Załącznik Nr 1 do Zarządzenia Nr 27/2018
Rektora z dnia 24 maja 2018 r.

Polityka ochrony danych osobowych w WSPiA Rzeszowskiej Szkole Wyższej

I. Postanowienia ogólne

§ 1

1. WSPiA Rzeszowska Szkoła Wyższa (zwana dalej „Uczelnią"), w ramach realizacji celów statutowych oraz innych celów wynikających z przepisów prawa przetwarza dane osobowe osób fizycznych.
2. Uczelnia jest Administratorem danych osobowych w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE z 2016 roku, nr L 119, poz. 1), dalej „Rozporządzenie" lub „RODO". Administratora danych osobowych reprezentuje Rektor.
3. Uczelnia może występować także w roli współadministratora lub podmiotu przetwarzającego dane osobowe – na zasadach wynikających z RODO.
4. Niniejsza Polityka ochrony danych osobowych w WSPiA Rzeszowskiej Szkole Wyższej, zwana „Polityką ochrony", opracowana została na podstawie przepisów RODO, spełniając wymagane prawem obowiązki w zakresie zapewnienia właściwej ochrony danych osobowych osób fizycznych przetwarzanych w Uczelni, jako Administratora danych osobowych.
5. Niniejsza Polityka bezpieczeństwa przetwarzania danych jest dokumentem określającym zasady postępowania, stosowane środki techniczne i rozwiązania organizacyjne mające na celu zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Uczelni.
6. Czynności w zakresie ochrony danych osobowych wykonuje Rektor Uczelni na podstawie obowiązujących przepisów prawa, w szczególności RODO oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U., poz. 1000).
7. Rektor, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wprowadza zasady postępowania w zakresie ochrony danych osobowych oraz wdraża odpowiednie środki techniczne i rozwiązania organizacyjne zapewniające zgodne z prawem przetwarzanie tych danych, a tym samym właściwą ich ochronę oraz zapobiegające zagrożeniom związanym z przetwarzaniem danych osobowych.

§ 2

Zasady i procedury określone w niniejszej Polityce ochrony obowiązują także przy przetwarzaniu danych osobowych w związku z realizacją w Uczelni projektów współfinansowanych ze źródeł zewnętrznych.

§ 3

Pojęcia używane w Polityce ochrony definiowane są następująco:

1) **dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania – bezpośrednio lub pośrednio – osobie fizycznej, w szczególności imię i nazwisko, umożliwiający zidentyfikowanie numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
2) **dane** – dane osobowe, chyba że z kontekstu wynika coś innego;
3) **szczególne kategorie danych osobowych (dane wrażliwe)** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
4) **dane biometryczne** – dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
5) **dane osobowe dzieci** – dane osób poniżej 16. roku życia;
6) **przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
7) **ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
8) **pseudoanimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
9) **profilowanie** – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy

lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

10) **zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie;
11) **bezpieczeństwo danych** – proces ciągłego zapewniania bezpieczeństwa rozumiany jako zespół działań podejmowany przez Uczelnie w celu zapewnienia poufności, integralności, dostępności przetwarzanych danych osobowych i obrony przed zagrożeniami;
12) **Administrator danych osobowych (Administrator, ADO)** – WSPiA Rzeszowska Szkoła Wyższa– w zakresie, w jakim samodzielnie lub wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych, reprezentowany przez Rektora Uczelni;
13) **Lokalny administrator danych osobowych (LAD)** – osoba wyznaczona przez Administratora danych osobowych, odpowiedzialna za koordynowanie, realizację i nadzorowanie zasad postępowania przy przetwarzaniu danych osobowych w jednostkach organizacyjnych Uczelni;
14) **Inspektor ochrony danych (IOD)** – osoba, której Administrator danych osobowych, powierzył pełnienie obowiązków w zakresie monitorowania przestrzegania przepisów prawa dotyczących ochrony danych osobowych oraz inne zadania określone przepisami Polityki w zakresie danych osobowych;
15) **Administrator systemu informatycznego (Administrator systemu, ASI)** – pracownik obsługujący systemy informatyczne, odpowiedzialny za eksploatację systemu;
16) **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
17) **odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z powszechnie obowiązującymi przepisami prawa i które przetwarzają te dane zgodnie z przepisami prawa powszechnie obowiązującego dotyczącymi ochrony danych osobowych;
18) **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający lub osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe;
19) **osoba upoważniona do przetwarzania danych osobowych** – osoba, która została upoważniona przez Administratora danych osobowych/Lokalnego administratora danych osobowych do przetwarzania danych osobowych;
20) **zgoda** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

21) **naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
22) **system informatyczny Administratora danych** – sprzęt komputerowy, oprogramowanie i 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;
23) **użytkownik** – osoba upoważniona do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
24) **identyfikator** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
25) **Rejestr** – zestawienie informacji, których zakres zależny jest od celu prowadzenia danego rejestru, w miarę potrzeb aktualizowanych.

§ 4

1. Uczelnia zapewnia ochronę danych osobowych, przestrzegając następujących zasad przetwarzania tych danych:
   1) w oparciu o podstawę prawną i zgodnie z prawem, przede wszystkim zgodnie z RODO (zasada legalizmu);
   2) w sposób rzetelny i uczciwy (zasada rzetelności);
   3) w sposób przejrzysty dla osoby, której dane dotyczą, z uwzględnieniem czytelnej i zrozumiałej komunikacji z podmiotem danych (zasada transparentności);
   4) w konkretnych celach i nie na „zapas" (zasada celowości), co oznacza, że zbieranie danych osobowych jest dokonywane dla oznaczonych, zgodnych z prawem celów i niepoddawane jest dalszemu przetwarzaniu niezgodnemu z tymi celami;
   5) nie więcej niż potrzeba dla realizacji danego celu (zasada minimalizacji danych/adekwatności), co oznacza, że dane są adekwatne, stosowne i ograniczone do tego, co niezbędne dla celów, dla których są przetwarzane;
   6) z dbałością o prawidłowość danych (zasada prawidłowości/poprawności), co oznacza, że przetwarzane dane są aktualne i zgodne prawdą;
   7) nie dłużej niż potrzeba (zasada czasowości), co oznacza, że dane są przechowywane w formie umożliwiającej identyfikację osoby której dotyczą, przez okres nie dłuższy, niż jest to niezbędne dla celów, w których dane te są przetwarzane;
   8) w sposób zapewniający integralność i poufność danych (zasada bezpieczeństwa), co oznacza, że dane te nie są ani przypadkowo ani celowo zmieniane, a osoby niepowołane nie poznają danych osobowych.

2. Uczelnia zapewnia jak najszerszą ochronę szczególnych kategorii danych osobowych. Dane te mogą być przetwarzane tylko w sytuacji, gdy spełniony jest jeden z warunków określonych w art. 9 ust. 2 RODO.
3. Zapewnieniu bezpieczeństwa przetwarzania danych osobowych i realizacji zasad Polityki bezpieczeństwa w Uczelni służą systemowe rozwiązania, na które składają się:
   1) szkolenia obejmujące problematykę przetwarzania danych osobowych i zasad ich ochrony;
   2) szacunkowa ocena ryzyka związanego z zapewnieniem bezpieczeństwa danych osobowych;
   3) dobór środków technicznych i rozwiązań organizacyjnych odpowiednich do zagrożeń i kategorii danych objętych ochroną;
   4) prowadzenie monitoringu skuteczności stosowanych zabezpieczeń w zakresie ochrony danych osobowych.

§ 5

Polityka ochrony odnosi się do danych osobowych przetwarzanych w:
1) tradycyjnych zbiorach danych tj. na papierowych nośnikach danych (np.: wykazy, ewidencje, listy, kartoteki, księgi, itp.),
2) systemach informatycznych i na nośnikach cyfrowych, w tym przenośnych.

§ 6

Wszyscy pracownicy Uczelni, niezależnie od podstawy prawnej zatrudnienia, zobowiązani są do przestrzegania zasad ochrony danych osobowych określonych w Polityce ochrony oraz zgłaszania Inspektorowi ochrony danych zauważonych nieprawidłowości lub naruszeń (np. porzucenie wydruków zawierających dane osobowe, pozostawienie niezabezpieczonych akt zawierających dane osobowe, nieuprawniony dostęp do systemu elektronicznego, w którym przetwarzane są dane osobowe, niezabezpieczenie pomieszczeń, szaf zawierających akta osobowe itp.).

II. Podstawa prawna przetwarzania danych osobowych w Uczelni

§ 7

1. Podstawę prawną przetwarzania danych osobowych w Uczelni stanowi art. 6 ust.1 RODO.
2. Zgodnie z powołanym w ust. 1 przepisem, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z poniższych warunków:
   1) osoba której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby której dane dotyczą lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby której dane dotyczą, wymagające ochrony danych osobowych w szczególności, gdy osoba której dane dotyczą jest dzieckiem.

§ 8

1. Zgoda może zostać uznana za przesłankę legalizującą przetwarzanie danych osobowych jeżeli spełnione są następujące warunki jej udzielenia tj.:
   1) dobrowolność – możliwość realnego wyboru udzielenia zgody lub odmowy udzielenia bez negatywnych konsekwencji dla podmiotu, którego dane mają być przetwarzane;
   2) konkretność – zgoda musi precyzyjnie określać cel przetwarzania danych;
   3) świadomość – konieczne jest zapewnienie osobie, której dane mają być przetwarzane niezbędnych informacji aby mogła zrozumieć na co wyraża zgodę i podjąć świadomą decyzję w tym względzie;
   4) jednoznaczność – zgoda wymaga jednoznacznego okazania w formie oświadczenia lub wyraźnego działania potwierdzającego jej udzielenie.
2. Zgoda powinna być wyrażona na piśmie, pod rygorem nieważności.
3. Uczelnia, organizując konferencje lub inne wydarzenia, może przetwarzać dane osobowe uczestników tylko na podstawie pisemnego oświadczenia o udzieleniu zgody na przetwarzanie danych osobowych od osób których dane osobowe będą przetwarzane dla celów organizacji konferencji lub innego wydarzenia. Obowiązek uzyskania takich oświadczeń spoczywa na pracowniku Uczelni odpowiedzialnym za organizację konferencji lub innego wydarzenia.
4. Rekrutacja osób (pracowników, studentów, innych osób fizycznych) do uczestnictwa w projektach współfinansowanych ze źródeł zewnętrznych odbywa się wyłącznie na podstawie zgody udzielonej przez te osoby.
5. Korzystanie przez osoby fizyczne z innych usług świadczonych przez Uczelnię (np. doradztwa w ramach Kliniki Prawa) odbywa się wyłącznie na podstawie zgody udzielonej przez te osoby.
6. Zamieszczanie danych biometrycznych w postaci wizerunku osób na stronach internetowych należących do Uczelni lub w materiałach promocyjnych, folderach reklamowych Uczelni wymaga uzyskania pisemnej zgody na przetwarzanie danych, zawierającej wyraźne oświadczenie o wyrażeniu zgody na korzystanie z wizerunku, jego publikację oraz przetwarzanie danych biometrycznych osoby, której zgoda dotyczy.

7. Nie ma obowiązku uzyskania zgody na publikację wizerunku osób powszechnie znanych w związku z pełnieniem przez nich funkcji publicznych, w szczególności politycznych, społecznych, zawodowych.
8. Nie ma obowiązku uzyskania zgody na publikację wizerunku osoby stanowiącej jedynie szczegół całości, takiej jak: zgromadzenie, krajobraz, publiczna impreza.
9. Zgoda, o której mowa w ust. 1 oraz ust. 3 – 5, może zostać w każdym czasie odwołana.
10. Wzór oświadczenia w sprawie udzielenia zgody na przetwarzanie danych osobowych jest opracowywany przez IOD odrębnie dla każdego zdarzenia, z uwzględnieniem jego specyfiki, determinującej zakres czynności i celów przetwarzania danych.
11. Pisemne oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych przechowuje – w dokumentacji sprawy, której zgoda dotyczy – osoba przetwarzająca dane na jej podstawie.

§ 9

1. Podstawa przetwarzania danych, o której mowa w § 7 ust. 2 pkt 2 Polityki ochrony, przewiduje następujące sytuacje:
   1) gdy przetwarzanie danych jest niezbędne do wykonania umowy lub
   2) gdy przetwarzanie danych jest niezbędne do podjęcia działań jeszcze przed zawarciem umowy, przy czym musi się to odbywać na żądanie osoby, której dane dotyczą tzn.: jeżeli osoba poinformuje Uczelnię o zamiarze zawarcia umowy, to można się na tym opierać w celu przetwarzania tych jej danych, bez których umowa o treści oczekiwanej przez tę osobę nie może zostać zawarta.
2. Jeżeli w związku z zawarciem umowy, Uczelnia dowie się o innej osobie, to jej dane osobowe mogą być przetwarzane tylko na innej podstawie, niż wskazana w tym paragrafie; zwykle podstawą tą będzie uzasadniony interes administratora danych osobowych (Uczelni).

III. Rozwiązania organizacyjne w zakresie przetwarzania danych osobowych w Uczelni

§ 10

W celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w Uczelni, Rektor ustala organizację przebiegu tego procesu, powołuje osoby na funkcje niezbędne do prawidłowego wykonywania czynności przetwarzania danych osobowych oraz określa zadania tych osób.

§ 11

1. Rektor może powołać lokalnych administratorów danych osobowych i przekazać im – odpowiednio do zakresu wykonywanych przez nich zadań – obowiązki i uprawnienia Administratora danych osobowych.

2. W sytuacji, o której mowa w ust. 1, lokalni administratorzy danych osobowych odpowiedzialni są za poprawne przetwarzanie danych osobowych w podległych jednostkach organizacyjnych.
3. Lokalny administrator danych osobowych jest zobowiązany dołożyć szczególnych starań w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności przestrzegać zasad ich przetwarzania, o których mowa w niniejszej Polityce ochrony.
4. Lokalny administrator danych osobowych zobowiązany jest do:
   1) zapoznania osób przetwarzających dane osobowe z obowiązującymi przepisami w zakresie ochrony danych;
   2) wdrażania i przestrzegania przepisów określonych w niniejszej Polityce ochrony oraz innych aktach prawa powszechnego i aktach wewnętrznych obowiązujących w Uczelni, związanych z ochroną danych osobowych;
   3) stwarzania właściwych warunków organizacyjno-technicznych zapewniających ochronę danych osobowych w podległych jednostkach;
   4) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących przepisów prawa, zmianą, utratą, uszkodzeniem lub zniszczeniem;
   5) kontroli dotyczącej ustalenia jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;
   6) nadzoru nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób;
   7) bieżącego zgłaszania do prowadzonego przez Inspektora ochrony danych rejestru osób upoważnionych do przetwarzania danych osobowych;
   8) udzielania pisemnych, indywidualnych upoważnień, z określeniem ich zakresu osobom, które zostały dopuszczone do przetwarzania danych osobowych oraz przekazywania tych upoważnień do Inspektora ochrony danych, w celu ich rejestracji;
   9) przestrzegania obowiązujących ustaleń w zakresie udostępniania danych osobowych osobom trzecim;
   10) przestrzegania zasad postępowania w sytuacji naruszenia ochrony danych osobowych;
   11) analizy sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych;
   12) konsultowania wszystkich wątpliwości związanych z ochroną danych osobowych z Inspektorem ochrony danych.

§ 12

1. W celu bieżącego monitorowania przestrzegania powszechnie obowiązujących przepisów prawa oraz aktów wewnętrznych w zakresie ochrony danych osobowych, w tym w szczególności postanowień Polityki ochrony, Rektor powołuje Inspektora ochrony danych (IOD).
2. Inspektor ochrony danych podlega bezpośrednio Rektorowi.
3. Zadaniem Inspektora ochrony danych jest w szczególności:

1) informowanie Administratora danych osobowych, pracowników Uczelni, którzy przetwarzają dane osobowe oraz innych podmiotów przetwarzających dane, o spoczywających na nich obowiązkach wynikających z powszechnie obowiązujących przepisów prawa oraz przepisów aktów wewnętrznych Uczelni dotyczących ochrony danych osobowych;
2) szkolenie pracowników uczestniczących w operacjach przetwarzania danych osobowych oraz podejmowanie działań zwiększających świadomość w zakresie ochrony tych danych;
3) monitorowanie przestrzegania powszechnie obowiązujących przepisów prawa oraz aktów wewnętrznych dotyczących ochrony danych osobowych, w tym w szczególności przepisów Polityki bezpieczeństwa informacji w zakresie danych osobowych;
4) okresowa kontrola procedur, procesów i dokumentów Uczelni oraz ich obiegu pod kątem ochrony danych osobowych;
5) przeprowadzanie audytów oraz analiz stanu bezpieczeństwa ochrony danych;
6) monitorowanie wdrażania i zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
7) informowanie Rektora o stwierdzonych naruszeniach ochrony danych osobowych oraz zagrożeniach tych naruszeń;
8) analizowanie zdarzeń i sytuacji, które doprowadziły do tych naruszeń;
9) wnioskowanie o usunięcie uchybień w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych wraz z przedstawieniem propozycji rozwiązań zmierzających do usunięcia naruszeń;
10) współpraca z organem nadzorczym do spraw ochrony danych osobowych, w tym przeprowadzanie konsultacji w sprawach związanych z przetwarzaniem danych osobowych;
11) inicjowanie, koordynowanie oraz współuczestniczenie w procesie tworzenia oraz zmiany wewnętrznych aktów prawnych Uczelni z zakresu ochrony danych osobowych;
12) inicjowanie i podejmowanie innych przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
13) prowadzenie i utrzymywanie niezbędnej dokumentacji wynikającej z obowiązujących przepisów w zakresie ochrony danych, w tym w szczególności:
    a) rejestru zbiorów danych osobowych administrowanych, współadministrowanych i powierzonych;
    b) rejestru czynności przetwarzania danych w Uczelni,
    c) rejestru kategorii przetwarzanych danych w Uczelni,
    d) prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych oraz wydanych upoważnień,
14) identyfikowanie i analizowanie zagrożenia i ryzyka, na które może być narażone przetwarzanie danych osobowych;

15) wnioskowanie do Rektora o wdrożenie określonych zabezpieczeń adekwatnych do zagrożeń i ryzyka;
16) podejmowanie w porozumieniu z Rektorem działań w przypadku wykrycia naruszeń w systemie zabezpieczeń danego systemu przetwarzania danych;
17) prowadzenie rejestru naruszeń bezpieczeństwa danych osobowych.

4. Rektor nadaje Inspektorowi ochrony danych uprawnienia do:
   1) wydawania – po każdorazowym uzgodnieniu z Rektorem – poleceń pracownikom przetwarzającym dane osobowe w zakresie stosowania określonych zabezpieczeń tych danych;
   2) czasowego wstrzymania – po każdorazowym uzgodnieniu z Rektorem – przetwarzania danych osobowych przez pracownika lub pracowników Administratora na zasadach określonych w Polityce ochrony w przypadku naruszenia bezpieczeństwa danych osobowych skutkującego wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą.

§ 13

1. Rektor, w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w systemach teleinformatycznych, powołuje Administratora systemu informatycznego (ASI).
2. Administrator systemu informatycznego podlega bezpośrednio Rektorowi.
3. W zakresie powierzonych zadań, Administrator systemu informatycznego współpracuje z Inspektorem ochrony danych.
4. Zadaniem Administratora systemu informatycznego jest nadzorowanie i koordynowanie wdrażania i zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemach teleinformatycznych, a w szczególności:
   1) identyfikacja i analiza zagrożenia oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych;
   2) określanie potrzeb w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe oraz wyznaczanie strategii zabezpieczania systemów informatycznych (procedury bezpieczeństwa i standardy zabezpieczeń);
   3) monitorowanie i zapewnianie ciągłości działania systemu informatycznego oraz baz danych;
   4) nadzór nad fizycznym zabezpieczeniem pomieszczeń serwerowni i węzłów sieci komputerowej;
   5) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   6) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych;
   7) prowadzenie rejestrów i ewidencji wskazanych w niniejszej Polityce ochrony oraz Instrukcji zarządzania systemami informatycznymi.

§ 14

Kierownicy jednostek organizacyjnych Uczelni zobowiązani są do przestrzegania Polityki bezpieczeństwa informacji w zakresie danych osobowych i zachowania bezpieczeństwa danych osobowych w podległych sobie jednostkach, w tym w szczególności dopuszczenia do przetwarzania danych osobowych wyłącznie pracowników przeszkolonych i posiadających odpowiednie upoważnienie oraz nadzoru nad przetwarzaniem danych osobowych przez pracowników komórki organizacyjnej, którą kierują.

IV. Tryb udzielanie upoważnień do przetwarzania danych osobowych, obowiązki osób upoważnionych oraz przesłanki odwołania i wygaśnięcia tych upoważnień

§ 15

1. Do przetwarzania danych osobowych mogą być dopuszczeni wyłącznie pracownicy (zatrudnieni na podstawie umowy o prace lub umowy cywilnoprawnej) posiadający upoważnienie do przetwarzania tych danych.
2. Upoważnień udzielają odpowiednio Rektor lub Lokalni administratorzy danych osobowych, zgodnie z procedurą wynikającą z ust. 3 – 13. Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik Nr 1 do Polityki ochrony.
3. Upoważnienie udzielane jest pracownikowi – bez względu na podstawę prawną – z chwilą powstania stosunku zatrudnienia.
4. Zakres udzielonego upoważnienia nadawany jest stosownie do zakresu czynności powierzonych danemu pracownikowi – po uzgodnieniu z bezpośrednim przełożonym. Zasadę określoną w zdaniu poprzedzającym stosuje się odpowiednio w przypadku zmiany stanowiska pracy osoby, jednostki organizacyjnej lub zakresu wykonywanych zadań.
5. Rejestr upoważnień prowadzony jest w jednostkach organizacyjnych Uczelni – w zależności od charakteru zatrudnienia danej osoby.

§ 16

1. Przed udzieleniem upoważnienia do przetwarzania danych osobowych, pracownicy powinni zostać przeszkoleni.
2. Zakres szkolenia powinien obejmować w szczególności: omówienie przepisów RODO oraz postanowień niniejszej Polityki ochrony.
3. Za przeprowadzenie lub zorganizowanie szkolenia odpowiada Inspektor ochrony danych.

§ 17

Osoby upoważnione do przetwarzania danych osobowych w Uczelni, oprócz obowiązków wynikających z § 5 Polityki ochrony, zobowiązane są do:

1) przetwarzanie dany wyłącznie w zakresie ustalonym indywidualnie w upoważnieniu;
2) zachowania poufności danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie poufności danych osobowych obowiązuje przez cały okres zatrudnienia w Uczelni, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji, albo po wygaśnięciu/rozwiązaniu umowy cywilnoprawnej łączącej tę osobę z Uczelnią;
3) złożenia pisemnego oświadczenia o zachowaniu poufności przetwarzanych danych;
4) stosowania określonych przez Rektora oraz Inspektora ochrony danych procedur oraz wytycznych mających na celu zgodne z prawem, w tym zawłaszcza adekwatne do wykonywanych przez nie zadań, przetwarzanie danych;
5) korzystania z systemu informatycznego Administratora danych osobowych oraz środowiska informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
6) zabezpieczania przetwarzanych danych osobowych przed dostępem osób nieupoważnionych; indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych osobowych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu. Szczegółowe zasady przetwarzania danych osobowych przez osoby upoważnione zawiera Załącznik Nr 2 do Polityki ochrony;
7) zgłaszania bezpośredniemu przełożonemu oraz Inspektorowi ochrony danych wszelkich naruszeń dotyczących przetwarzania danych osobowych oraz podejmowania koniecznych działań ograniczających skutki tych naruszeń;
8) wykonywania poleceń Rektora oraz Inspektora ochrony danych w zakresie ochrony danych osobowych.

§ 18

1. Udzielone upoważnienie do przetwarzania danych osobowych może zostać odwołane w następujących przypadkach:
   1) odwołania z funkcji lub zmiany zakresu obowiązków służbowych pracownika, która spowodowała utratę lub ograniczenie potrzeby przetwarzania danych;
   2) spowodowania przez osobę – celowym działaniem – incydentu mającego negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych;
   3) zaistnienia uzasadnionej obawy, że przetwarzanie danych osobowych przez osobę wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.
2. Odwołanie upoważnienia może nastąpić na wniosek jednej z następujących osób: Rektora, Lokalnego administratora danych osobowych, Inspektora ochrony danych, przełożonego pracownika, osoby odpowiedzialnej w Uczelni za sprawy informatyzacji.

3. Procedura odwołana upoważnień obejmuje:
   1) przekazanie Inspektorowi ochrony danych pisemnego wniosku o odwołanie upoważnienia (za wyjątkiem sytuacji, gdy wnioskującym jest Inspektor ochrony danych) z określeniem imienia i nazwiska pracownika oraz jego identyfikatora w systemie informatycznym (jeśli pracownik posiada dostęp do systemu informatycznego), zakresu upoważnienia, które ma zostać odwołane, a także przyczyny konieczności odwołania lub ograniczenia upoważnienia; jeżeli wnioskującym o odwołanie lub ograniczenie zakresu upoważnienia jest Inspektor ochrony danych sporządzą on notatkę zawierającą wskazane informacje;
   2) w przypadku posiadania przez pracownika, którego upoważnienie zostało odwołane uprawnień do systemu informatycznego, przekazanie przez Inspektora ochrony danych Administratorowi systemu informatycznego polecenia unieważnienia hasła, zablokowania konta użytkownika, odebrania wszelkich uprawnień do systemu. Administrator systemu winien bez zbędnej zwłoki wykonać niezbędne czynności;
   3) odwołanie pracownikowi upoważnienia do przetwarzania danych osobowych i odebranie (jeśli nastąpiło) uprawnień do systemu informatycznego.
4. Wygaśnięcie upoważnienia do przetwarzania danych osobowych następuje w przypadku:
   1) rozwiązania stosunku pracy;
   2) wygaśnięcia lub rozwiązania umowy cywilnoprawnej;
   3) odwołania upoważnienia.

§ 19

1. Naruszenie polityki, zasad bezpieczeństwa ochrony danych osobowych oraz przyjętych w Uczelni procedur w tym zakresie przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane w kategorii ciężkiego naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
2. Pracownicy, z którymi rozwiązany został stosunek pracy z powodu naruszenia przepisów prawa dotyczących bezpieczeństwa przetwarzania danych osobowych i zasad określonych w niniejszej Polityce ochrony danych osobowych, mogą ponosić również za swoje czyny odpowiedzialność karną, m.in. za: stworzenie możliwości dostępu do danych osobowych osobie lub osobom nieupoważnionym; nieuprawnione kopiowanie danych osobowych; niezabezpieczenie komputera przenośnego; przetwarzanie danych osobowych w wersji papierowej poza wyznaczonymi miejscami w Uczelni.

§ 20

Pracownicy, którzy w zakresie swoich obowiązków nie wykonują czynności związanych z przetwarzaniem danych osobowych (osoby sprzątające, portierzy,, konserwatorzy itp.), a których obowiązki wymagają pracy podczas nieobecności

osób upoważnionych do przetwarzania danych osobowych w pomieszczeniach, w których dane osobowe są przetwarzane, muszą zostać zapoznani z zasadami dotyczącymi ochrony danych osobowych oraz uzyskać upoważnienie od przełożonego do przebywania w tych pomieszczeniach.

V. Infrastruktura przetwarzania danych osobowych w Uczelni

§ 21

Uczelnia zapewnia przetwarzanie danych osobowych w formie elektronicznej w systemach informatycznych spełniających określone wymogi techniczne i w zakresie bezpieczeństwa.

VI. Udostępnianie danych osobowych w Uczelni

§ 22

1. Uczelnia udostępnia przetwarzane dane osobowe wyłącznie:
   1) osobom, które przetwarzają dane osobowe na podstawie udzielonych - zgodnie procedurą określoną w niniejszej Polityce ochrony – upoważnień do przetwarzania danych osobowych w Uczelni;
   2) podmiotom przetwarzającym – na podstawie umowy powierzenia przetwarzania danych osobowych, która w szczególności określa:
      a) przedmiot i czas trwania przetwarzania,
      b) charakter i cel przetwarzania,
      c) rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
      d) obowiązki i prawa Administratora (Uczelni),
      e) obowiązki podmiotu przetwarzającego wynikające z art. 28 RODO
   3) podmiotom uprawnionym do dostępu i przetwarzania danych osobowych określonej kategorii na podstawie odpowiednich przepisów prawa.
2. Dostęp do danych osobowych, o którym mowa w ust. 1 pkt 3, po okazaniu dokumentów potwierdzających uprawnienia mogą mieć w szczególności pracownicy: Państwowej Inspekcji Pracy, Zakładu Ubezpieczeń Społecznych, organów skarbowych, policji i służb specjalnych (Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego), sądów powszechnych, Najwyższej Izby Kontroli, Urzędu Ochrony Danych Osobowych, a także inne osoby, podmioty i organy upoważnione przez przepisy prawa i działające w granicach przyznanych im uprawnień.

§ 23

Uczelnia ma obowiązek informować osobę o przetwarzaniu jej danych osobowych w następujących sytuacjach:
1) zbierając dane bezpośrednio od tej osoby;
2) zbierając dane o osobie z innych źródeł niż ta osoba;

3) zmieniając cel przetwarzania danych osobowych lub dodając nowy cel;
4) w wykonaniu żądania dostępu do danych.

§ 24

Jeżeli dane pozyskiwane są od osoby, której dotyczą Uczelnia, jako Administrator danych osobowych, powinna przekazać tej osobie informację o następującym zakresie:

1) nazwę i dane kontaktowe;
2) gdy ma to zastosowanie – dane kontaktowe Inspektora ochrony danych;
3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania dla każdego celu;
4) jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionych interesów realizowane przez Administratora lub przez stronę trzecią;
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
8) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
9) jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
10) informacje o prawie wniesienia skargi do organu nadzorczego;
11) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
12) gdy ma to zastosowanie – informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

§ 25

Jeżeli dane zostały pozyskane przez Uczelnię nie od osoby, której dotyczą, oprócz informacji wymienionych w § 23, należy poinformować osobę której dane są przetwarzane, o kategoriach pozyskanych danych oraz o źródle pozyskania danych, w tym o źródle publicznie dostępnym.

§ 26

Jeżeli Uczelnia planuje zmienić cel przetwarzanych informacji lub dodać nowy cel – należy poinformować o tym osobę, której dane są przetwarzane oraz udzielić informacji, których jeszcze nie posiada.

§ 27

Każda osoba której dane osobowe dotyczą, na podstawie art. 15 RODO ma prawo do uzyskania potwierdzenia, czy jej dane osobowe są przetwarzane w Uczelni, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji o:

1) celu przetwarzania;
2) kategorii odnośnych danych osobowych;
3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) w miarę możliwości – planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
5) prawie do: dostępu do danych, żądania od administratora danych ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
8) gdy ma to zastosowanie – zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, RODO oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

§ 28

Uczelnia zamieszcza obowiązkowe klauzule informacyjne także w materiałach promujących konferencję naukową lub inne wydarzenie, we wszelkich formach informacji (w tym na stronach internetowych), jeżeli w związku z organizacją konferencji naukowej lub innego wydarzenia następować będzie przetwarzanie danych osobowych. Obowiązek ten spoczywa na kierowniku jednostki organizacyjnej, która realizuje zadania w zakresie promocji i marketingu Uczelni lub organizatorze wydarzenia. Klauzule informacyjne opracowywane są każdorazowo – w zależności od potrzeb i uwzględniają specyfikę tego wydarzenia.

§ 29

1. Uczelnia może udostępnić dane osobowe studenta osobie trzeciej wyłącznie na podstawie pisemnego upoważnienia okazanego pracownikowi Uczelni

upoważnionemu do przetwarzania danych osobowych chyba, że dotyczy to sytuacji, o której mowa w § 19 ust. 2.

2. Udostępnienie przez Uczelnię danych osobowych studenta innemu studentowi, w szczególności staroście roku – może zostać dokonane również na podstawie pisemnego upoważnienia udzielonego przez studenta, którego dane osobowe dotyczą.

VII. Zdarzenia naruszające ochronę danych osobowych (incydenty) oraz tryb postępowania w przypadku naruszenia danych osobowych

§ 30

1. Do zdarzeń naruszających ochronę danych osobowych należą w szczególności zagrożenia losowe:
   1) zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia (zarówno danych w formie papierowe jak też elektronicznej) lub uszkodzenia infrastruktury technicznej systemu informatycznego, co sprawia, że ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych;
   2) wewnętrzne (np. niezamierzone pomyłki operatorów, administratora/administratorów lokalnych danych osobowych, awarie sprzętowe, błędy oprogramowania) – mogą one powodować zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
2. Zagrożenia losowe zamierzone (świadome i celowe) – to najpoważniejsze zagrożenia naruszenia poufności danych. W tym przypadku zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. Można je podzielić na:
   1) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);
   2) nieuprawniony dostęp do systemu z wewnątrz sieci informatycznej;
   3) nieuprawniony przekaz danych;
   4) bezpośrednie zagrożenie materialnych składników systemu, np. w wyniku kradzieży składników systemu.
3. Do przypadków zakwalifikowanych jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, zaliczyć należy w szczególności
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych;

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
7) dokonanie modyfikacji danych lub zmiany w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń (w szczególności haseł i identyfikatorów w systemie informatycznym);
9) nieprzypadkowe działania, odbiegające od ustalonych procedur, wskazujące na przełamanie lub zaniechanie ochrony danych osobowych (np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.);
10) zamiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;
11) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.).

4. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj.: na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej, pozostawienie wydruków zawierających dane osobowe w drukarkach, kserokopiarkach, umieszczenie takich wydruków w koszach na śmieci bez wcześniejszego zniszczenia w niszczarce itp.).
5. Rejestr incydentów naruszających dane osobowe prowadzi Inspektor ochrony danych.

§ 31

1. W przypadku stwierdzenia – przez upoważnionego pracownika przetwarzającego dane osobowe lub inną osobę zatrudnioną w Uczelni – naruszenia danych lub podejrzenie ich naruszenia, osoba ta jest zobowiązana niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego, który następnie zobowiązany jest powiadomić niezwłocznie Administratora systemu

informatycznego (jeżeli zdarzenie dotyczy przetwarzania danych w systemie informatycznym) oraz Inspektora ochrony danych.

2. Do czasu przybycia na miejsce naruszenia danych osobowych Administratora systemu informatycznego lub/i Inspektora ochrony danych należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość;
   2) udokumentować wstępnie zaistniałe naruszenie.
3. Administrator systemu informatycznego, który stwierdził naruszenie danych przetwarzanych w systemie informatycznym:
   1) ustala wszystkie okoliczności zdarzenie, czas wystąpienia zdarzenia oraz źródło informacji o zdarzeniu;
   2) ustala skutki zdarzenia dla bezpieczeństwa przetwarzania danych osobowych;
   3) podejmuje działania, adekwatne do rodzaju, skali i skutków zdarzenia, zapobiegające dalszym niepożądanym skutkom jego wystąpienia, np. odłącza urządzenie z sieci, zmienia hasło użytkownika jeżeli uzyskano dostęp do sieci z jego wykorzystaniem;
   4) informuje niezwłocznie Rektora o zaistniałym zdarzeniu;
   5) dokumentuje szczegółowo zaistniały przypadek naruszenia lub próby naruszenia danych osobowych, sporządzając raport zawierający w szczególności:
      a) stwierdzenie faktu naruszenia danych osobowych, wskazując jakie dane zostały naruszone oraz rodzaj naruszenia;
      b) wskazanie osoby powiadamiającej oraz innych osób udzielających informacji o zdarzeniu naruszenia ochrony danych osobowych;
      c) określenie czasu i miejsca: naruszenia/ujawnienia naruszenia ochrony danych i powiadomienia o tym fakcie;
      d) określenie okoliczności towarzyszących naruszeniu danych osobowych;
      e) wskazanie przesłanek uzasadniających wybraną metodę działania po stwierdzeniu naruszenia danych;
      f) wstępną ocenę przyczyn zaistnienia zdarzenia i wnioski z tym związane.
      g) wstępne propozycje działań zapobiegających wystąpieniu analogicznych zdarzeń;
   6) sporządza raport; Administrator systemu informatycznego doręcza go niezwłocznie Rektorowi i Inspektorowi ochrony danych;
   7) przywraca funkcjonowanie systemu informatycznego do bezpiecznego przetwarzania danych osobowych.
4. Inspektor ochrony danych stosuje odpowiednio procedurę określoną w ust. 3, jeżeli naruszenie danych osobowych nie jest związane z systemem informatycznym.
5. Po zaistnieniu incydentu naruszającego bezpieczeństwo danych osobowych należy dokonać w Uczelni, z udziałem osób pełniących funkcje związane z przetwarzaniem i udostępnianiem danych osobowych, wnikliwej analizy przyczyn zaistniałego incydentu i przedsięwziąć działania zapewniające w przyszłości bezpieczne przetwarzanie danych osobowych w Uczelni (np.

przeprowadzić ponowne szkolenia pracowników, wzmocnić zabezpieczenia komputerów)

§ 32

1. Rejestr zaistniałych incydentów związanych z przetwarzaniem danych osobowych prowadzi Inspektor ochrony danych.
2. Inspektor ochrony danych prowadzi rejestr incydentów w odniesieniu do zdarzeń związanych z przetwarzaniem danych w formie tradycyjnej.

§ 33

Jeżeli naruszenie ochrony danych osobowych skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, Rektor zgłasza ten fakt Prezesowi Urzędu Ochrony Danych Osobowych – niezwłocznie, nie później jednak niż w terminie 72. godzin od stwierdzenia naruszenia danych. Zgłoszenie powinno spełniać wymogi formalne określone w art. 33 ust. 3 RODO.

Postanowienia końcowe

§ 34

Z uwagi na wymianę infrastruktury informatycznej w Uczelni, w której przetwarzane są dane osobowe (serwery, system operacyjne, programy komputerowe), dokumenty wymagane do opracowania na podstawie niniejszej Polityki, zostaną opracowane po całkowitym odbiorze wskazanych urządzeń przez Uczelnię oraz dostawców (rejestry budynków i pomieszczeń, opis systemu, itp.).

REKTOR

Prof. Jerzy Posłuszny