Państwowa Wyższa Szkoła Zawodowa
w Głogowie
ul. Piotra Skargi 5, 67-200 Głogów

POLITYKA BEZPIECZEŃSTWA

Dział Informatyzacji i Dokumentacji Multimedialnej
PWSZ w Głogowie

Spis treści

1. Wstęp

Władze Państwowej Wyższej Szkoły Zawodowej w Głogowie świadome 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,
- przetwarzanie danych osobowych w celach prywatnych,
- wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

2. Postanowienia ogólne

2.1. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

1. **administratorze danych** – rozumie się przez to administratora danych Państwowej Wyższej Szkoły Zawodowej w Głogowie, reprezentowanej przez Rektora Uczelni,
2. **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji reprezentowaną przez Administratora Sieci mgr inż. Roberta Zybaczyńskiego,
3. **administratorze systemu** – rozumie się przez to pracownika Działu Informatyzacji i Dokumentacji Multimedialnej reprezentowanego przez mgr inż. Pawła Zybaczyńskiego,
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. 31a 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 Uczelni na piśmie,
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 przygotowane przez system informatyczny zestawienia 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 (Dz. U. nr 100, poz. 1024),
14. **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. nr 171, poz. 1800 ze zm.),
15. **publicznej sieci telekomunikacyjnej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. nr 171, poz. 1800 ze zm.),
16. **serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,
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. Dz. U. 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.

2.2. Cel

Wdrożenie polityki bezpieczeństwa u administratora danych 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 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.

2.3. 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.

3. Organizacja przetwarzania danych osobowych

3.1. Administrator danych osobowych

Administrator danych osobowych reprezentowany przez Rektora Uczelni 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. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
3. wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań i czynności;
4. wyznacza pracownika Działu Osobowego 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;
5. zleca kierownikowi Działu Gospodarczo-Technicznego, by we współpracy z administratorem systemu oraz administratorem bezpieczeństwa informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
6. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

3.2. 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. sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
3. koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych,
4. nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
5. przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem,
6. zatwierdza wzory dokumentów (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne administratora danych,
7. nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych przez pracownika Działu Osobowego,
8. prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
9. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,
10. przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków osób upoważnianych do przetwarzania danych osobowych,
11. przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych,

3.3. Administrator systemu

Administrator systemu 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 z pozycji administratora,
2. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

3. na wniosek pracownika Działu Osobowego 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 pracownika Działu Osobowego,
7. zmienia w poszczególnych stacjach roboczych hasła 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.

3.4. Pracownik Działu Osobowego

Pracownik działu osobowego realizuje przede wszystkim następujące zadania w zakresie ochrony danych osobowych:

1. prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych, **Załącznik nr 3.**
3. występuje z wnioskiem do administratora danych o zmianie obowiązków pracownika upoważnionego do przetwarzania danych osobowych, **Załącznik nr 4.**
4. przekazuje informacje do administratora systemu o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych.
5. przekazuje informacje do administratora systemu o zablokowaniu i wyrejestrowaniu użytkownika z systemu informatycznego.
6. występuje z wnioskiem o odwołanie upoważnienia do przetwarzania danych osobowych, **Załącznik nr 5.**

3.5. Osoba upoważniona do przetwarzania danych osobowych

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

1. 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;
2. 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;
3. zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4. stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

5. korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
6. zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

4. Infrastruktura przetwarzania danych osobowych

4.1. Obszar przetwarzania danych osobowych

Tabela 1. Wykazu budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych:

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych	
Adres: ul. Piotra Skargi 5, 67-200 Głogów	Pomieszczenia: – piwnica serwerownia główna – parter, numery pokojów: 004, 005,015, 009 – I piętro, numery pokojów: 116, 118, 119, 122 – II piętro, numery pokojów: 221,215, 215A, 215B, 215C – III piętro, numery pokojów: 321

4.2. Zbiory danych

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zlokalizowanych w Głogowie przy ul. Piotra Skargi 5				
Lp.	Zbiór danych	Programy zastosowane do przetwarzania / Nazwa zasobu*	Lokalizacja zbioru/zasobu	Miejsce przetwarzania danych
Kwestura				
1.	„Kadr Płace''	Płatnik	Piwnica - serwerownia	I piętro – pokój 116 I piętro – pokój 118
2.	„Kadry Płace''	Symfonia Premium	Piwnica - serwerownia	I piętro – pokój 118
3.	„Finanse i Księgowość''	Symfonia Premium	Piwnica - serwerownia	I piętro – pokój 116 I piętro – pokój

				118
4.	System obsługi płatności masowych studentów	EORDO	Piwnica - serwerownia	I piętro – pokój 116
5.	VULCAN	Płace	Piwnica - serwerownia	I piętro – pokój 118
Dział Osobowy				
6.	„Kadry Płace''	Symfonia Premium	Piwnica - serwerownia	III piętro – pokój 321
7.	Akta osobowe	Forma papierowa	III piętro – pokój 321	III piętro – pokój 321
Dział Organizacji Nauczania				
8.	System obsługi studenta	EORDO	Piwnica - serwerownia	II piętro – pokój 221
9.	Harmonogramy obron	Excel oraz forma papierowa	II piętro – pokój 221	II piętro – pokój 221
Dziekanat				
10.	System obsługi studenta	EORDO	Piwnica - serwerownia	parter – pokój 009
11.	Album studenta	Forma papierowa	parter – pokój 009	parter – pokój 009
Biuro Projektów				
12.	Dane uczestników projektu	PEFS- Excel	pater – pokój 005	pater – pokój 005
13.	Dane uczestników projektu	Forma papierowa	pater – pokój 005	pater – pokój 005
14.	Deklaracje zgłoszeń do projektu	Forma papierowa	pater – pokój 005	pater – pokój 005
Dział Informatyzacji i Dokumentacji Multimedialnej				
15.	Oświadczenia studentów z dostępem do sieci WI-FI	Oświadczenia w formie papierowej	I piętro – pokój 122	I pietro – pokój 122
16.	Użytkownicy sieci WI-FI	Serwer INTRUX	Piwnica - serwerownia	I pietro – pokój 122
17.	System obsługi studenta	EORDO	Piwnica - serwerownia	I piętro – pokój 122
Biblioteka Uczelniana				
18.	System obsługi studenta - wypożyczalnia	LIBRA	Piwnica - serwerownia	pater – pokój 015

19.	Szkolenia biblioteczne	Excel	pater – pokój 015	pater – pokój 015
Dział Gospodarczo-Techniczny				
20.	Harmonogramy	Excel	I piętro – pokój 119	I piętro – pokój 119
Sekretariat Dyrektorów Instytutów				
21.	Listy pracowników dla Dyrektorów Instytutów	Excel	I I piętro – pokój 215, 215A, 215B, 215C	I I piętro – pokój 215, 215A, 215B, 215C
22.	Listy studentów dla Dyrektorów Instytutów	Excel	I I piętro – pokój 215, 215A, 215B, 215C	I I piętro – pokój 215, 215A, 215B, 215C

4.3. System informatyczny

System informatyczny administratora danych obsługiwany jest przez trzy serwery zlokalizowane w serwerowni z wydzieloną bezpieczną siecią LAN. System ten ma bezpieczne połączenie z Internetem, który jest zarządzany przez nowoczesny system INTRUX. W systemie informatycznym przetwarzane są dane z następujących komórek:

- Kwestury,
- Działu Organizacji Nauczania,
- Działu Osobowego,
- Dziekanatu,
- Biura Projektów,
- Działu Informatyzacji i Dokumentacji Multimedialnej,
- Biblioteki Uczelnianej,
- Działu Gospodarczo-Technicznego,
- Sekretariatu Dyrektorów Instytutów.

Poszczególne stacje robocze są zlokalizowane na:

1. parterze – numery pokojów: 004, 005, 022, 009
2. I piętrze – numery pokojów: 116, 118, 119, 122

3. II piętrze – numery pokojów: 221,215, 215A, 215B, 215C
4. III piętrze – numery pokojów: 321

4.4. Ewidencje

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

1. Pracownik Działu Osobowego prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
2. administrator bezpieczeństwa informacji prowadzi ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom,
3. administrator systemu prowadzi ewidencję haseł do stanowisk roboczych poszczególnych użytkowników oraz ich identyfikatorów, a także ewidencje: komputerów przenośnych, nośników przenośnych oraz kluczy kryptograficznych.

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

5.1. Zbiór danych Kwestury oraz Działu Osobowego

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

Pierwszy zakres 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. upoważnionemu pracownikowi Działu Osobowego,
2. pracownikom Kwestury.

Dane tego zakresu są udostępniane przez upoważnionych pracowników księgowości ZUS-owi i urzędom skarbowym.

Zakres drugi 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:

1. Rektor Uczelni oraz
2. pracownicy Działu Osobowego.

Dane z zakresu drugiego 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 są przetwarzane tylko w pierwszym i drugim zakresie. Na polecenie upoważnionego pracownika Działu Osobowego pracownicy tego działu przygotowują w programie „Edytor 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.

Dane pierwszego i drugiego zakresu przetwarzane są za pomocą programu „Płace", 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 poczty elektronicznej i jest uwierzytelniany corocznie zmienianym certyfikatem dostępu z przypisanym mu hasłem. Na tym samym komputerze przetwarzane są dane (imię i nazwisko, adres, numer rachunku) w systemie bankowości elektronicznej za pomocą programu „Przeglądarka" i aplikacji „Bankowość", dostępnej po połączeniu z siecią internet (on-line), w którym tworzy się przelewy wynagrodzeń. Każdorazowy przelew opatrzony jest bezpiecznym podpisem elektronicznym, składanym przez Kwestora lub Rektora Uczelni.

5.2. Zbiór danych systemu dziekanatowego

Architektura programu EORDO pozwala pracować na wielu stanowiskach równocześnie. EORDO dba o to aby dane nigdy nie straciły spójności nawet w przypadku równoczesnej edycji tych samych danych na dwóch stanowiskach. EORDO oferuje wysoką wydajność oraz bardzo bogate możliwości konfiguracji pozwalające na dostosowanie systemu do indywidualnych potrzeb uczelni.

Transmisja danych pomiędzy poszczególnymi warstwami systemu jest szyfrowana i kompresowana. Administrator programu EORDO może włączyć mechanizm wymuszający stosowanie tylko silnych haseł przez użytkowników systemu oraz może określić, jak często hasła muszą być zmieniane. Wszelkie modyfikacje w bazie danych są logowane dzięki czemu można kontrolować przebieg i źródło zmian.

W systemie są gromadzone wszystkie dane osobowe niezbędne do prowadzanie i obsługi

Moduł finansowy

- system płatności masowych - generowanie kont wirtualnych dla studentów i kandydatów, importowanie elektronicznych wyciągów bankowych, zaawansowana obsługa zobowiązań studentów, obsługa płatności w ratach, generowanie faktur, naliczanie odsetek,
- wydruki raportów finansowych,
- automatyczne przygotowywanie list stypendialnych,
- naliczanie stypendiów w oparciu o system konfigurowalnych wtyczek uwzględnianie dochodów i średnich studentów,
- generowanie plików poleceń przelewów do systemów bankowych.

Obsługa procesu dydaktycznego

- lista kursów na poszczególnych wydziałach, kierunkach,
- lista prowadzonych zajęć w poszczególnych semestrach,
- lista budynków i sal w których odbywają się zajęcia,
- obsługa grup studenckich oraz zbiorów grup studenckich,
- obsługa bloków kursów (np. blok językowy)
- zaawansowana obsługa ramówek programowych,
- możliwość przydzielania grupom studentów czasu zezwolenia na zapisy,

- zaawansowane wydruki: suplementy, karty osiągnięć, protokoły egzaminacyjne, dzienniki studenta i wiele innych.

5.3. Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

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

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

6.1. Bezpieczeństwo osobowe

Zachowanie poufności

1. Administrator danych przeprowadza nabór na wolne stanowiska w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
2. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.
3. 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.

Szkolenia w zakresie ochrony danych osobowych

1. Administrator bezpieczeństwa informacji uwzględnia następujący plan szkoleń:

a) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
b) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
c) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

2. Tematyka szkoleń obejmuje:
   a) przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
   b) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
   c) obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
   d) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych,
   e) zasady i procedury określone w polityce bezpieczeństwa.

6.2. 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. Serwerownia w której mogą przebywać wyłącznie pracownicy Działu Informatyzacji i Dokumentacji Multimedialnej, inne osoby upoważnione do przetwarzania tylko w towarzystwie tych pracowników, a osoby postronne w ogóle nie mają dostępu; złożony na portierni klucz do tego pomieszczenia jest przechowywany w woreczku zalakowanym referentką;
2. 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.

6.3. Zabezpieczenie sprzętu

1. Serwery są zlokalizowane w odrębnym, klimatyzowanym pomieszczeniu, zamykanym drzwiami antywłamaniowymi z kontrolą dostępu, systemem pożarowym, włamaniowym oraz zalania. W serwerowni mogą przebywać wyłącznie pracownicy Działu Informatyzacji i Dokumentacji Multimedialnej, inne osoby upoważnione do przetwarzania tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu.
2. Pracownicy Działu Informatyzacji i Dokumentacji Multimedialnej 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 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 dziale informatyki. Natomiast poważne naprawy wykonywane przez personel zewnętrzny 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. Na stacjach roboczych całej sieci uczelnianej jest zainstalowany e-Agent systemu E- Audytor nowej generacji zaprojektowanym z wykorzystaniem najnowszych technologii w sposób kompleksowy i elastyczny z uwzględnieniem pełnego spektrum aspektów związanych z zarządzaniem zasobami informatycznymi: sprzęt, oprogramowanie, pliki, licencje, serwis i konserwacja, upgrade sprzętu i oprogramowania, planowanie i rozliczanie. System umożliwia monitoring wydruków, kompleksowe zarządzanie majątkiem IT, zdalną kontrolę stanowisk (eRemoteDesktop), dysponowanie instalacjami czy konfiguracjami (Task Server), automatyzację procesów administracyjnych i wiele innych.

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.

6.4. 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;
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 tylko w postaci zaszyfrowanej;
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;

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.

6.5. Postępowanie z nośnikami 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) 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.

6.6. 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 7 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 „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
4. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie.
5. 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.

6. 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.
7. Należy stosować następujące sposoby kryptograficznej ochrony danych:
   - przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się POP – tunelowanie, szyfrowanie połączenia,
   - przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https://.

6.7. 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 Działu Informatyzacji i Dokumentacji Multimedialnej po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych przez pracownika Działu Osobowego, 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 Działu Informatyzacji i Dokumentacji Multimedialnej 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 Działu Informatyzacji i Dokumentacji Multimedialnej.

6.8. Kontrola dostępu do sieci

1. System informatyczny posiada szerokopasmowe połączenie z Internetem. Dostęp do niego jest jednak ograniczony. Na poszczególnych stacjach roboczych można przeglądać tylko wyznaczone strony www.
2. Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od publicznej sieci telekomunikacyjnej.
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 Kwestury, upoważniony przez Rektora Uczelni, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

6.9. Komputery przenośne i praca na odległość

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych 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 komputerów przenośnych administratora danych 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 komputera przenośnego należącego do administratora danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych.
6. Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia 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 zakończenia pracy u administratora danych.
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.

6.10. Monitorowanie dostępu do systemu i jego użycia

System informatyczny administratora danych śledzi, kto, kiedy i jakie programy uruchamia na poszczególnych stacjach roboczych. Ponadto system ten zapewnia odnotowanie:

1. daty pierwszego wprowadzenia danych do systemu,

2. identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
3. źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą,
4. informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,
5. sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

6.11. Przeglądy okresowe

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 poszczególnych działów, 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.

6.12. Udostępnianie danych osobowych

Udostępnianie danych osobowych na podstawie ustawy

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 dnia 22 kwietnia 2004 r. w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Załącznik nr 6 do niniejszej Polityki Bezpieczeństwa)

Udostępnianie danych osobowych na podstawie ustaw szczególnych

- Udostępnianie informacji Policji

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,
   - wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
2. 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.
3. 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.
4. 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.
5. 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.

6.13. 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, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy. 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.

7. Przeglądy polityki bezpieczeństwa i audyty 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 Rektorem 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. Zakres, przebieg i rezultaty

audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji, jak i kierownika Działu Informatyzacji i Dokumentacji Multimedialnej.

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

8. 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).