Polityka bezpieczeństwa przetwarzania danych osobowych

Uniwersytet Przyrodniczy w Lublinie

Spis treści

I. Wstęp

Rektor Uniwersytetu Przyrodniczego w Lublinie, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanych w związku z wykonywaniem zadań administratora danych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m. in. takim jak:

1/. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej;

2/. Niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);

3/. Awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;

4/. Podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;

5/. Celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;

6/. Ataki z Internetu;

7/. Naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:

- niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na portiernię),
- naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
- ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u administratora danych,
- ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,
- niewykonywanie stosownych kopii zapasowych,
- wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

II. Postanowienia ogólne

1. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

1/. Administratorze bezpieczeństwa informacji - rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,

2/. Administratorze danych osobowych - rozumie się przez to administratora danych - Uniwersytet Przyrodniczy w Lublinie reprezentowany przez Rektora,

3/. Administratorze systemu informatycznego - rozumie się przez to wskazanego pracownika Ośrodka Informatyki Uniwersytetu Przyrodniczego w Lublinie,

4/. Haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,

5/. Identyfikatorze - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

6/. Integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

7/. Odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
- osoby, której dane dotyczą
- osoby upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31 a ustawy,
- podmiotu, o którym mowa w art. 31 ustawy,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

8/. Osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Rektora Uniwersytetu Przyrodniczego w Lublinie,

9/. poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

10/. Przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy

11/. Raporcie - rozumie się przez to wygenerowane przez system informatyczny zestawienie zakresu i treści przetwarzanych danych,

12/. Rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

13/. Rozporządzeniu - rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024),

14/. Serwisancie - rozumie się przez to firmę zewnętrzną lub pracownika Ośrodka Informatyki zajmującego się modernizacją, instalacją, naprawą i konserwacją sprzętu komputerowego,
15/. Sieci publicznej - rozumie się przez to sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800)
16/. Sieci telekomunikacyjnej - rozumie się przez to sieć telekomunikacyjną w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800)
17/. "Systemie informatycznym administratora danych - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,"
18/. Teletransmisji - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
19/. Ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2002 r. nr 101, poz. 926 ze zm.),
20/. Uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
21/. Użytkowniku - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

2. Cel

Wdrożenie polityki bezpieczeństwa u administratora danych osobowych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym administratora danych i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

W związku z tym, że w obu zbiorach administratora danych osobowych przetwarzane są między innymi dane wrażliwe, a system informatyczny administratora danych posiada szerokopasmowe połączenie z internetem, niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3. Zakres stosowania

1/. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.
2/. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

III. Organizacja przetwarzania danych osobowych

1. Administrator Danych Osobowych

Administrator danych osobowych reprezentowany przez Rektora Uniwersytetu Przyrodniczego w Lublinie realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1/. Podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
2/. Może delegować swoje kompetencje na Kanclerza Uniwersytetu Przyrodniczego w Lublinie,
3/. Upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
4/. Wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań i czynności
5/. Wyznacza kierownika jednostki organizacyjnej jako właściwego do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
6/. Zleca każdemu kierownikowi jednostki organizacyjnej uczelni, by we współpracy z administratorem systemu informatycznego oraz administratorem bezpieczeństwa informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
7/. Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator Bezpieczeństwa Informacji

Administrator bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1/. Sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych - w celu zapewnienia bezpieczeństwa danych,
2/. Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
3/. Sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
4/. Bierze udział w wewnętrznych audytach przestrzegania przepisów o ochronie danych osobowych,
5/. Nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
6/. Prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
7/. Przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków osób upoważnianych do przetwarzania danych osobowych,
8/. Przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i organizuje szkolenia osób upoważnianych do przetwarzania danych osobowych,

9/. W porozumieniu z administratorem danych osobowych oraz kierownikiem działu personalnego na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

3. Administrator Systemu Informatycznego

Administrator systemu informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1/. Zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych i serwera z pozycji administratora,
2/. Przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3/. Na wniosek kierownika jednostki organizacyjnej przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4/. Nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5/. Podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6/. Wyrejestrowuje użytkowników na polecenie administratora danych lub kierownika jednostki organizacyjnej,
7/. Upoważniony jest do zmiany na stacjach roboczych haseł dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych,
8/. W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora bezpieczeństwa informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
9/. Prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10/. Sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
11/. Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Kierownik jednostki organizacyjnej uczelni

Kierownik jednostki organizacyjnej realizuje przede wszystkim następujące zadania w zakresie ochrony danych osobowych:

1/. Występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych,

2/. Występuje z wnioskiem do administratora systemu informatycznego o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych,
3/. Występuje z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego.

5. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

4/. Może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
5/. Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
6/. Zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
7/. Stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
8/. Korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
9/. Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Wykaz budynków wchodzących w skład obszaru przetwarzania danych osobowych w Lublinie :

- ul. Akademicka 12, 13, 15
- ul. Dobrzańskiego 3, 33, 37
- ul. Doświadczalna 44
- ul. Głęboka 28, 30, 31
- ul. Langiewicza 6 ,8, 12
- ul. Leszczyńskiego 7, 58
- ul. Skromna 8

2. Zbiory danych

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych znajduje się w posiadaniu administratora bezpieczeństwa informacji.

3. Ewidencje

W ramach struktury organizacyjnej administratora danych prowadzone są następujące ewidencje wchodzące w skład dokumentacji z zakresu ochrony danych osobowych:

1/. Kierownik jednostki organizacyjnej prowadzi ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom,
2/. Administrator systemu informatycznego prowadzi przechowywaną w kasie pancernej lub innym przeznaczonym do tego celu miejscu ewidencję haseł, identyfikatorów, komputerów przenośnych, nośników.

V. Struktura zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania danych

1. Zbiór danych „Kadry i płace"

Zbiór ten obejmuje dane byłych i obecnych pracowników oraz osób świadczących usługi na rzecz administratora danych na innej podstawie niż stosunek pracy.

Zakres pierwszy danych tego zbioru, tzn. imię i nazwisko osoby oraz jej numer telefonu, dostępny jest wytypowanym pracownikom administratora danych. Zakres drugi danych tego zbioru, tzn. imię i nazwisko osoby, jej adres, numer telefonu, wysokość wynagrodzenia, podstawowe, niezbędne do ustalenia wysokości wynagrodzenia, dane dotyczące stażu pracy, wykształcenia, urlopów i zwolnień, numer dowodu osobistego, numer konta bankowego, numer NIP i PESEL, imiona rodziców, datę i miejsce urodzenia, dostępny jest:

1/. Pracownikom działu personalnego,
2/. Pracownikom księgowości (kwestury)
3/. Upoważnionym pracownikom ośrodka informatyki

Dane tego zakresu są udostępniane przez upoważnionych pracowników kwestury dla ZUS, KRUS PFRON i Urzędom skarbowym.

Zakres trzeci danych tego zbioru obejmuje dane kadrowe (w tym wiele danych wrażliwych), tj. informacje o odbytych szkoleniach, urlopach, dokładne dane dotyczące wykształcenia, ewentualnie zainteresowań i hobby, informacje o posiadanych dzieciach, zawartych związkach małżeńskich, a także dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych zwłaszcza w wyniku badań profilaktycznych (wstępnych, okresowych i kontrolnych). Dostęp do tych danych posiadają wyłącznie upoważnieni pracownicy działu personalnego.

Dane z zakresu trzeciego mogą być udostępniane organom prowadzącym kontrolę, w tym zwłaszcza Państwowej Inspekcji Pracy i sądom powszechnym w związku z prowadzonym postępowaniem.

W systemie informatycznym administratora danych dane zbioru „Kadry i płace" są przetwarzane tylko w pierwszym i drugim zakresie. Na polecenie kierownika działu personalnego pracownicy tego działu przygotowują w edytorze tekstu teksty umów o pracę, porozumień i wypowiedzeń zmieniających, informacje o warunkach zatrudnienia, przekazywane zgodnie z art. 29 kp, zakresy obowiązków, korespondencję w sprawie zatrudnienia i wysokości zarobków. Dane te są niezwłocznie wprowadzane do odpowiednich zasobów serwera. Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora użytkownika (identyfikatora pracownika księgowości administratora danych).

Dane pierwszego i drugiego zakresu przetwarzane są za pomocą programu „SIMPLE/TETA", z którego niezbędne dane są importowane półautomatycznie do programu „Płatnik", służącego do korespondencji z Zakładem Ubezpieczeń Społecznych. Kontakt z ZUS-em odbywa się za pomocą szyfrowanego połączenia i jest uwierzytelniany corocznie zmienianym certyfikatem dostępu z przypisanym mu hasłem. Na innym komputerze przetwarzane są dane (imię i nazwisko, adres, numer rachunku) w systemie bankowości elektronicznej za pomocą programu „Home-banking" i aplikacji bankowości elektronicznej, dostępnej po połączeniu z siecią internet (on-line), w którym tworzy się przelewy wynagrodzeń. Każdorazowy przelew opatrzony jest bezpiecznym podpisem elektronicznym, składanym przez pracownika księgowości upoważnionego przez władze uczelni.

2. Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

Ze względu na fakt, że system informatyczny administratora danych połączony jest z siecią publiczną zgodnie z § 6 ust. 4 rozporządzenia zapewniony jest wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym. Wynikające z tego konsekwencje są uwzględnione w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

VI. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczności przetwarzanych danych)

1. Bezpieczeństwo osobowe - zachowanie poufności

1/. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji etycznych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
2/. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

2. Szkolenia w zakresie ochrony danych osobowych

1/. Administrator bezpieczeństwa informacji uwzględnia następujący plan szkoleń: szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
2/. Szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
3/. Przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

Tematyka szkoleń obejmuje:

- przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
- sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
- obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
- odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
- zasady i procedury określone w polityce bezpieczeństwa.

3. Strefy bezpieczeństwa

W siedzibie administratora danych wydzielono strefę bezpieczeństwa klasy I, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tej strefy wchodzą:

1/. Pomieszczenie z serwerem, w którym mogą przebywać wyłącznie pracownicy ośrodka informatyki, inne osoby upoważnione do przetwarzania tylko w towarzystwie tych pracowników, a osoby postronne nie mają dostępu,
2/. Pomieszczenie kwestury z kasą pancerną, w którym mogą przebywać pracownicy kwestury, inni użytkownicy danych tylko w towarzystwie pracowników kwestury,
3/. W strefie bezpieczeństwa klasy II do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych.

4. Zabezpieczenie sprzętu

1/. Serwery są zlokalizowane w odrębnym, klimatyzowanym pomieszczeniu, zamykanym drzwiami antywłamaniowymi. Okno tego pomieszczenia jest zabezpieczone. W pokoju mogą przebywać wyłącznie pracownicy ośrodka informatyki, inne osoby upoważnione do przetwarzania tylko w ich towarzystwie, a osoby postronne nie mają dostępu.
2/. Pracownicy Ośrodka Informatyki wskazują użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:
   - ochronę nośników przenośnych - w tym także nośników danych, na których przechowywane są kopie zapasowe,
   - prawidłową lokalizację komputerów.
3/. Wszystkie urządzenia systemu informatycznego administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).
4/. Okablowanie sieciowe (strukturalne) zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.
5/. Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do przetwarzania danych prowadzona jest tylko przez jego pracowników, przede wszystkim zatrudnionych w ośrodku informatyki. Natomiast poważne naprawy wykonywane przez personel zewnętrznych podmiotów realizowane są w siedzibie administratora danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.
6/. Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych.
7/. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez administratora bezpieczeństwa informacji.

5. Zabezpieczenia we własnym zakresie

Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1/. Ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
2/. Niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;
3/. Dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);

4/. Niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
5/. Pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych;
6/. Kasowania po wykorzystaniu danych na dyskach przenośnych;
7/. Nieużywania powtórnie dokumentów zadrukowanych jednostronnie;
8/. Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku i niepozostawianie w miejscu widocznym;
9/. Powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet, gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
10/. Przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;
11/. Opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
12/. Kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;
13/. Udostępniania danych osobowych pocztą elektroniczną;
14/. Niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
15/. Wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
16/. Kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie zasilającej;
17/. Niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
18/. Niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
19/. Zachowania tajemnicy danych, w tym także wobec najbliższych;
20/. Chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
21/. Umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
22/. Zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

23/. Zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
24/. Zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza na portierni. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym administratora budynku, który zgłasza firmie sprzątającej lub własnym pracownikom jednorazową rezygnację z wykonania usługi sprzątania. W takim przypadku także należy zostawić klucz na portierni.

6. Postępowanie z nośnikami pamięci i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1/. Dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM, pendrive) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;
2/. Uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;
3/. Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;
4/. Po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

7. Wymiana danych i ich bezpieczeństwo

1/. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to - przynajmniej w pewnym stopniu - uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego administratora danych.
2/. Sporządzanie kopii zapasowych następuje w trybie opisanym w pkt. 9 instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3/. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora bezpieczeństwa informacji oraz w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
4/. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w

porozumieniu z administratorem bezpieczeństwa informacji. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa informacji lub pracowników działu informatyki oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

5/. Administrator systemu w porozumieniu z administratorem bezpieczeństwa informacji dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

6/. Należy stosować następujące sposoby kryptograficznej ochrony danych: przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https:// (technologia SSL)

8. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu lub z jego upoważnienia inny pracownik ośrodka informatyki po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek kierownika działu personalnego, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.

W razie potrzeby, po uzyskaniu uprzedniej akceptacji administratora bezpieczeństwa informacji, administrator systemu lub z jego upoważnienia inny pracownik ośrodek informatyki może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.

Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora bezpieczeństwa informacji po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji i pracowników ośrodka informatyki.

9. Kontrola dostępu do sieci

1/. System informatyczny posiada szerokopasmowe połączenie z Internetem. Dostęp do niego jest jednak ograniczony do zarejestrowanych służbowych komputerów.

2/. Administrator danych wykorzystuje centralne i lokalne zapory sieciowe w celu separacji wewnętrznych lokalnych (fizycznych i wirtualnych) sieci od sieci publicznej.

3/. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.
4/. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie pracownik działu kwestury, upoważniony przez władze uczelni, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

10. Komputery przenośne i praca na odległość (zdalna)

1/. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby uczelni nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach, stosowanie własnych charakterystycznych toreb na laptopy nie jest dopuszczalne.
2/. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.
3/. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.
4/. Wykorzystywanie służbowych komputerów przenośnych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.
5/. W domu niedozwolone jest udostępnianie domownikom służbowego komputera przenośnego. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na służbowym komputerze przenośnym.
6/. Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia służbowego komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:
   - postępowania w razie nieobecności w pracy dłuższej niż 5 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji i uzgodnić z nim zwrot komputera przenośnego administratorowi danych;
   - zwrotu sprzętu w razie rozwiązania umowy o pracę w uczelni.
7/. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

11. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy)

1/. Administrator Bezpieczeństwa Informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania.

Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza kierownicy jednostek organizacyjnych, są obowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

2/. Administrator Bezpieczeństwa Informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.

3/. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora bezpieczeństwa informacji i kierownika jednostki, w której usunięto dane osobowe.

4/. Wzory dokumentów przewidujących powiadomienie, o którym mowa w art. 24 lub 25 ustawy, mogą być stosowane po zaakceptowaniu przez administratora bezpieczeństwa informacji.

12. Udostępnianie danych osobowych

Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie po złożeniu wypełnionego wniosku, którego wzór został ustalony w załączniku nr 1 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.

1/. Udostępnianie danych osobowych na podstawie ustaw szczególnych - udostępnianie informacji Policji

1.1/. Udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:

- oznaczenie wnioskodawcy,
- wskazanie przepisów uprawniających do dostępu do informacji,
- określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,

1.2/. Wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

1.3/. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

1.4/. Osoba udostępniająca dane osobowe jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu

w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.

1.5/. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

1.6/. Jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępnienia informacji.

13. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

1/. Stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
2/. Niezabezpieczenia nośnika lub komputera przenośnego,
3/. Zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

VII. Przegląd polityki bezpieczeństwa i audyt systemu

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1/. Zmian w budowie systemu informatycznego,
2/. Zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
3/. Zmian w obowiązującym prawie.

Administrator bezpieczeństwa informacji po uzgodnieniu z władzami uczelni może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu informatycznego. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji, jak i administratora systemu informatycznego.

Rektor, biorąc pod uwagę wnioski administratora bezpieczeństwa informacji, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot lub eksperta.

VIII. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

Każdej osobie upoważnionej do przetwarzania danych administrator bezpieczeństwa informacji przekazuje wyciąg z polityki bezpieczeństwa, a użytkownikom dodatkowo z instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, przygotowany z uwzględnieniem stanowiska tej osoby (obowiązków).