobjętych systemem. Wniosek przekazuje się do IOD lub KODO, zgodnie z właściwością. Wzór wniosku stanowi **załącznik nr 2** do Polityki.
7. Wzór upoważnienia do przetwarzania danych osobowych określony został w **załączniku nr 3** do niniejszej Polityki.

8. Upoważnienie przyznawane jest na czas trwania umowy o pracę lub innej umowy cywilnoprawnej chyba, że bezpośredni przełożony zadecyduje inaczej, a także na czas określonego zadania, które nierozerwalnie związane jest z przetwarzaniem danych.
9. Upoważnienie jest przyznawane przed rozpoczęciem przetwarzania danych osobowych.
10. Uprawnienia do przetwarzania danych osobowych wygasają z chwilą ustania stosunku pracy/ wygaśnięcia umowy cywilnoprawnej, porozumień lub z upływem okresu ważności upoważnienia.
11. Decyzję o cofnięciu uprawnień w okresie ich trwania podejmuje Administrator lub właściwy LADO.
12. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Inspektor Ochrony Danych.
13. Koordynator Ochrony Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w ramach poszczególnych wydziałów i pozostałych jednostek organizacyjnych badawczych, badawczo-rozwojowych, dydaktycznych oraz prowadzonych wspólnie z innymi podmiotami, określonych w Regulaminie Organizacyjnym UG.
14. Nadane upoważnienia przechowywane są w systemie informatycznym lub innej dopuszczonej formie.

3. Szkolenia w zakresie ochrony danych osobowych

§ 19.

1. Każda osoba przetwarzająca dane osobowe na UG, zobowiązana jest do zapoznania się z powszechnie obowiązującymi przepisami prawa w tym zakresie, uregulowaniami wewnętrznymi, a także stosowanymi sposobami zabezpieczenia tych danych.
2. Obowiązek, o którym mowa w ust. 1 realizowany jest poprzez szkolenie e-learningowe dostępne na portalu edukacyjnym UG. Dopuszcza się możliwość szkolenia w innej formie niż ww., w szczególności szkolenie przeprowadzane bezpośrednio przez IOD.
3. Szkolenie przeprowadza się nie rzadziej niż raz na 5 lat, a także każdorazowo w przypadku znaczących zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub w sposobach zabezpieczenia stosowanych w Uczelni.

§ 20.

1. Osoba o jakiej mowa w § 19 ust. 1 potwierdza zapoznanie się ze szkoleniem dotyczącym ogólnych zasad przetwarzania danych osobowych oraz zobowiązuje się zachować w tajemnicy dane osobowe, z którymi zetknął się w trakcie realizacji zadań w UG związanych z przetwarzaniem danych osobowych oraz sposoby ich zabezpieczenia.
2. W przypadkach przewidzianych w *Instrukcji nadawania, zmiany i odwołania uprawnień do przetwarzania danych osobowych*, dopuszcza się możliwość potwierdzenia zapoznania ze szkoleniem oraz zobowiązania się do zachowania w tajemnicy w formie tradycyjnej – papierowej, zgodnie ze wzorem określonym w **załączniku nr 4** do Polityki.
3. Oświadczenie, o którym mowa w ust. 2 otrzymuje i ewidencjonuje Inspektor Ochrony Danych w zakresie jednostek Administracji Centralnej, Koordynatorzy Ochrony Danych Osobowych w zakresie poszczególnych wydziałów/ jednostek ogólnouniwersyteckich.

4. Współpraca z osobami trzecimi.

§ 21.

1. Do przetwarzania danych osobowych mogą zostać dopuszczone osoby niebędące pracownikami Uczelni.
2. Wobec osób, o których mowa w ust. 1 przepisy od § 17 do § 20 stosuje się odpowiednio oraz zgodnie z zasadami określonymi w *Instrukcji nadawania, zmiany i odwołania uprawnień do przetwarzania danych osobowych przy pomocy systemu informatycznego ODO*.

5. Udostępnianie danych osobowych

§ 22.

1. Udostępnianie danych osobowych podmiotom lub osobom spoza Uczelni może nastąpić na podstawie rozporządzenia – w przypadkach wskazanych w art. 6 i 9 albo na podstawie regulacji zawartych w przepisach krajowych ustaw szczególnych.
2. Dane osobowe udostępniane są:
   1) na podstawie umowy lub porozumienia;
   2) na pisemny, uzasadniony wniosek, chyba że przepisy ustawy stanowią inaczej.
3. Wniosek o udostępnienie danych osobowych powinien zawierać, w szczególności następujące informacje:
   1) dane wnioskodawcy lub pełnomocnika wnioskodawcy;
   2) dane osoby, której wniosek dotyczy;
   3) zakres danych, które podlegają udostępnieniu;
   4) podstawę prawną upoważniającą do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych.
4. Wnioski o udostępnienie danych osobowych podmiotom zewnętrznym podlegają ewidencji.
5. Ewidencję wniosków, o których mowa powyżej, prowadzą wg właściwości jednostki organizacyjne wymienione w załączniku nr 11. Ewidencję prowadzi się zgodnie ze wzorem stanowiącym załącznik nr 12 do niniejszej Polityki.

6. Powierzenie przetwarzania danych osobowych

§ 23.

1. Umowa powierzenia przetwarzania danych osobowych dotyczy wyłącznie danych osobowych wynikających z realizacji umowy zasadniczej.
2. Przetwarzanie danych osobowych może zostać powierzone, w zakresie działalności prowadzonej przez UG, innemu podmiotowi, pod warunkiem zawarcia z tym podmiotem pisemnej umowy, na zasadach określonych w art. 28 rozporządzenia.
3. Zezwala się na korzystanie wyłącznie z usług takich podmiotów przetwarzających, które zobowiązują się do ochrony danych osobowych oraz zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych wskazanych w art. 32 rozporządzenia.
4. Umowa, o której mowa w ust. 1 powinna w szczególności określać:
   1) przedmiot i czas trwania przetwarzania;
   2) charakter i cel przetwarzania;
   3) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;

4) obowiązki i prawa Administratora oraz podmiotu przetwarzającego wynikające bezpośrednio z art. 28 rozporządzenia,

a także zapewniać Administratorowi możliwość kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych w podmiocie, będącym stroną umowy zarówno przed jak i w trakcie trwania umowy.

5. Umowa o powierzenie przetwarzania danych powinna zostać przed podpisaniem, przekazana do Inspektora Ochrony Danych celem zaopiniowania.
6. Jednostka organizacyjne jest zobowiązana do przekazania kopii umowy powierzenia przetwarzania danych osobowych do IOD.
7. Wzór umowy powierzenia stanowi załącznik nr 5 do niniejszej Polityki
8. W uzasadnionych przypadkach dopuszcza się zastosowanie innego wzorca umowy – pod warunkiem, iż będzie on uwzględniał elementy o jakich mowa w ust 3.

7. Współadministrowanie

§ 24.

1. Współadministrowanie odbywa się na zasadach określonych w art. 26 rozporządzenia.
2. Współadministratorzy w przejrzysty sposób muszą określić odpowiednie zakresy swojej odpowiedzialności zawierając pisemne porozumienie, w tym wypełnić obowiązki informacyjne w odniesieniu do osób, których dane przetwarzają.
3. Umowa o współadministrowaniu danych powinna zostać przed podpisaniem, przekazana do Inspektora Ochrony Danych celem zaopiniowania.
4. Jednostka organizacyjne jest zobowiązana do przekazania kopii dokumentu dot. współadministrowania danych osobowych do IOD.

8. Naruszenie ochrony danych osobowych

§ 25.

1. Wprowadza się jako obowiązującą w Uczelni „Instrukcję postępowania w przypadku naruszenia ochrony danych osobowych", stanowiącą **załącznik nr 6** do Polityki.
2. Zobowiązuje się Lokalnych Administratorów Danych Osobowych do wdrożenia niniejszej instrukcji, a następnie nadzorowania jej przestrzegania w podległych im obszarach.
3. W Uniwersytecie funkcjonuje Uczelniany zespół reagowania na incydenty ochrony danych osobowych w następującym składzie:
   1) Inspektor Ochrony Danych i/lub jego zastępca;
   2) Radca prawny Uniwersytetu Gdańskiego;
   3) Pracownik Zespołu Prasowego Centrum Komunikacji i Promocji;
   4) Głównego specjalisty ds. ryzyka;
   5) Pracownik Biura Bezpieczeństwa i Oceny Ryzyka referujący ustalenia dot. ujawnionego zdarzenia.
4. Przewodniczącym zespołu o jakim mowa w ust. 3 jest Inspektor Ochrony Danych lub jego zastępca,
5. W przypadku gdy zdarzenie dotyczy systemów teleinformatycznych członkiem zespołu o jakim mowa w ust 1 jest również Dyrektor Centrum Informatycznego lub wskazany przez niego pracownik.
6. Przewodniczący może włączyć do prac inne osoby, jeśli uzna, że są one niezbędne do realizacji zadań Zespołu.

7. W przypadku wpłynięcia do UG informacji o zdarzeniu, IOD lub osoba przez niego wskazana analizuje otrzymane informacje oraz podejmuje niezbędne czynności wyjaśniające.

9. Dopełnienie obowiązku informacyjnego

§ 26.

1. Na formularzach, kwestionariuszach oraz innych dokumentach za pomocą których zbierane są dane osobowe, niezależnie od ich formy (papierowej czy elektronicznej), umieszcza się klauzulę informacyjną lub informację o klauzuli.
2. Wzór klauzuli informacyjnej stanowi **Załącznik nr 7** do niniejszej Polityki .
3. Kierownicy jednostek, zajmujących się pozyskiwaniem danych osobowych bezpośrednio od osoby, której one dotyczą winni zadbać, aby dokumenty, o których mowa w ust. 1 posiadały aktualną klauzulę informacyjną dostosowaną do obowiązujących przepisów.

10. Nadzór nad przestrzeganiem ochrony danych osobowych

§ 27.

1. Podstawową formą nadzoru nad przestrzeganiem zasad przetwarzania i ochrony danych osobowych na Uniwersytecie Gdańskim jest bieżąca kontrola funkcjonalna realizowana przez kierowników jednostek organizacyjnych.
2. Nadzór instytucjonalny nad przestrzeganiem zasad ochrony danych osobowych przeprowadzany jest na bieżąco przez IOD, a także przez zespół powoływany przez Administratora w celu przeprowadzenia kontroli zgodności przetwarzania danych osobowych z obowiązującymi w tym zakresie przepisami prawa w wybranych jednostkach organizacyjnych Uczelni.
3. W skład zespołu, o którym mowa w ust. 2 wchodzą w szczególności następujące osoby:
   1) Inspektor Ochrony Danych i/lub jego zastępca;
   2) Dyrektor Centrum Informatycznego lub wskazana przez niego osoba.
4. Skład zespołu może zostać uzupełniony o inne osoby wskazane przez IOD.
5. Zespół realizuje swoje działania w oparciu o upoważnienie wydane przez Administratora, które określa: osoby przeprowadzające kontrolę, przedmiot oraz jej termin.
6. Planowe kontrole przeprowadza się na podstawie planu zatwierdzonego przez Administratora.
7. Nadzór o jakim mowa w pkt 2 może być realizowany w formie ankiet sprawdzających przekazywanych w formie elektronicznej.

§ 28.

1. Zespół po przeprowadzeniu czynności kontrolnych sporządza protokół kontroli.
2. Protokół kontroli powinien zawierać, w szczególności:
   1) nazwę kontrolowanej jednostki;
   2) datę rozpoczęcia i zakończenia czynności kontrolnych;
   3) skład zespołu kontrolującego;
   4) imię i nazwisko kierownika jednostki kontrolowanej lub osoby jego zastępującej;
   5) określenie przedmiotu kontroli;
   6) opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
   7) wnioski i zalecenia pokontrolne;
   8) datę i miejsce podpisania protokołu przez członków komisji oraz przez kierownika kontrolowanej jednostki lub osoby jego zastępującej.

3. Protokół podpisują członkowie zespołu i kierownik kontrolowanej jednostki lub osoba jego zastępująca.
4. Z protokołem zapoznany zostaje właściwy LADO.
5. Jednostka kontrolowana zobowiązana jest do pisemnego powiadomienia IOD o wykonaniu zaleceń pokontrolnych, w terminie nie dłuższym niż 6 miesięcy od daty podpisania protokołu.

VI. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

§ 29.

1. Inspektor Ochrony Danych prowadzi centralny rejestr czynności przetwarzania danych osobowych w Uniwersytecie Gdańskim opracowany na podstawie zgłoszeń otrzymywanych z poszczególnych jednostek organizacyjnych.
2. Rejestr, o którym mowa w ust. 1 stanowi zestawienie wszystkich podstawowych procesów i czynności związanych z przetwarzaniem danych osobowych w Uczelni. W rejestrze tym zamieszcza się następujące informacje:
   1) nazwę oraz dane kontaktowe Administratora oraz inspektora ochrony danych;
   2) cele przetwarzania;
   3) podstawę prawną przetwarzania;
   4) nazwę systemu lub oprogramowania służącego do przetwarzania danych;
   5) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
   6) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   7) transfer danych do państwa trzeciego lub organizacji międzynarodowej;
   8) planowane terminy usunięcia poszczególnych kategorii danych;
   9) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
3. Kierownicy jednostek organizacyjnych są zobowiązani do zgłaszania do IOD wszystkich czynności przetwarzania danych osobowych realizowanych w ramach podległych im jednostek, zgodnie ze wzorem określonym w **załączniku nr 8** do niniejszego dokumentu, o ile nie zostały one zgłoszone wcześniej. W przypadku przetwarzania danych osobowych w systemach informatycznych, które nie zostały wcześniej zgłoszone do danej czynności przetwarzania, wymagana jest opinia Dyrektora Centrum Informatycznego. Ocenę ryzyka, o której mowa w § 33 ust. 2, przeprowadza osoba zgłaszająca czynność przetwarzania danych do rejestru i dokumentuje zgodnie z regulacjami zawartymi w Polityce Zarządzania Ryzykiem
4. Zgłoszenie, o którym mowa w ust. 1 zatwierdza właściwy LADO.

§ 30.

1. W przypadku, gdy w ramach zawartej umowy Uczelnia staje się Podmiotem Przetwarzającym, Inspektor Ochrony Danych zobowiązany jest również do prowadzenia rejestru kategorii czynności przetwarzania dokonywanych na zlecenie innego Administratora.
2. Rejestr, o którym mowa w ust. 1 sporządza się na podstawie dostarczonych do IOD kopii umów powierzenia. Zobowiązuje się kierowników jednostek organizacyjnych do niezwłocznego przekazania do IOD wymienionych umów.
3. W rejestrze zamieszcza się w szczególności następujące informacje:
   1) nazwę oraz dane kontaktowe podmiotu przetwarzającego oraz każdego Administratora, w imieniu którego działa podmiot przetwarzający, a także Inspektora Ochrony Danych;
   2) kategorie przetwarzań dokonywanych w imieniu każdego z Administratorów;
   3) transfer danych do państwa trzeciego lub organizacji międzynarodowej;
   4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

VII. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH ORAZ ICH ZABEZPIECZENIE

§ 31.

1. Uniwersytet ustala obszar przetwarzania danych osobowych, obejmujący wszystkie pomieszczenia, w których wykonuje się jakiekolwiek operacje na danych osobowych, w szczególności wprowadzanie, modyfikowanie, archiwizowanie, usuwanie dane, a także wszystkie miejsca, gdzie przechowuje się systemy informatyczne lub nośniki informacji zawierające dane osobowe, jak szafy z dokumentacją papierową lub zawierającą elektroniczne nośniki informacji.
2. W celu zapewnienia bezpieczeństwa pracowników i studentów, ochrony mienia, dochodzenia roszczeń, zachowania tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę stosuje się wideomonitoring zgodnie z zapisami Regulaminu Pracy. Dostęp do nagrań z wideomonitoringu jest ograniczony do osób upoważnionych i wykorzystywany wyłącznie w celach bezpieczeństwa i dochodzenia roszczeń.
3. W celu ochrony obszaru przetwarzania przed dostępem osób nieuprawnionych stosuje się instalację alarmową, system kart dostępowych oraz politykę klucza, zabezpieczając w ten sposób budynki i pomieszczenia. Ewidencję poboru i zdania kluczy prowadzi Straż Uniwersytecka.

§ 32.

1. Dane osobowe przetwarza się wyłącznie w warunkach zapewniających ochronę przed dostępem osób nieuprawnionych, przy zastosowaniu wymaganych środków ochrony fizycznej oraz zachowaniu zasad bezpieczeństwa teleinformatycznego, a także z uwzględnieniem środków technicznych i organizacyjnych określonych w art. 32 rozporządzenia.
2. Dobór środków ochrony danych zależy od przeprowadzonej oceny ryzyka i powinien uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i powagę zdarzeń, które mogą doprowadzić do naruszenia praw i wolności osób, których dane są przetwarzane.
3. Aktualizacja oceny ryzyka powinna być przeprowadzona w przypadku zaistnienia istotnych zmian ale nie rzadziej niż raz na rok. Za aktualizację ryzyk odpowiada IOD.

1. Środki ochrony fizycznej

§ 33.

1. Dostęp do budynków i pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe podlega kontroli.
2. Kontrola, o której mowa w ust. 1 polega na:
   1) prowadzeniu ewidencji pobierania i zwrotu kluczy do pomieszczeń;
   2) prowadzeniu ewidencji wydawania i zdawania kart dostępowych do pomieszczeń;
   3) monitorowaniu obiektów i znajdujących się w nich pomieszczeń oraz ciągów komunikacyjnych przy pomocy systemu telewizji dozorowej, systemu elektronicznego zabezpieczenia, a także poprzez bezpośrednią obserwację prowadzoną przez pracowników i strażników Straży Uniwersyteckiej.
3. Uczelnia może wprowadzać inne formy zabezpieczenia dostępu do obszarów przetwarzania danych osobowych.

§ 34.

1. W pomieszczeniach, w których odbywa się przetwarzanie danych mogą przebywać osoby posiadające upoważnienie do przetwarzania danych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych. Przebywanie pozostałych osób w wyżej wymienionym obszarze jest dozwolone w obecności pracownika upoważnionego do przetwarzania danych osobowych, z zastrzeżeniem ust. 2.
2. Personel pomocniczy, sprzątający lub techniczny może przebywać w pomieszczeniach przetwarzania danych osobowych bez nadzoru osoby upoważnionej po podpisaniu zobowiązania do ochrony danych osobowych oraz zachowania w tajemnicy znanych im sposobów zabezpieczenia danych osobowych, zarówno w trakcie trwania zatrudnienia lub świadczenia usług na rzecz Administratora, jak również po ich ustaniu.
3. Wzór zobowiązania, o którym mowa w ust. 2 stanowi **załącznik nr 9** do Polityki.
4. Przebywanie pracowników lub innych osób w obszarze przetwarzania danych osobowych po godzinach pracy jednostki lub w dniach wolnych od pracy jest dopuszczalne po uzyskaniu zgody bezpośredniego przełożonego.

§ 35.

Pomieszczenia, w których przetwarza się dane osobowe (w szczególności takie jak pomieszczenia biurowe, centra wydruków, serwerownie itp.) powinny być zabezpieczone przed dostępem osób nieuprawnionych oraz być wyposażone w środki ochrony przeciwpożarowej.

§ 36.

1. W pomieszczeniach, w których znajduje się część ogólnodostępna będąca jednocześnie miejscem przetwarzania danych osobowych, należy oddzielić obszar przetwarzania danych od części ogólnodostępnej.
2. Wydzielenie części pomieszczenia, w której przetwarzane są dane osobowe może być realizowane w szczególności poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych, uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.

§ 37.

1. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
2. W przypadku nieobecności pracownika upoważnionego do przetwarzania danych osobowych, dokumenty należy zabezpieczyć oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiających dostęp do danych osobom niepowołanym.

§ 38.

1. Podstawowym sposobem przechowywania dokumentów zawierających dane osobowe jest ich przechowywanie w zamkniętych na klucz szafach lub innych przeznaczonych do tego celu urządzeniach biurowych.
2. Klucze do szaf lub urządzeń biurowych, w których przechowywane są dane osobowe, po zakończeniu dnia pracy zabezpiecza się przed dostępem osób nieuprawnionych.
3. Sposób przechowywania i zabezpieczenia elektronicznych nośników informacji zawierających dane osobowe zawiera Polityka bezpieczeństwa teleinformatycznego.

2. Kontrola dostępu do systemu

§ 39.

1. Każdy użytkownik posiadający upoważnienie do przetwarzania danych osobowych w systemie informatycznym otrzymuje jednoznaczny i niepowtarzalny identyfikator oraz ustala hasło.
2. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3. Sposób uwierzytelniania użytkownika w systemie informatycznym określa Polityka bezpieczeństwa teleinformatycznego.
4. Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
5. Użytkownicy systemu zobowiązani są w szczególności do:
   1) zachowania w tajemnicy loginów i haseł uwierzytelniających użytkownika w systemie do przetwarzania danych osobowych;
   2) ścisłego przestrzegania zakresu nadanego upoważnienia;
   3) zgłaszania zdarzeń związanych z naruszeniem bezpieczeństwa ochrony danych osobowych w systemie informatycznym oraz niewłaściwym funkcjonowaniem systemu przetwarzania danych.

3. Komputery przenośne i praca na odległość

§ 40.

1. Nie zaleca się wynoszenia służbowych komputerów przenośnych zawierających dane osobowe poza obszar przetwarzania danych osobowych.
2. Wynoszenie służbowych komputerów przenośnych zawierających dane osobowe poza obszar przetwarzania danych jest dopuszczalne jedynie w uzasadnionych przypadkach i pod warunkiem:
   1) właściwego ich zabezpieczenia przed dostępem osób nieuprawnionych oraz zagubieniem lub zniszczeniem;
   2) stosowania środków ochrony kryptograficznej wobec przetwarzanych danych osobowych;
   3) otrzymania zgody LADO na użytkowanie komputera przenośnego poza obszarem przetwarzania danych.
3. Zgoda, o której mowa w ust. 2 pkt 3 winna mieć formę pisemną.
4. Zabrania się udostępniania służbowych komputerów przenośnych zawierających dane osobowe osobom trzecim (domownikom, współlokatorom, itp.) oraz pozostawiania ich bez nadzoru poza obszarem przetwarzania danych, a także korzystania z nich w miejscach publicznych.
5. Osoba użytkująca służbowy komputer przenośny poza obszarem przetwarzania danych ponosi pełną odpowiedzialność za ich zabezpieczenie przed dostępem osób nieuprawnionych, a także zagubieniem lub zniszczeniem.
6. W przypadku zaistnienia warunków szczególnych (np. pandemia) istnieje możliwość pracy zdalnej z możliwością przetwarzania danych osobowych, na zasadach określonych przez Administratora, bez konieczności posiadania pisemnej zgody. Dane osobowe mogą być przetwarzane zgodnie z pkt 2 ust 1-2.
7. Zalecenia w zakresie wykonywania pracy zdalnej określa Polityka bezpieczeństwa teleinformatycznego.

4. Plany awaryjne i zapobiegawcze

§ 41.

Systemy informatyczne zabezpiecza się urządzeniami podtrzymującymi zasilanie, co umożliwia ich funkcjonowanie w przypadku awarii zasilania lub zakłóceń w sieci zasilającej.

§ 42.

1. Dane osobowe przetwarzane w systemach informatycznych zabezpiecza się przez wykonywanie kopii zapasowych oraz programów służących do ich przetwarzania, na oddzielnych serwerach.
2. Sporządzanie kopii zapasowych następuje w trybie opisanym w Polityce bezpieczeństwa teleinformatycznego
3. Nadzór nad prawidłowym wykonywaniem, przechowywaniem oraz usuwaniem kopii zapasowych sprawuje Dyrektor Centrum Informatycznego lub osoba przez niego upoważniona we współpracy z LADO.
4. Sposób, miejsce i okres przechowywania kopii zapasowych zawiera Polityka bezpieczeństwa teleinformatycznego

§ 43.

1. Systemy informatyczne służące do przetwarzania danych osobowych zabezpiecza się przed niepożądanymi atakami co najmniej poprzez:
   1) korzystanie z programów antywirusowych;
   2) stosowanie mechanizmów zabezpieczających przed nieautoryzowanym dostępem z sieci (firewall).
2. Za zastosowanie zabezpieczeń, o których mowa w ust. 1 w systemach informatycznych służących do przetwarzania danych osobowych odpowiada Dyrektor Centrum Informatycznego lub LADO, zgodnie z właściwością,

5. Usuwanie danych osobowych

§ 44.

1. Dane osobowe w postaci umożliwiającej identyfikację osób, których one dotyczą, przechowuje się nie dłużej niż zakłada to cel przetwarzania danych.
2. Po osiągnięciu celu, o którym mowa w ust. 1, przy braku szczególnych okoliczności, dane osobowe podlegają usunięciu, chyba że przepisy innych ustaw stanowią inaczej.
3. Usuwanie zbędnych danych polega w szczególności na:
   1) trwałym, fizycznym zniszczeniu danych w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod;
   2) anonimizacji danych osobowych, polegającej na pozbawieniu danych osobowych cech pozwalających na identyfikację osób fizycznych, których dane dotyczą.
4. Za odpowiednie zniszczenie danych osobowych odpowiada komisja powołana przez kierownika jednostki organizacyjnej, w której przetwarzane są dane osobowe
5. Z przebiegu usuwania danych sporządza się stosowny protokół, który stanowi **załącznik nr 10** do Polityki. Protokół zniszczenia danych osobowych podpisują wszyscy członkowie powołanej komisji.
6. Protokół, o którym mowa w ust. 5 przechowuje właściwy kierownik jednostki organizacyjnej, w której usunięto dane osobowe lub osoba przez niego upoważniona.

§ 45.

1. Dokumenty papierowe zawierające dane osobowe, niszczy się przez pocięcie w niszczarce, która zapewnia zniszczenie materiału w sposób uniemożliwiający odtworzenie jego treści.
2. Elektroniczne nośniki informacji zawierające dane osobowe, pozbawia się wcześniej zapisu tych danych w sposób nieodwracalny, a w przypadku gdy nie jest to możliwe niszczy fizycznie w sposób uniemożliwiający ich odczytanie.
3. Sposób usuwania danych z systemów informatycznych określa Polityka bezpieczeństwa teleinformatycznego.

§ 46.

1. Wprowadza się obowiązek okresowego przeglądu przetwarzanych danych osobowych pod kątem usuwania zbędnych danych.
2. Za przeprowadzenie czynności, o której mowa w ust. 1 odpowiadają kierownicy jednostek organizacyjnych – w stosunku do przetwarzanych danych osobowych w podległych im jednostkach.

6. Wymiana danych i ich bezpieczeństwo

§ 47.

Obieg dokumentów zawierających dane osobowe, winien odbywać się w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych.

§ 48.

1. Przesyłanie danych osobowych z wykorzystaniem skrzynki poczty elektronicznej powinno odbywać się wyłącznie za pośrednictwem służbowych adresów e-mail.
2. Zaleca się, o ile to możliwe, przekazywanie pocztą elektroniczną tylko jednostkowych danych, a nie całych zbiorów lub szerokich z nich wypisów.
3. Dane osobowe szczególnych kategorii oraz dane zawierające poza imieniem i nazwiskiem numer PESEL, przesyła się w postaci zaszyfrowanej. Hasło dostępu do pliku zawierającego dane osobowe przekazuje się, o ile to możliwe, innym kanałem informacyjnym w stosunku do przekazywanych plików. W uzasadnionych przypadkach można odstąpić od przesyłania danych w postaci zaszyfrowanej.
4. W celu wysłania korespondencji mailowej do wielu odbiorców jednocześnie wśród, których znajdują się adresaci, którzy z uzasadnionych przyczyn nie posiadają służbowych kont pocztowych w domenie UG, należy obowiązkowo wykorzystywać pole „UDW” (Ukryte do wiadomości) w oknie programu pocztowego zamiast domyślnego pola „DO” czy „DW” lub skorzystać z systemu do dystrybucji masowej korespondencji e-mailowej będącego w dyspozycji Dyrektora Centrum Informatycznego.

§ 49.

7. Ochrona danych w fazie projektowania oraz domyślna ochrona danych

1. W przypadku opracowywania, projektowania, dokonywania wyboru, a także w toku samego wykorzystywania usług, aplikacji czy innych produktów opierających się na przetwarzaniu danych niezbędnym jest uwzględnienie ochrony danych już w fazie projektowania (privacy by design) oraz domyślnej ochrony danych (privacy by default) przy zastosowaniu odpowiednich środków technicznych i organizacyjnych.

2. Przy tworzeniu i wdrażaniu technologii opartych na przetwarzaniu danych wymagana jest konsultacja z Inspektorem Ochrony Danych, w zakresie informatyki z Dyrektorem Centrum Informatycznego lub osobą przez niego wyznaczoną.
3. Nadzór nad realizacją zasad, o których mowa w ust. 1 powierza się Lokalnym Administratorom Danych Osobowych.

VIII. OCENA SKUTKÓW DLA OCHRONY DANYCH

§ 50.

1. Jeżeli planowana operacja przetwarzania danych - w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia prywatności osób, których dane dotyczą koniecznym jest przeprowadzenie oceny skutków dla ochrony danych.
2. Ocenę skutków, o której mowa w ust. 1 przeprowadza się w przypadkach i na zasadach określonych w art. 35 rozporządzenia.
3. W zależności od potrzeb w ocenie skutków dla ochrony danych biorą udział:
   1) Inspektor Ochrony Danych;
   2) Dyrektor Centrum Informatycznego lub osoba przez niego upoważniona;
   3) pracownicy Biura Bezpieczeństwa i Oceny Ryzyka, a także inne osoby, które uznane zostaną za pomocne w realizacji tego zadania.

IX. POSTANOWIENIA KOŃCOWE

§ 51.

1. Polityka w zakresie danych osobowych jest dokumentem wewnętrznym Uczelni i stanowi element Polityki Bezpieczeństwa Uniwersytetu Gdańskiego.
2. W sprawach nieuregulowanych w niniejszym dokumencie, mają zastosowanie przepisy rozporządzenia oraz inne akty prawne, które znajdują zastosowanie do przetwarzania danych osobowych i ochrony prywatności.

X. LISTA ZAŁĄCZNIKÓW

Załącznik nr 1 – Instrukcja nadawania, zmiany i odwołania uprawnień do przetwarzania danych osobowych

Załącznik nr 2 – Wzór wniosku o nadanie/zmianę/odwołanie uprawnień do przetwarzania danych osobowych.

Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 4 – Wzór oświadczenia osoby upoważnionej do przetwarzania danych osobowych.

Załącznik nr 5 – Wzór umowy powierzenia.

Załącznik nr 6 – Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.

Załączniki nr 7 – Wzór klauzuli informacyjnej.

Załącznik nr 8 – Wzór zgłoszenia czynności przetwarzania danych osobowych.

Załącznik nr 9 – Wzór zobowiązania do ochrony danych osobowych oraz zachowania poufności.

Załącznik nr 10 – Wzór protokołu zniszczenia danych.

Załącznik nr 11 – Wykaz jednostek organizacyjnych UG udostepniających dane osobowe wraz z zakresem udostępnienia.

Załącznik nr 12 – Wzór ewidencji wniosków o udostępnianie danych osobowych.