ZARZĄDZENIE Nr 2/05 /2018

REKTORA WYŻSZEJ SZKOŁY MENEDŻERSKIEJ W WARSZAWIE

z dnia 22 maja 2018 r.

w sprawie ochrony danych osobowych przetwarzanych w Wyższej Szkole Menedżerskiej w Warszawie

Na podstawie art. 66 ust.2 ustawy z dnia 27 lipca 2005 roku Prawo o szkolnictwie wyższym. (tj. Dz. U. z 2012 r., poz. 572, z późń. zm.), art. 3 ust 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zarządza się, co następuje:

§1

Przetwarzanie danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie (WSM lub Uczelnia) służy w szczególności do realizacji zadań wynikających z art.13 ust.1 ustawy z dnia 27 lipca 2005 roku prawo o szkolnictwie wyższym, a także przepisów innych ustaw, gdy jest to niezbędne do zapewnienia prawidłowego funkcjonowania WSM, a nie narusza zarazem praw osób, których to dotyczy.

§ 2

1. Rektor, realizując kompetencje Administratora Danych Osobowych, wyznacza osobę odpowiedzialną za bezpieczeństwo danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie, zwaną dalej Inspektorem Ochrony Danych (IOD).
2. O fakcie wyznaczenia IOD oraz jego danych kontaktowych Administrator Danych Osobowych zawiadamia Prezesa UODO. Analogicznie postępuje w przypadku odwołania IOD. Dane kontaktowe IOD są podane do publicznej wiadomości w sposób zwyczajowo przyjęty.

§ 3

1. IOD wykonuje zadania z zakresu ochrony danych osobowych, określone zakresem czynności, zgodnie z przepisami RODO, w ścisłej współpracy z:
    1) Dyrektorami Centrów
    2) Dziekanami Wydziałów;
    3) Głównym Informatykiem.

2. Zobowiązuje się IOD do prowadzenia dokumentacji odzwierciedlającej wykonywanie zadań z zakresu ochrony danych osobowych, określonej w dokumentacji, o której mowa w § 4 ust. 2 niniejszego zarządzenia.

3. Udostępnianie podmiotom zewnętrznym, celem przetwarzania do celów innych niż określone w § 1 niniejszego Zarządzenia, danych osobowych dotyczących pracowników WSM, odbywa się wyłącznie za pośrednictwem Kanclerza oraz Dziekanów - w przypadku doktorantów lub studentów, po uprzednim uzyskaniu zgody Rektora.

§ 4

1. Wprowadza się w Uczelni obowiązujące zasady ochrony danych osobowych przetwarzanych w zbiorach danych WSM.
2. Zasady ochrony danych osobowych zawarte zostały w:
   1) Polityce Bezpieczeństwa Danych Osobowych, stanowiącej załącznik nr 1 do niniejszego Zarządzenia;
   2) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącej załącznik nr 2 do niniejszego Zarządzenia;
   3) Regulaminie korzystania z firmowej poczty elektronicznej i sieci Internet przez pracowników Wyższej Szkoły Menedżerskiej w Warszawie oraz osoby z nim współpracujące, stanowiącej załącznik nr 3 do niniejszego Zarządzenia;
   4) Instrukcji postępowania w przypadku stwierdzenia przypadków naruszenia bezpieczeństwa informacyjnego w WSM, stanowiącej załącznik nr 4 do niniejszego zarządzenia;
   5) innego rodzaju procedurach, wydanych mocą Zarządzeń Rektora WSM, tworzących łącznie system dokumentacji Zarządzania Bezpieczeństwem Informacyjnym w WSM.
3. Aktualizacji dokumentów opisanych w ust. 2 dokonuje IOD, w ścisłej współpracy z jednostkami organizacyjnymi wskazanymi w § 3 ust. 1.

§ 5

Nieprzestrzeganie przepisów w zakresie ochrony danych osobowych przez pracownika WSM może być uznane za ciężkie naruszenie przez niego podstawowych obowiązków pracowniczych, co w konsekwencji skutkować może nałożeniem kary porządkowej lub innymi konsekwencjami przewidzianym przepisami kodeksu pracy.

§ 6

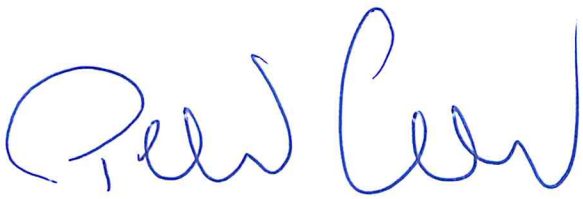
Z dniem 25 maja 2018 wszystkim osobom zaangażowanym w proces przetwarzania danych osobowych w WSM należy wydać nowe upoważnienia, zgodne z wzorem określonym w Polityce, o której mowa w § 4 ust. 1 pkt. 1.

§ 7

Z dniem 25 maja 2018 r. tracą moc dotychczasowe zarządzenia dotyczące ochrony danych osobowych w WSM .

§ 8

Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.



.....

Prof. dr hab. Paweł Czarnecki, MBA, Dr h.c. Mult.
Rektor
Wyższej Szkoły Menedżerskiej w Warszawie

Wyższa Szkoła Menedżerska
w Warszawie

Polityka Bezpieczeństwa Danych Osobowych

Załącznik nr 1 do zarządzenia Rektora WSM w Warszawie nr 2/05/2018
z dnia 22 maja 2018r.

Warszawa, Maj 2018

Wyższa Szkoła Menedżerska w Warszawie

Wersja Dokumentu: 1/2018

Dokument przygotował:

Dyrektor Centrum Administracyjno –technicznego inż. Dariusz Grabiec

Dokument zatwierdził:

J.M. Rektor Prof. dr hab. Paweł Czarnecki MBA dr h.c.

Wprowadzono do stosowania Zarządzeniem Rektora 2/05/2018
z dnia 22 maja 2018 roku

Spis treści

Wstęp

Polityka Bezpieczeństwa Danych Osobowych (PBDO) Wyższej Szkoły Menedżerskiej w Warszawie – uczelni niepublicznej, określanej w dalszej części również mianem Uczelnia lub skrótem WSM, opracowana została na podstawie wymogów prawnych określonych w Rozporządzeniu ogólnym. Zawiera ona zakres zabezpieczeń stosowanych w odniesieniu do danych osobowych, wskazanie obowiązujących środków organizacyjnych i technicznych oraz mechanizmy ochrony tych danych przetwarzanych w zbiorach zarówno w formie papierowej, jak również elektronicznej, a także danych osobowych przetwarzanych poza zbiorem. PBDO normuje mechanizmy aktualizacji dokumentacji związanej z ochroną danych osobowych, a także wprowadza jednolite zasady wydawania upoważnień do przetwarzania danych osobowych, pozwala zarazem monitorować proces udostępniania tych danych i inne aspekty związane z ich przetwarzaniem.

1. Podstawowe pojęcia i definicje:

Poniżej zestawiono najważniejsze pojęcia i definicje, obowiązujące w treści niniejszej Polityki, ale zarazem we wszystkich innych składnikach dokumentacji Uczelni stosowanych w procesach przetwarzania danych osobowych przez wszystkie zaangażowane w ten proces osoby.

1) **Rozporządzenie ogólne (RODO)** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, opublikowane w Dzienniku Urzędowym Unii Europejskiej L Nr 119/1.

2) **Administrator** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. W znaczeniu określonym powyżej Administratorem jest Wyższa Szkoła Menedżerska w Warszawie, a czynności operacyjne związane z realizacją zadań Administratora spoczywają na Rektorze.

3) **Organ nadzorczy** - oznacza niezależny organ publiczny ustanowiony zgodnie z art. 51 Rozporządzenia ogólnego.

4) **Polityka Bezpieczeństwa Danych Osobowych** – Niniejszy dokument opracowany w celu określenia obowiązujących zasad w trakcie procesu przetwarzania danych osobowych. Jest on zestawem zasad, praw, procedur i praktycznych rozwiązań regulujących sposób zarządzania tym procesem, w szczególności jego zabezpieczenia i ochrony, a także dystrybucji wewnątrz Uczelni, jak i w kontaktach z otoczeniem.

5) **Inspektor Ochrony Danych (IOD)** - osoba wyznaczona przez Administratora, której zadania polegają w szczególności na realizacji celów powierzonych jej przez

Administratora, w tym wymagań stawianych przed nią na podstawie niniejszej Polityki, zgodnych z przepisami Rozporządzenia ogólnego, w szczególności art. 39.

6) **Administrator Systemu Informatycznego (ASI)** – osoba wyznaczona przez Administratora, której zadaniem jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

7) **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

8) **Minimalizacja danych** – przetwarzanie danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.

9) **Prawidłowość i aktualność danych** – właściwość rozumiana jako konieczność podjęcia wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

10) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie, utrzymywanie eksploatacja, dostosowywanie i zmienianie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem oraz przypadkową utratą, zmianą, zniszczeniem lub uszkodzeniem.

11) **Integralność danych** – własność danych polegająca na braku możliwości wprowadzenia do nich zmian w sposób nieautoryzowany.

12) **Poufność danych** – własność danych polegająca na tym, że nie są one udostępniane lub ujawniane nieautoryzowanym osobom, podmiotom lub procesom.

13) **Dostępność danych** – własność danych, polegająca na tym, że są one osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.

14) **Obszar przetwarzania danych osobowych** – budynki, pomieszczenia lub części pomieszczeń WSM, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i elektronicznej, a także wszystkie obszary, w których ma miejsce przetwarzania danych osobowych przez podmioty przetwarzające w związku z działalnością prowadzoną przez WSM.

15) **Zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, dane której dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

16) **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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.

17) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

18) **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.

19) **Pseudonimizacja** - 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.

20) **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.

21) **Bezpieczeństwo informacji** – stan rozumiany jako zachowanie trzech podstawowych atrybutów związanych z przetwarzaniem informacji, tj. poufności, integralności oraz dostępności, a jednocześnie zapewnienia odporności systemów i usług do tego służących.

22) **Bezpieczeństwo systemu informatycznego** - zapewnienie odporności sieci lub każdej części systemu, na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych przy zastosowaniu środków technicznych i organizacyjnych.

23) **Rozliczalność** – konieczność przestrzegania przepisów Rozporządzenia ogólnego przez Administratora, a także możliwość wykazania tego przestrzegania.

24) **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

25) **Usuwanie danych osobowych** – działanie bez zbędnej zwłoki polegające na zniszczeniu danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

26) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy też rozproszony funkcjonalnie lub geograficznie.

27) **Szczególne kategorie danych osobowych** - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

28) **Wnioski o skorzystanie z praw (WSP)** - żądania od osób, których dane dotyczą, skierowane do WSM w celu skorzystania z przysługujących im praw w odniesieniu do problematyki danych osobowych.

29. **System ochrony danych osobowych** – system składający się ze zbioru środków prawnych, zarządczych, organizacyjnych i technicznych, utworzony w celu zapewnienia pożądanego przez Administratora poziomu bezpieczeństwa tych danych.

30. **Sytuacja kryzysowa** to zazwyczaj niespodziewane i niepożądane zdarzenie lub seria wydarzeń, które mogą stanowić istotne zagrożenie dla pozycji oraz stabilności organizacji jako całości, lub tylko jej części.

2. Cele, zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji dot. osób fizycznych

1) Celem niniejszej Polityki Bezpieczeństwa Danych Osobowych (zwanej dalej Polityką) jest określenie zasad przetwarzania danych osobowych, jako zestaw praw, reguł, procedur i praktycznych doświadczeń regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz WSM, jak i w kontaktach z otoczeniem zewnętrznym. Polityka Bezpieczeństwa Danych Osobowych stanowi dokument odnoszący się całościowo do problemu zabezpieczenia i zgodnego z przepisami prawa tych danych u Administratora, z uwzględnieniem i poszanowaniem praw osób, których dane dotyczą.

2) Zakres bezpieczeństwa dotyczy wszelkich procesów wykonywanych w obszarze przetwarzania danych osobowych w powiązaniu z prowadzoną działalnością i stanowi część całościowego systemu kierowania Uczelnią.

3) Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie do:

- danych osobowych przetwarzanych w związku z realizacją przez WSM wszelakich procesów biznesowych i świadczenia usług, które dokonywane może być w systemach informatycznych oraz w tradycyjnej - papierowej formie,
- przechowywania danych osobowych na wszelkich nośnikach danych (magnetycznych, optycznych, elektronicznych takich jak: zewnętrzny dysk, dysk twardy, płyta CD/DVD, pamięć masowa typu flash), a także w książkach i kartotekach ewidencyjnych;
- danych osobowych przetwarzanych zarówno w zbiorach danych, zestawach oraz pojedynczych informacjach dotyczących osoby fizycznej;
- informacji dotyczących bezpieczeństwa danych osobowych, w szczególności informacji służących do uwierzytelnienia się w systemach informatycznych, w których mogą występować dane osobowe.

3. Oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji

1) Najwyższe kierownictwo Uczelni, reprezentowane przez Rektora, stojąc na stanowisku, że dane osobowe są priorytetowym zasobem każdej organizacji, wdrożyło niniejszą Politykę. Gwarancją sprawnej i skutecznej ochrony informacji, szczególnie danych osobowych, jest zapewnienie odpowiedniego do wymogów poziomu ich bezpieczeństwa oraz zastosowanie rozwiązań technicznych i organizacyjnych, zapewniających skuteczne tego spełnienie. Rektor WSM wprowadzając Politykę Bezpieczeństwa Danych Osobowych deklaruje, że będzie ona podlegała ciągłemu doskonaleniu, uwzględniając w szczególności zmiany w otoczeniu prawnym, biznesowym oraz wynikające ze stanowiska Organu nadzorczego, a także właściwych organów Unii Europejskiej.

2) Podejście do bezpieczeństwa danych osobowych w Uczelni opiera się na czterech kluczowych regułach:

- Reguła poufności informacji - zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym,

- Reguła integralności informacji - zapewnienie zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania,

- Reguła dostępności informacji - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba,

- Reguła odporności systemów i usług przetwarzania - zapewnienie odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych.

3) Celem wdrożonego w WSM Systemu ochrony danych osobowych jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- będzie gwarantem pełnej ochrony danych wszystkich osób związanych z Uczelnią (studenci, słuchacze, doktoranci, uczestnicy kursów, pracownicy naukowi, dydaktyczni i administracyjni) oraz ciągłości procesu ich przetwarzania;
- zapewni zachowanie poufności informacji chronionych, integralności i dostępności danych osobowych;
- zapewni odporność systemów i usług przetwarzania danych osobowych;
- zagwarantuje odpowiedni poziom bezpieczeństwa danych osobowych, bez względu na jej postać, we wszystkich systemach jej przetwarzania;
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa danych osobowych, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę Uczelni;
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania
- danych osobowych;
- zapewni gotowość do podjęcia działań w Sytuacjach kryzysowych dla bezpieczeństwa WSM, jego interesów oraz posiadanych i powierzonych mu informacji.

4) W ramach modyfikacji lub wprowadzania nowych systemów oraz procesów mających związek z przetwarzaniem Danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie wprowadza się wymagania związane z uwzględnianiem ochrony danych w fazie projektowania. W ramach ww. procesów uwzględnia się również domyślną ochronę danych, co oznacza wprowadzanie takich ustawień systemu informatycznego czy oprogramowania, które jako ustawienia pierwotne zapewnią ochronę tych danych. Zmiana tych ustawień powinna następować jedynie na wyraźne żądanie użytkownika oprogramowania/systemu. W ramach opisanych działań należy brać pod uwagę koszt nowego wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a w szczególności ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i jego wadze. Wdrożone środki mają zapewnić aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

4. Zasady, standardy i wymagania zgodności stanowiące podstawę dla treści Polityki Bezpieczeństwa Danych Osobowych WSM

1) Przepisy prawa

- krajowe akty prawne:

Konstytucja Rzeczypospolitej Polskiej:

Art. 47 Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.
Art. 51 1) Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2) Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3) Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4) Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5) Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Ustawa „Prawo o szkolnictwie wyższym";

Ustawa „Kodeks cywilny" – w odniesieniu do warunków zawierania i wykonywania umów (art. 66 i następne kc);

- Przepisy prawa Unii Europejskiej:

Rozporządzenia:

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO),

Rozporządzenie (WE) Nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

Dyrektywy:

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej).

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym).

Dyrektywa 2016/680 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

5. Zasady realizacji szkoleń i doskonalenia zawodowego w zakresie bezpieczeństwa danych osobowych

1) Każdy pracownik Uczelni, mający dostęp do danych osobowych jest zobowiązany do uczestniczenia w programie szkolenia i doskonalenia zawodowego w zakresie związanym z bezpieczeństwem informacji, w szczególności danych osobowych. Szkolenia są prowadzone na koszt WSM.
Szkolenia mają na celu, poza zapoznaniem pracowników z problematyką bezpieczeństwa i ochrony danych osobowych, uświadomić im jak ważne jest odpowiednie przetwarzanie i ochrona tych danych, z punktu widzenia zapewnienia praw osób, których one dotyczą, ale również bezpieczeństwa prawnego i biznesowego WSM.
Szkolenia mogą mieć charakter wewnętrzny lub zewnętrzny.

2) Wyróżnia się następujące rodzaje szkoleń:
- szkolenia odnoszące się do aktualnej problematyki ochrony danych osobowych, w tym, w szczególności do Rozporządzenia ogólnego dla osób nowozatrudnionych;

- okresowe szkolenia przypominające odnoszące się do aktualnej problematyki ochrony danych osobowych, w tym, w szczególności do Rozporządzenia ogólnego dla pracowników.

Szczegółowy program szkoleń, pod względem merytorycznym, winien być zaakceptowany przez Inspektora Ochrony Danych, który jest jednocześnie odpowiedzialny za kwalifikowanie pracowników do udziału w poszczególnych rodzajach szkoleń, ustalenie częstotliwości realizacji kolejnych szkoleń, a także prowadzenie dokumentacji z tym związanej.

6. Podstawowe zasady ochrony bezpieczeństwa danych osobowych

1) Ochrona bezpieczeństwa Danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie opiera się na następujących zasadach:

- zasadzie rozdziału kompetencji - funkcje i zadania w obszarze związanym z przetwarzaniem danych osobowych realizują inne zespoły pracowników, niż w obszarze kontroli przestrzegania postanowień zawartych w przepisach prawa oraz dokumentacji wewnętrznej;
- zasadzie indywidualnej odpowiedzialności - za utrzymanie właściwego poziomu bezpieczeństwa informacyjnego odpowiadają, zgodnie z zakresem swoich obowiązków i uprawnień, konkretne osoby, które muszą mieć świadomość tej odpowiedzialności;
- zasadzie uzasadnionej obecności - prawo przebywania w określonych pomieszczeniach Uczelni mają wyłącznie osoby, które są do tego uprawnione;
- zasadzie uprawnień koniecznych – każdy użytkownik systemu informatycznego posiada prawa ograniczone wyłącznie do zasobów, które są niezbędne do wykonywania powierzonych mu zadań służbowych;
- zasadzie stałej gotowości – system związany z ochroną danych osobowych funkcjonuje w sposób nieprzerwany, odpowiednio do warunków realizacji zadań Uczelni;
- zasadzie wyceny aktywów informacyjnych, w szczególności danych osobowych Uczelni w oparciu o jednolite metody i wzorce.

2) Zasady związane z zapobieganiem i wykrywaniem wirusów i innego rodzaju złośliwego oprogramowania zostały określone w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie.

7. Zasady przetwarzania danych osobowych wymagane przez Rozporządzenie ogólne

Zgodnie z przepisami Rozporządzenia ogólnego w WSM wprowadza się następujące zasady przetwarzania danych osobowych:

1) Zasada przejrzystego przetwarzania: Dane osobowe przetwarza się z zapewnieniem osobom fizycznym informacji o tym, jak, dlaczego i jak długo te dane są przetwarzane. WSM zapewnia, że osoby, których dane dotyczą zostaną poinformowane o przetwarzaniu ich danych osobowych przez Uczelnię, w tym o celu ich przetwarzania oraz podmiotach przetwarzających, którym te dane przekazuje.

W związku z tym, gromadząc dane określonej osoby, WSM musi udostępnić osobie, której te dane dotyczą informację zawierającą co najmniej:

- nazwę i dane kontaktowe Uczelni, która będzie Administratorem danych osoby, której one dotyczą;
- dane kontaktowe Inspektora Ochrony Danych w Uczelni;
- krótki opis celu (celów), dla którego dane osoby, której dane dotyczą mogą być przetwarzane oraz podstawa prawna takiego przetwarzania (patrz Zasada 2 poniżej). Jeżeli przetwarzanie odbywa się w oparciu o uzasadnione interesy WSM, lub osoby trzeciej, informacja powinna również zawierać krótki opis tego uzasadnionego interesu;
- dane odbiorców (w tym podmioty przetwarzające) lub kategorie odbiorców, którym dane osoby, której dane dotyczą mogą zostać ujawnione;
- w stosownych przypadkach informacje o tym, że dane osoby, której dane dotyczą mogą być przesyłane za granicę oraz informacje o mechanizmach do tego służących;
- okres przechowywania danych lub (jeśli nie jest to możliwe) kryteria stosowane do określenia okresu przechowywania (retencji danych);
- istnienie prawa do dostępu, sprostowania, usuwania, sprzeciwu i przenoszenia danych; oraz w stosownych przypadkach prawo do wycofania zgody na przetwarzanie danych osobowych;
- prawo do złożenia skargi do Organu nadzorczego;
- informację czy podanie danych osobowych jest wymogiem ustawowym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania oraz jakie są konsekwencje niepodania danych;
- informację o stosowaniu jakiegokolwiek zautomatyzowanego procesu podejmowania decyzji lub profilowania oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2) Zasada zgodności z prawem: WSM przetwarza tylko dane osobowe, włączając w to Szczególne kategorie danych osobowych, w sytuacji posiadania ważnej do tego podstawy. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- 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;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- 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.

W przypadku Szczególnych kategorii danych osobowych należy spełnić co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń;
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego.

8. Struktura zarządzania bezpieczeństwem danych osobowych

Tworzy się następującą strukturę zarządzania bezpieczeństwem danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie:

1) Administrator (określony zgodnie z definicją)

2) Inspektor Ochrony Danych (IOD)
Jest on odpowiedzialny za realizację następujących zadań:

- informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na podstawie przepisów prawa odnoszących się do ochrony danych osobowych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania przepisów prawa oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków,
- działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
- współpraca z Organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla Organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

- inne zadania szczegółowo określone w niniejszej Polityce, dotyczące zapewnienia bezpieczeństwa danych osobowych.

Osoba pełniąca funkcję IOD, w zakresie czynności z tym związanych, podlega wyłącznie Administratorowi, personalnie Rektorowi.

3) Administrator Systemu Informatycznego (ASI)

Funkcję Administratora Systemu Informatycznego pełni Kierownik Działu IT, który wykonuje polecenia Inspektora Ochrony Danych w wyznaczonym przez niego obszarze działania.
Do obowiązków ASI należy w szczególności:

- rejestrowanie i wyrejestrowywanie użytkowników systemu informatycznego na podstawie wniosku zaakceptowanego przez kierownika jednostki organizacyjnej i/lub przełożonego;
- dokonywanie zmiany uprawnień użytkowników systemu na podstawie wniosku zaakceptowanego przez kierownika jednostki organizacyjnej i/lub przełożonego;
- przestrzeganie opracowanych dla systemu procedur bezpieczeństwa;
- utrzymanie systemu w sprawności technicznej w stopniu określonym w dokumentacji powykonawczej;
- konfigurowanie urządzeń i oprogramowania;
- aktualizowanie i konfigurowanie oprogramowania antywirusowego;
- reagowanie na naruszenia bezpieczeństwa i usuwanie ich skutków;
- nadzorowanie właściwego użytkowania oraz serwisowania urządzeń i oprogramowania;
- wykonywanie kopii bezpieczeństwa informatycznych baz danych osobowych oraz systemów informatycznych.

9. Podstawowe zasady postępowania w przypadku naruszenia ochrony danych osobowych

1) Przetwarzanie danych osobowych powinno mieć miejsce w zakresie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji, a zarazem do realizowanych czynności przetwarzania związanych z potrzebami biznesowymi użytkowników systemów informatycznych. Za monitorowanie stanu bezpieczeństwa informacyjnego, a w przypadku jego naruszenia za podjęcie niezwłocznie działań związanych z ich eliminacją odpowiada Inspektor Ochrony Danych we współpracy z Administratorem Systemu Informatycznego.

   - Szczegółowy sposób postępowania w przypadku stwierdzenia wystąpienia naruszenia bezpieczeństwa informacyjnego jest określony w „Instrukcji postępowania w sytuacji stwierdzenia przypadków naruszenia bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie", a także w przepisach, "Regulaminu korzystania z firmowej poczty elektronicznej oraz sieci Internet przez pracowników WSM oraz osoby z nim współpracujące".

2) W zakresie technicznych środków zabezpieczenia przed wystąpieniem naruszeń bezpieczeństwa danych osobowych zastosowanie mają natomiast przepisy procedur wykonawczych Działu IT.

10. Dane współadministrowane

W przypadku gdy dane osobowe będą współadministrowane przez dwóch lub większą liczbę Administratorów – przetwarzanie danych może odbywać się jedynie na podstawie umowy, w której Administratorzy w przejrzysty sposób określą odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów prawa dotyczących ochrony danych osobowych.
Za monitorowanie przestrzegania zgodności przetwarzania z właściwymi umowami odpowiedzialny jest Inspektor Ochrony Danych.

11. Czynności związane z realizacją praw osób, których dane dotyczą

1) Informacje ogólne
Wyższa Szkoła Menedżerska w Warszawie ma obowiązek umożliwiania osobom, których dane dotyczą, korzystania z ich praw dostępu, usuwania, sprostowania, sprzeciwu i przenoszenia danych osobowych.
Podstawowe prawa osób, których dane dotyczą, a także sposób umożliwiania korzystania z tych praw zostały zdefiniowane w niniejszej Polityce. Określono w szczególności to, w jaki sposób Uczelnia powinna ułatwiać osobom fizycznym korzystanie ze swoich praw oraz w jaki sposób odpowiadać na konkretne prośby osób, których dane dotyczą, w zakresie wykonywania ich praw. W kontekście realizowania określonych praw osób, których dane dotyczą, należy pamiętać o każdorazowym pouczeniu tych osób o możliwości złożenia skargi do Organu nadzorczego, w sytuacji gdyby rozstrzygnięcie WSM w jej sprawie byłoby uznane za niesatysfakcjonujące.
Udzielanie informacji o przetwarzaniu danych osobowych, a także w sprawach związanych z realizacją określonych żądań osób, których dane dotyczą, jest realizowane co do zasady nieodpłatnie. Odpłatny tryb udzielania informacji, może być zastosowany wyłącznie w szczególnych, indywidualnych wypadkach, powodowanych oceną nadmiarowego kierowania tego rodzaju wniosków. W takich jednak okolicznościach opłata za udzielenie informacji musi uwzględniać wyłącznie faktycznie poniesione w tym zakresie przez WSM koszty.
IOD nadzoruje w sposób bezpośredni każdy proces działań związanych z realizacją praw osób, pełniąc zarazem rolę tzw. punktu kontaktowego dla tych osób. Dane dotyczące jego numeru telefonu oraz adresu poczty elektronicznej muszą być dostępne na stronie internetowej Uczelni, a także na wszystkich formularzach wykorzystywanych w procesie pozyskiwania danych od tych osób.
2) Wyższa Szkoła Menedżerska w Warszawie umożliwia w szczególności realizację następujących praw:

- Prawo dostępu do danych: osoby, których dane dotyczą mają prawo do informacji, jakie dane osobowe przetwarza na ich temat Uczelnia oraz mają prawo do uzyskania kopii tych danych osobowych.

- Prawo do bycia zapomnianym: osoby, których dane dotyczą, mają prawo do usunięcia danych osobowych, jeśli Uczelnia nie ma podstawy wynikającej z zasady zgodności z prawem do dalszego przetwarzania danych. W niektórych przypadkach WSM może podjąć decyzję o nieusuwaniu danych, ale zamiast tego ograniczyć ich użycie (na przykład, aby można było z niego korzystać tylko w przypadku roszczenia prawnego).
- Prawo do sprostowania danych: osoby, których dane dotyczą mają, prawo do uzupełnienia niedokładnych danych, a także ich poprawienia i / lub uzupełnienia niekompletnych danych.
- Prawo do wniesienia sprzeciwu: osoby, których dane dotyczą mają prawo sprzeciwić się wykorzystywaniu ich danych osobowych do określonego celu, na przykład do profilowania podejmowania decyzji zautomatyzowanych.
- Prawo do przenoszenia danych: osoby, których dane dotyczą, mają prawo do otrzymywania danych osobowych, które dostarczyły WSM, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego oraz mają prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Uczelni.
- Prawo do ograniczenia przetwarzania: osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania, w razie zrealizowania się przesłanek wynikających z aktualnych przepisów prawa.

Prawa o których mowa powyżej realizowane są poprzez umożliwienie podmiotowi wykonywania m.in. następujących czynności:

- przeglądanie danych osobowych, które przetwarza na ich temat Wyższa Szkoła Menedżerska w Warszawie;
- żądanie usunięcia wszelkich informacji, co do których wyrażają wolę, aby Wyższa Szkoła Menedżerska w Warszawie już nie miała dostępu;
- żądanie skorygowania wszelkich niedokładności i błędów danych i aktualizacja tych danych, które tego wymagają,
- żądanie zmiany ustawienia swojego konta w systemie informatycznym, tak aby ich dane osobowe nie były już wykorzystywane do określonego celu (np. rezygnacja z możliwości marketingu);
- żądanie uzyskania kopii danych w powszechnie używanym i przeznaczonym do odczytu maszynowego formacie.

3) Realizacja wniosków w sprawach o dostęp do danych
Zgodnie z zasadą przejrzystego przetwarzania Wyższa Szkoła Menedżerska w Warszawie informuje osobę, której dane dotyczą o przysługujących jej prawach, prostym, jasnym i zrozumiałym językiem.
Proces realizacji praw osób podlega w każdym indywidualnym przypadku analizie pod kątem zgodności z prawem powszechnym i wewnętrznymi przepisami Uczelni.
Osoby, których dane dotyczą są również uprawnione do złożenia pisemnego lub ustnego wniosku, do WSM w celu skorzystania z przysługujących im praw.
Żądania od osób, których dane dotyczą, skierowane do WSM w celu skorzystania z tych praw są określane jako "wnioski o skorzystanie z praw" (WSP) i bezwzględnie należy rejestrować datę otrzymania WSP i sam wniosek.
Nie obowiązuje żaden konkretny wzór wniosku o skorzystanie z praw. Należy akceptować składane w tych sprawach wnioski w każdej dogodnej dla wnioskodawców formie. Jeżeli dana osoba odmawia złożenia wniosku na piśmie, WSM powinna wysłać wnioskodawcy pisemną informację tak szybko, jak to możliwe, potwierdzając charakter i zakres wniosku.

Przed podjęciem jakichkolwiek działań w związku z WSP należy podjąć wszelkie możliwe działania w celu uwierzytelnienia tożsamości osoby, której dane dotyczą lub osoby upoważnionej do działania w jej imieniu.
Wyższa Szkoła Menedżerska w Warszawie ma obowiązek odpowiedzieć na WSP w ciągu jednego miesiąca. Jeśli żądanie jest według oceny IOD szczególnie skomplikowane, udzielenie odpowiedzi może zostać przedłużone do okresu nie przekraczającego 2 miesięcy. W takich jednak przypadkach Uczelnia ma obowiązek udzielenia wstępnej odpowiedzi żądającemu w ciągu jednego miesiąca, wyjaśniając, dlaczego konieczne jest wydłużenie okresu.
Etapami odpowiedzi na „wniosek o skorzystanie z praw są następujące działania:

- poinformowanie Inspektora Ochrony Danych bez zbędnej zwłoki oraz jednostek biznesowych, w których kompetencji jest dalsze działanie o wpłynięciu wniosku;
- zidentyfikowanie, które systemy, bazy danych, zestawy informacji w formie papierowej mogą zawierać informacje dotyczące jednostek organizacyjnych odpowiedzialnych za przetwarzanie informacji będących przedmiotem wniosku. Realizacja zadań odbywa się tu przy pełnej współpracy z właściwymi jednostkami organizacyjnymi oraz Działem IT i jest koordynowana przez IOD;
- po zakończeniu działań przez odpowiednią jednostkę biznesową dostarcza ona kopię wszelkich informacji zidentyfikowanych do Inspektora Ochrony Danych;
- IOD dokonuje przeglądu informacji w celu zidentyfikowania wszelkich danych osobowych dotyczących wnioskodawcy. W przypadku stwierdzenia braku przeciwskazań natury prawnej, IOD podejmuje decyzję o przesłaniu kopii danych osobowych wymaganych przez daną osobę.

Wyższa Szkoła Menedżerska w Warszawie nie powinna ujawniać, usuwać ani w inny sposób wpływać na dane osobowe dotyczące osób innych niż sam wnioskodawca, chyba że strona trzecia wyrazi na to zgodę lub uzasadnione jest dostarczenie (lub usunięcie danych itp.) bez ich zgody.

4) Realizacja wniosków o usunięcie danych i prawo do bycia zapomnianym
Prawa do usunięcia danych i do bycia zapomnianym nie są prawami absolutnymi. Wyższa Szkoła Menedżerska w Warszawie nie musi usuwać danych osobowych, które należy zachować:

- w celu ochrony przed roszczeniami prawnymi (np. umowy, historia zatrudnienia lub korespondencja z klientem w sprawie skargi);
- w celu spełnienia obowiązku prawnego;
- w celu wykonania umowy.

Osoba, której dane dotyczą, nie ma prawa do wyrażenia sprzeciwu wobec wykorzystywania jej informacji w celu, który jest niezbędny do wypełnienia zobowiązań prawnych Uczelni. WSM powinna spełnić żądania usunięcia i / lub sprzeciwu wobec przetwarzania w odniesieniu do następujących danych (o ile nie są one przedmiotem skargi lub postępowania sądowego):

- informacje o profilowaniu klienta;
- pliki cookie;
- zebrane w celach marketingowych;
- niezrealizowane wnioski o nawiązanie stosunku pracy, po okresie, na jaki zostały przekazane dane do rekrutacji.

Jeśli zapadnie decyzja odmowna w sprawie wniosku (w całości lub w odniesieniu do określonego prawa), odpowiedź musi zawierać powody odrzucenia wniosku. Jeśli zdecydowano się na spełnienie żądania usunięcia przez "ograniczenie" danych osobowych, należy to wskazać i wyjaśnić w odpowiedzi.

Odpowiedź powinna zostać dostarczona w sposób zgodny z przepisami prawa właściwymi do komunikacji z osobami, których dane dotyczą lub w sposób, na który dana osoba wyraziła zgodę.

5) Realizacja wniosków w sprawie przeniesienia danych
Prawo do przenoszenia danych uprawnia wnioskodawcę do kopii danych w powszechnie używanym i nadającym się do odczytu komputerowego formacie.
Ma zastosowanie tylko w przypadku kiedy:

- dane osobowe są zapisywane elektronicznie (tj. nie ma zastosowania do plików papierowych); i
- dane osobowe zostały zebrane od osoby, której dane dotyczą; a także
- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie lub dane zostały przetworzone w celu wykonania umowy (lub czynności poprzedzających zawarcie umowy) z osobą fizyczną.

Jeśli osoba zwróciła się do WSM o przesłanie danych osobowych bezpośrednio do strony trzeciej, należy upewnić się, że otrzymane instrukcje są jasne i szczegółowe, w tym powinny uwzględniać informacje do kogo ze strony trzeciej należy przesłać dane osobowe oraz pisemne potwierdzenie od osoby składającej wniosek, że odbiorca spodziewa się danych osobowych. Jeśli nie uzyskano konkretnych instrukcji od osoby składającej wniosek, należy przesłać dane osobowe bezpośrednio do osoby składającej wniosek.
Wyższa Szkoła Menedżerska w Warszawie może utrzymywać dane osoby, której dane dotyczą, dotyczące otrzymanych zapytań i żądań oraz kopie wysłanych odpowiedzi, w celu prowadzenia dokumentacji i archiwizacji dotyczących zapytań i żądań od osoby, której dane dotyczą, a także wysłanych odpowiedzi pod warunkiem, że kontekst danych tej osoby będzie zrozumiały dla każdego pracownika Uczelni, który ma do nich dostęp. Dane takie powinny zostać usunięte niezwłocznie, w sytuacji kiedy dane takie nie spełniałyby dalej funkcji ewidencyjnej dla celów ochrony przed roszczeniami prawnymi.

12. Pozyskiwanie zgody na przetwarzanie danych osobowych

1) Aby uzyskać zgodę na przetwarzanie danych osoby, której one dotyczą, muszą zostać spełnione następujące warunki:

- dobrowolność: osoba, której dane dotyczą, musi mieć rzeczywisty wybór, czy wyrazić zgodę na przetwarzanie. Może to być wybór, czy w ogóle podać swoje dane osobowe, a także czy wyraża zgodę na ich przetwarzanie.
- konkretność: zgoda powinna być ograniczona do wyraźnie określonego celu lub celów przetwarzania. Zgoda na wiele celów nie powinna być "łączona", aby osoba, której dane dotyczą, mogła wyrazić zgodę wyłącznie na zasadzie "wszystko albo nic"; zamiast tego osoba, której dane dotyczą powinna mieć oddzielny wybór dla każdego celu.
- jednoznaczność: zgoda powinna wymagać pozytywnego działania ze strony osoby, której dane dotyczą. Zazwyczaj oznacza to zaznaczenie pola lub przesunięcie przełącznika lub wprowadzenie przez osobę, której dane dotyczą dodatkowych informacji, które nie będą wykorzystywane do celów innych niż przetwarzanie.
- odwoływalność: Osoba, której dane dotyczą, musi mieć możliwość wycofania swojej zgody w dowolnym czasie, na przykład poprzez usunięcie danych osobowych, zmianę ustawień swojego konta lub skontaktowanie się z WSM.

W przypadku danych osobowych Szczególnych kategorii zgoda musi być wyraźna, co oznacza, że musi być ona potwierdzona jednoznacznym w formie i treści oświadczeniem (ustnym lub pisemnym) przez osobę, której dane dotyczą, a nie tylko działaniem. Na przykład decyzja o podaniu opcjonalnych danych osobowych lub wyborze konkretnej usługi nie stanowi wyraźnej zgody, chyba że towarzyszy jej pole wyboru umożliwiające wyrażenie zgody na przetwarzanie.

2) W procesie pozyskiwania zgody oraz dalszego przetwarzania danych należy stosować się do zasad:

- Zasada ograniczenia celu przetwarzania
  Wyższa Szkoła Menedżerska w Warszawie powinna zbierać dane klienta tylko w konkretnym, wyraźnym i prawnie uzasadnionym celu.
  Jeżeli WSM przetwarza dane, osoby której dane dotyczą w sposób, który może być niezgodny z pierwotnym celem, dla którego został zebrany, Uczelnia jest zobligowana do uzyskania dobrowolnej, konkretnej, świadomej i jednoznacznej zgody osoby, której dane dotyczą na przetwarzanie lub dopilnowania, że osoba, której dane dotyczą, została poinformowana o możliwości nowego przetwarzania oraz, że WSM może zgodnie z zasadą zgodności z prawem przetwarzać dane osoby, której dane dotyczą nawet bez zgody tej osoby. Działanie takie będzie wymagało każdorazowo zatwierdzenia przez Inspektora Ochrony Danych.
  Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, WSM przed rozpoczęciem przetwarzania dokona oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

- Minimalizacja danych
  Ilość danych klienta zebranych lub wykorzystanych w dowolnym celu musi być ograniczona do wielkości niezbędnej służącej realizacji tego celu. W przypadku gromadzenia przez Wyższą Szkołę Menedżerską w Warszawie danych osoby, której dane dotyczą za pomocą standardowego formularza (w trybie online lub offline) każde pytanie w formularzu musi być bezpośrednio związane z celem, dla którego one zbierane.
  Jeśli WSM zamierza zebrać dodatkowe "opcjonalne" dane osoby, do której dane dotyczą w tym samym lub innym celu, Uczelnia musi wskazać tej osobie, jakie dane osobowe należy podać, a które są opcjonalne.

- Prawidłowość
  Wyższa Szkoła Menedżerska w Warszawie podejmuje działania skutkujące tym, że dane osoby, której dane dotyczą są kompletne, dokładne i aktualne. Witryny internetowe WSM powinny umożliwiać osobie, której dane dotyczą, poprawianie i aktualizowanie własnych danych, pod warunkiem, że będzie ona możliwa do zweryfikowania swojej tożsamości zanim podejmie działania z tym związane.
  Jeżeli Wyższa Szkoła Menedżerska w Warszawie w inny sposób pozyska informację, że dane osoby, do której dane dotyczą są niedokładne, niekompletne lub nieaktualne, musi podjąć uzasadnione kroki w celu skorygowania, uzupełnienia lub zaktualizowania tych danych. Uczelnia może również podejmować wewnętrzne kroki w celu utrzymania należytej jakości danych, w tym poprzez okresowe przeprowadzanie procesu czyszczenia danych.

WSM może utrzymywać dane osoby, której dane dotyczą, które są nieaktualne do celów prowadzenia dokumentacji i archiwizacji, pod warunkiem, że kontekst danych tej osoby będzie zrozumiały dla każdego pracownika Uczelni, który ma do nich dostęp.

- Ograniczenie przechowywania danych
  Wyższa Szkoła Menedżerska w Warszawie może przechowywać dane osoby, których dane dotyczą wyłącznie w możliwej do zidentyfikowania formie tak długo, jak jest to konieczne do celów, dla których zostały pierwotnie zebrane. Po upływie tego okresu dane osoby, których one dotyczą, powinny zostać usunięte lub zniszczone, lub poddane procesowi anonimizacji, tak, aby nie można było już zidentyfikować danej osoby.
  WSM może przechowywać dane osoby, której dane dotyczą przez dłuższe okresy, jeśli uzna to za konieczne w związku z postępowaniem sądowym lub potencjalnym postępowaniem sądowym. Długość tego okresu jest uzależniona każdorazowo od długości przewidywanego okresu przedawnienia roszczeń wynikających z zawartych umów.

- Stosowanie odpowiednich środków bezpieczeństwa danych
  Wyższa Szkoła Menedżerska w Warszawie musi stosować i utrzymywać odpowiednie środki techniczne i organizacyjne w celu ochrony danych osoby, której dane dotyczą przed nieuprawnionym dostępem i uniknięcia ich przypadkowej utraty, uszkodzenia lub zniszczenia. Środki te zostały opisane w niniejszej Polityce, a także w innych regulacjach wewnętrznych związanych choćby pośrednio z procesami przetwarzania danych osobowych.
  Podstawą wdrożenia adekwatnych do zagrożeń środków bezpieczeństwa są wyniki realizowanej na bieżąco analizy ryzyka, a na etapie wdrażania nowych rozwiązań organizacyjnych i informatycznych również wyniki procesów oceny skutków dla oceny prywatności i domyślnej ochrony danych. Za koordynację wymienionych działań odpowiada Inspektor Ochrony Danych.

- Rozliczalność
  Wszyscy pracownicy zatrudnieni w Wyższej Szkole Menedżerskiej w Warszawie mający dostęp do danych osobowych muszą przestrzegać niniejszej Polityki i powinni być w stanie wykazać przestrzeganie jej przepisów.

13. Elementy analizy ryzyka informacyjnego

Analiza ryzyka informacyjnego stanowi integralną część procesu zapewnienia bezpieczeństwa danych osobowych. Konkretne mechanizmy i zakresy odpowiedzialności zostały zawarte w odrębnych politykach i procedurach.
Wymienione poniżej elementy powinny być każdorazowo uwzględniane w ramach prowadzonej analizy ryzyka:

- mechanizmy dotyczące oceny ryzyka związanego z przetwarzaniem danych, które zawarte zostały w treści właściwych norm;

- mechanizmy dotyczące przeglądu stosowanych środków ochrony danych osobowych, w tym oceny ich skuteczności, które zostały zawarte w arkuszach analitycznych sporządzonych oddzielnie dla każdego z systemów przetwarzających dane osobowe;
- mechanizmy dotyczące kryteriów wyboru podmiotu przetwarzającego, pod kątem tego, czy zapewnia on adekwatne środki techniczne i organizacyjne, które została zawarte w procedurze outsourcingu;
- mechanizmy dotyczące bieżącej weryfikacji podmiotu przetwarzającego pod kątem spełniania wymagań przewidzianych przepisami Rozporządzenia ogólnego, a także wymagań umownych dotyczących zapewnienia bezpieczeństwa danych, w tym zasady dotyczące audytu zostały zawarte w procedurze outsourcingu oraz karcie audytu.

14. Wykaz stosowanych środków organizacyjnych i technicznych

1) Prowadzenie Rejestru czynności przetwarzania

Każdy Administrator oraz jego przedstawiciel (jeżeli istnieje) prowadzi i jest odpowiedzialny za Rejestr czynności przetwarzania danych osobowych. Obowiązek ten spoczywa również na podmiocie, któremu dane powierzono do przetwarzania. W Wyższej Szkole Menedżerskiej w Warszawie za prowadzenie rejestru odpowiedzialny jest Inspektor Ochrony Danych. Rejestr prowadzony jest zgodnie ze wzorem stanowiącym Załącznik Nr 1 do niniejszej Polityki.

2) Sposób przepływu danych pomiędzy poszczególnymi systemami

Przepływy informacyjne pomiędzy systemami są określone w Schemacie przepływów danych prowadzonym przez IOD. Przedmiotowy schemat może mieć postać graficzną lub tabelaryczną zgodną z wzorem określonym w Załączniku nr 2 do niniejszej Polityki. Opracowanie załącznika jest realizowane w ścisłej współpracy z Kierownikiem Działu IT.

3) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych

Środki techniczne i organizacyjne zostały określone w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie" wprowadzonej przez Rektora.

15. Analiza zagrożeń dla przetwarzanych i gromadzonych danych osobowych

Źródłem zagrożeń dla przetwarzanych danych osobowych mogą być min.:

- połączenie z siecią Internet;
- zdarzenia losowe (pożar, zalanie, odcięcie od źródeł zasilania, etc.)
- włamania do obiektów stanowiących obszar przetwarzania danych, kradzież sprzętu, dokumentów, etc.;
- błędy ludzkie takie np. jak:

- ujawnienie loginu i hasła do systemu informatycznego współpracownikom i osobom z zewnątrz,
- udostępnianie stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
- udostępnianie osobom nieuprawnionym dostępu do systemów informatycznych służących do przetwarzania danych osobowych,
- używanie oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
- nieautoryzowane przenoszenie programów komputerowych, dysków twardych z jednego stanowiska na inne,
- kopiowanie danych na zewnętrzne nośniki bez wymaganego zezwolenia,
- wynoszenie danych poza obszar ich legalnego przetwarzania,
- samowolne instalowanie i używanie jakichkolwiek programów komputerowych w szczególności programów do użytku prywatnego,
- używanie nośników danych udostępnionych przez osoby postronne,
- zapisywanie na dyskach sieciowych WSM plików nie związanych w sposób bezpośredni z wykonywaniem zadań Uczelni (zdjęcia prywatne, filmy, etc.),
- przesyłanie dokumentów i danych z wykorzystaniem konta pocztowego prywatnego,
- otwieranie załączników i wiadomości poczty elektronicznej od nieznanych i niezaufanych nadawców,
- tworzenie kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania,
- narażenie sprzętu i nośników danych na kradzież (w tym pozostawienie komputera przenośnego w miejscu publicznym, w samochodzie, bez zabezpieczenia),
- wyrzucanie nośników danych każdego rodzaju, w tym dokumentów papierowych zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia uniemożliwiającego ich odtworzenie,
- pozostawianie dokumentów na biurku, albo w innym niezabezpieczonym przed dostępem osób nieuprawnionych po zakończonej pracy, pozostawianie otwartych dokumentów elektronicznych na ekranie monitora bez blokady konsoli,
- ignorowanie nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
- ignorowanie przepisów niniejszej Polityki oraz innych regulacji oraz wytycznych i zaleceń z zakresu ochrony danych osobowych,
- nie wylogowanie się z systemu komputerowego przed opuszczeniem miejsca pracy,
- ustawienie monitora komputerowego, w sposób umożliwiający wgląd osobom postronnym,
- pozostawianie bez nadzoru osób spoza grona pracowników Uczelni przebywających w obszarze przetwarzania danych osobowych,
- pozostawienie zewnętrznych nośników informacji podłączonych do komputera np. zewnętrzny dysk, pamięć flash i płyty w napędzie,
- zapisywanie na kartkach haseł i pozostawianie ich w miejscach widocznych dla innych osób,
- pozostawianie dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach lub w centrach wydruku,
- pozostawianie kluczy w drzwiach, szafach, biurkach, zostawianie otwartych pomieszczeń, w których przetwarza się dane osobowe.

16. Reguły odnoszące się do ochrony danych osobowych przetwarzanych w formie elektronicznej

1) Uwzględniając fakt przetwarzania w Wyższej Szkole Menedżerskiej w Warszawie danych osobowych, nie wykluczając danych Szczególnych kategorii, wprowadza się najwyższe wymagane standardy ich ochrony i zabezpieczenia. Obowiązują w tym zakresie wymienione poniżej zasady:

- każdy system informatyczny służący do przetwarzania danych osobowych jest chroniony przed zagrożeniami pochodzącymi z sieci publicznej, poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym do niego dostępem.
- stosuje się mechanizmy kontroli dostępu do danych osobowych, wprowadzając ustalony imiennie dla każdego użytkownika systemu odrębny identyfikator. Dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia poprzez wprowadzenie hasła;
- system informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed działaniem tzw. złośliwego oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed utratą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
- urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji należy wcześniej pozbawić zapisów tych danych. W przypadku, gdy nie jest to możliwe, uszkodzić w sposób uniemożliwiający ich odczytanie;
- w razie konieczności naprawy zachować szczególną ostrożność, aby nie doszło do ujawnienia danych osobowych. Ostatecznie pozbawić wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie;
- pracownik użytkujący komputer przenośny zawierający dane osobowe powinien zachować szczególną ostrożność podczas jego transportu i przechowywania poza obszarem przetwarzania danych osobowych.

2) Środki ochrony w zakresie zabezpieczenia sprzętowego

Do przetwarzania danych osobowych stosowany winien być sprzęt informatyczny, systematycznie wymieniany stosownie do dokonującego się postępu technologicznego. Poszczególne składniki infrastruktury sprzętowej powinny się charakteryzować co najmniej:

- serwery powinny być wyposażone w pamięć operacyjną z detekcją błędów, redundantne zasilacze, dyski hot-swap;
- zapis na dyskach serwerów winien być redundantny,
- system firewall;

- zasilanie serwerów oraz stacji roboczych wskazanych kluczowych pracowników Uczelni powinien być zabezpieczony w źródło zasilania awaryjnego;
- sieć lokalna powinna być poddana segmentacji;
- mechanizm wykonywania kopii zapasowych winien być realizowany w oparciu o ściśle realizowany schemat;
- miejsce pracy serwerów winno być zabezpieczone skutecznym systemem klimatyzacji
- pomieszczenia serwerowni winny być wyposażone w skuteczny i automatycznie uruchamiany system gaszenia pożaru, system alarmowy/antywłamaniowy wraz z monitoringiem wizyjnym.

2) Środki ochrony w ramach oprogramowania urządzeń teletransmisji
W tym zakresie stosuje się:

- wielopoziomową filtrację na routerach wg adresów, protokołów i usług;
- translację adresów IP;
- dopuszczenie do komunikacji wyłącznie protokołów, które są niezbędne do zachowania złożonej funkcjonalności systemu;
- zabezpieczenia dostępu do urządzeń aktywnych.

3) Środki ochrony w ramach oprogramowania systemu
W tym zakresie stosuje się:

- zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii zapasowych;
- w celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych;
- system informatyczny powinien pozwalać na definiowanie odpowiednich praw dostępu do zasobów informatycznych;
- w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło;
- rejestracja nieudanych prób logowania do systemu;
- w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją;
- oprogramowanie antywirusowe jest stale aktywne, a baza definicji wirusów regularnie aktualizowana;
- kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.

17. Ochrona danych osobowych przetwarzanych w formie papierowej

Dane osobowe przetwarzane i gromadzone przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach. Dane te należy przechowywać w szafach zamykanych na klucz lub w sejfach, kasetkach, itp.

Obszar przetwarzania i gromadzenia danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych jest dopuszczalne za zgodą Administratora w obecności pracowników Uczelni.

Sposób postępowania z kluczami do pomieszczeń i szaf został opisany w rozdziale poświęconym ochronie fizycznej pomieszczeń, w których przetwarza się dane osobowe.

18. Procedura nadawania upoważnień do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora.
   Upoważnienie do przetwarzania danych osobowych wydawane jest w formie pisemnej, na czas określony w jego treści. Ważność upoważnienia ustaje automatycznie w dniu rozwiązania stosunku pracy, stosunku zlecenia lub innego stosunku prawnego łączącego daną osobę z Wyższą Szkołą Menedżerską w Warszawie.

2) Przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych należy:
   - zapoznać go z wykazem przepisów dotyczących ochrony danych osobowych, oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Uczelni,
   - przyjąć – po zapoznaniu się pracownika w wyznaczonym okresie czasu z przekazanymi mu przez IOD materiałami dot. ochrony danych osobowych w WSM stosowne pisemne oświadczenie według wzoru określonego w Załączniku nr 3 do niniejszej Polityki,
   - wydać upoważnienie do przetwarzania danych osobowych w konkretnych zasobach, w zakresie niezbędnym do wykonania zadań na zajmowanym stanowisku (Załącznik nr 4 do Polityki).

3) IOD jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w w/w zakresie.
   Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona w formie elektronicznej zgodnie ze wzorem stanowiącym Załącznik nr 5 do niniejszej Polityki.

4) Dopuszcza się możliwość upoważniania do przetwarzania danych osobowych osób będących pracownikami firm zewnętrznych, które wykonują zadania na rzecz WSM w obszarze, gdzie przetwarza się dane osobowe. Każdorazowo zakres upoważnienia określa umowa.

19. Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

1) Obszarem, w którym przetwarzane są dane osobowe jest siedziba Wyższej Szkoły Menedżerskiej w Warszawie lub inne pomieszczenia, do których Uczelnia posiada tytuł prawny, a także miejsca zajmowane przez podmioty, którym dane powierzono do przetwarzania. Obszar przetwarzania danych osobowych dzieli się na obszar podlegający ochronie standardowej i obszar podlegający ochronie w sposób szczególny. Za strefy szczególnie chronione uznaje się pomieszczenia zajmowane przez Rektora oraz Dział IT. Miejsca te muszą być zamykane w sposób uniemożliwiający dostęp do tych stref osobom nieupoważnionym i zabezpieczone elektronicznym systemem kontroli dostępu.
IOD może przeprowadzać bezpośrednią kontrolę stanu zabezpieczeń fizycznych zbiorów danych osobowych oraz zgłaszać do Administratora, lub bezpośrednio do właściwego kierującego jednostką organizacyjną swoje uwagi, a także rekomendować zlecenie kontroli specjalistycznej firmie.
Kierujący poszczególnymi jednostkami organizacyjnymi odpowiadają za należyte zabezpieczenie fizyczne zasobów danych osobowych w podległych im jednostkach.
Za prowadzenie aktualnego wykazu pomieszczeń, w których przetwarzane są dane osobowe jest odpowiedzialny IOD. Wzór wykazu zawiera Załącznik nr 6.
Przebywanie wewnątrz obszaru, o którym mowa w ust. 1, osób nieupoważnionych do dostępu do danych osobowych jest możliwe tylko w obecności osoby posiadającej aktualne upoważnienie do przetwarzania tych danych.
Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do przetwarzania tych danych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
Pomieszczenia, o których mowa w niniejszym ustępie powinny mieć następujące zabezpieczenia:

- drzwi do pomieszczeń, w których przetwarzane są dane osobowe są zamykane na klucz;
- dokumenty z danymi osobowymi poza godzinami pracy powinny być zamykane na klucz w szafach, lub szufladach biurek. Dokumenty zawierające Dane szczególnych kategorii podlegają szczególnej ochronie. W szczególności niedopuszczalne jest nawet chwilowe pozostawienie tego rodzaju danych bez nadzoru osoby posiadającej upoważnienie do ich przetwarzania;
- w sytuacji braku w pomieszczeniu zamykanej na klucz szafy, stosować należy inne skuteczne środki zabezpieczające zgromadzone dane przed ich nieuprawnionym udostępnieniem osobom nieupoważnionym, w szczególności nie należy dopuszczać do pozostawiania dokumentów z danymi na blatach biurek, a także pozostawiać ekranów monitorów komputerowych bez włączonego wygaszacza;
- pomieszczenia muszą podlegać ochronie i monitorowaniu przez pracowników ochrony w systemie 24 godzinnym przez wszystkie dni w roku.

2) Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru, o którym mowa w pkt. 1.

3) Pracownik może przebywać w pomieszczeniach służbowych po godzinach pracy lub w dniach wolnych od pracy tylko po uzyskaniu zgody swojego bezpośredniego przełożonego.

4) Fakt przebywania osób nieupoważnionych w pomieszczeniach podlegających Kierownikowi Działu IT odnotowany jest w odrębnej ewidencji.

5) Po zakończeniu pracy osoby odpowiedzialne za pomieszczenia, w których są przetwarzane dane osobowe, są obowiązane sprawdzić zamknięcie szaf i pomieszczeń.

20. Ogólne zasady powierzania danych osobowych

1) Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 RODO, na podstawie pisemnej umowy zawartej pomiędzy Wyższą Szkołą Menedżerską w Warszawie, a danym podmiotem, któremu zleca się dokonanie określonych czynności związanych z przetwarzaniem danych osobowych, w celu ściśle oznaczonym.

2) W procesie wyboru podmiotu przetwarzającego należy brać pod uwagę to, aby podmiot ten zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi prawne.

3) Projekt umowy powierzenia danych osobowych innemu podmiotowi do przetwarzania przygotowuje IOD, uwzględniając w tym zakresie następujące warunki:
- podmiot przetwarzający może je przetwarzać wyłącznie w zakresie i celu przewidzianym w umowie;
- podmiot przetwarzający jest obowiązany przed rozpoczęciem przetwarzania danych spełnić ustalone środki zabezpieczające dane,
- podmiot przetwarzający jest obowiązany wyrazić zgodę na poddanie się audytowi Administratora, odnośnie prawidłowości przestrzegania przepisów zawartej umowy powierzenia danych,
- podmiot przetwarzający jest zobowiązany wyrazić gotowość do pomocy Administratorowi w realizacji jego obowiązków wynikających z przepisów prawa,
- umowa powinna zawierać zapisy dotyczące zachowania poufności oraz trybu nadawania upoważnień do przetwarzania danych osobowych.

3) Projekt umowy określonej w ust 2 parafują:
- Inspektor Ochrony Danych,
- Kierownik Działu IT (gdy dotyczy powierzania danych przetwarzanych w systemach informatycznych),
- Kierujący właściwą jednostką organizacyjną Uczelni której dotyczy umowa i przetwarzane na jej podstawie dane osobowe .

Zaparafowany projekt umowy jest przedkładany przez IOD do akceptacji i podpisania władzom Uczelni.

21. Zasady doskonalenia dokumentacji bezpieczeństwa danych osobowych

Podstawą wprowadzania zmian w treści niniejszej Polityki oraz wszystkich innych składników dokumentacji bezpieczeństwa danych osobowych w WSM są wyniki analizy

ryzyka, które wskazać mogą zagrożenia związane z obniżeniem się poziomu bezpieczeństwa informacyjnego, poniżej poziomu akceptowanego przez Rektora. Głównymi przesłankami takiej sytuacji mogą być w szczególności:

- zmiany przepisów prawa;
- zasadnicze zmiany w zakresie ustawowych zadań Uczelni, a także jej zadań własnych;
- istotne zmiany w strukturze wewnętrznej i organizacji Uczelni;
- istotne zmiany narzędzi i metod przetwarzania informacji w WSM;
- zmiany celu przetwarzania danych (szczególnie danych osobowych), a także zakresu tego przetwarzania;
- stwierdzonej, nasilonej, skutecznej i nielegalnej penetracji zasobów informacyjnych Uczelni.

Za opracowanie propozycji zmian w treści dokumentacji, o której mowa w punkcie poprzedzającym odpowiada Inspektor Ochrony Danych, który co najmniej raz w roku dokonuje cyklicznego przeglądu Polityki w kontekście wyszczególnionych powyżej przesłanek. Zmiany w treści tej dokumentacji dokonywane są w formie Zarządzenia Rektora.

22. Odniesienia do innych dokumentów i procedur

Polityka Bezpieczeństwa Danych Osobowych znajduje swoje rozwinięcie w treści innych składników dokumentacji bezpieczeństwa informacyjnego, które powinny być zgodne z zasadami i regułami w niej określonymi.
Do najważniejszych dokumentów w tym zakresie zaliczyć należy:

- Instrukcja zarządzania systemem informatycznym do przetwarzania danych osobowych;
- Regulamin korzystania z poczty elektronicznej oraz sieci Internet przez pracowników WSM oraz osoby z nią współpracujące;
- Procedura zarządzania incydentami bezpieczeństwa informacyjnego.

23. Załączniki

Załącznik Nr 1

Wzór rejestru czynności przetwarzania

Nazwa procesu	Administrator				Cele przetwarzania	Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Kategorie odbiorców danych	Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	[illegible]	Planowane terminy usunięcia danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Inne szczególne środki bezpieczeństwa danych			
	Administrator (nazwa, adres, dane kontaktowe)	Współadministrator (nazwa, adres, dane kontaktowe)	Przedstawiciel administratora	Inspektor ochrony danych (imię, nazwisko, dane kontaktowe)									Zastosowano pseudonimizację i szyfrowanie danych	Zapewniono zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego	Zapewniono zdolność do stałego zapewnienia poufności, integralności i dostępności systemów i usług przetwarzania	Zapewniono testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania
Obsługa kadrowa pracowników Uczelni	Wyższa Szkoła Menedżerska w Warszawie, ul. Kawęczyńska 36, 03-772 Warszawa	brak	brak	Jan Kowalski, tel.: 22/5555555, e-mail: iod@wsm.warszawa.pl	Realizacja obowiązków wynikających ze stosunku pracy	Osoby zatrudnione na podstawie umowy o pracę	dane osobowe tzw. zwykłe oraz dane szczególnych kategorii (dane o stanie zdrowia)	Podmioty i organy uprawnione na podstawie konkretnych przepisów prawa	nie dotyczy	nie dotyczy	50 lat od daty ustania stosunku pracy	Szafy metalowe zamykane na klucz, zabezpieczone przed dostępem osób nieuprawnionych. System informatyczny zabezpieczony przed nieuprawnionym dostępem loginem i hasłem użytkownika	nie	tak	tak	tak

Załącznik nr 2

Sposób przepływu danych pomiędzy poszczególnymi systemami (przykład)

System (Moduł) A	System (Moduł) B	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Program Kadry - Płace	Program Płatnik	Jednokierunkowo z Programu Kadry - Płace do programu Płatnik	Półautomatycznie – eksport pliku z programu kadrowo – płacowego na serwer, który następnie pobierany jest przez program Płatnik

Załącznik nr 3

Wzór oświadczenia osoby o zachowaniu w tajemnicy danych osobowych

OŚWIADCZENIE

Ja niżej podpisany(a) ..... oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań	*)
zadań i obowiązków służbowych wynikających z umowy o pracę	
zadań wynikających z umowy cywilnoprawnej	
zadań wynikających z umowy praktyki	

*) we właściwym miejscu wstawić znak „x"

zarówno w trakcie wykonywania umowy jak i po jej ustaniu.
Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Wyższej Szkole Menedżerskiej w Warszawie dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia służbowego nie będę wykorzystywał(a) danych osobowych ze zbiorów WSM.
Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Wyższej Szkole Menedżerskiej w Warszawie zasadach dotyczących przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa Danych Osobowych.
Oświadczam, że zostałem(am) zapoznany(a) z przepisami o ochronie danych osobowych oraz o grożących mi konsekwencjach w przypadku ich chociażby nieumyślnego naruszenia.

....., dn. .....r.

data i miejsce złożenia oświadczenia

.....
podpis osoby składającej oświadczenie

Załącznik nr 4
Upoważnienie dla pracownika do przetwarzania danych osobowych

UPOWAŻNIENIE nr ...../.....

Na podstawie § 7 ust. 3 Polityki Bezpieczeństwa Danych Osobowych (Zarządzenie Nr .../..... Rektora Wyższej Szkoły Menedżerskiej w Warszawie z dnia ..... 2018 r.)
Upoważniam

Pana/Panią .....

do przetwarzania danych osobowych będących w zasobach
.....
(nazwa jednostki organizacyjnej)

Upoważnienie ma zastosowanie do przetwarzania danych w formach:
- elektronicznej
- papierowej*.

Zakres upoważnienia obejmuje następujące poziomy dostępu:
- odczyt
- zapis
- modyfikacja
- drukowanie
- usuwanie (niszczenie) *

Informuję, że z chwilą wydania upoważnienia jest Pan/Pani do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał(a) Pan/Pani dostęp w związku z wykonywaniem obowiązków służbowych, jak również sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia w WSM.
Upoważnienie wydano na okres ..... .

....
miejscowość, data podpis

nr pomieszczenia, w którym dana osoba pracuje ----------
nr telefonu ----------

*niepotrzebne skreślić

Załącznik nr 5

Wzór ewidencji osób upoważnionych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Jednostka organizacyjna : np.. Administacja

stan na dzień .....

0	2	3		3	4	ZAKRES UPOWAŻNIENIA					5	6	7	10	11		12	12
			Zatrudnienie								Lokalizacja			Data				
LP	Nazwisko	Imię	Umowa o pracę Zlecenie Dzieło Praktyki	Stanowisko - funkcja	Nazwa działu	O	Z	M	D	U	Budynek	kondygnacja	numer pokoju	nadania ostatniego upoważnienia	ustania upoważnienia	Data złożenia oświadczenia	Identyfikator	Uwagi
N.p.	**Kowalski**	Jan	U	Referent	Dziekanat						F	0	F001				jan.kowalski	
Adm/1																		
Adm/2																		
Adm/3																		
Adm/4																		
Adm/5																		
Adm/6																		
Adm/7																		

Załącznik nr 6

Wzór wykazu pomieszczeń, w których przetwarzane są dane osobowe

Wykaz pomieszczeń w których przetwarzane są dane osobowe

0	1	2	3	4	Kierownik jednostki		6					7
	Lokalizacja											
LP	Budynek	kondygnacja	numer pokoju	Nazwa działu	osoby zatrudnione	forma przechowywania danych	Sposób zabezpieczenia pomieszczenia		Ilość stanowisk pracy	mail	telefon	Uwagi

Zatwierdzam :

REKTOR

prof. zw. dr hab. Paweł Czarnecki

Załącznik nr 2 do zarządzenia Rektora WSM 2/05/2018 r. z dnia 22 maja 2018 r

INSTRUKCJA zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie

Spis treści:

Rozdział 1

Postanowienia ogólne

§ 1

Niniejsza „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie" zwana dalej **Instrukcją,** ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Wyższej Szkole Menedżerskiej w Warszawie, w celu ich bezpiecznego wykorzystywania oraz zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem. .

§ 2

Instrukcja została opracowana na podstawie art. 66 ust.2 ustawy z dnia 27 lipca 2005 roku Prawo o szkolnictwie wyższym. (tj. Dz. U. z 2012 r., poz. 572, z późń. zm.), art. 3 ust 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

§ 3

Określenia i skróty użyte w Instrukcji oznaczają:

1. **Administrator Danych Osobowych –** Rektor Wyższej Szkoły Menedżerskiej w Warszawie, zwany

dalej **ADO .**

2. **Inspektor Ochrony Danych Osobowych** - osoba wyznaczona przez **Administratora Danych Osobowych**, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, zwana dalej **IODO.**
3. **Administrator Systemów Informatycznych** - osoba wyznaczona przez **ADO**, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych, zwany dalej **ASI.**
4. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
5. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
6. **Osoba upoważniona lub użytkownik systemu** - osoba posiadająca upoważnienie wydane przez **ADO** lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej **użytkownikiem.**
7. **Przełożony użytkownika** - kierownik komórki organizacyjnej **WSM** , zwany dalej **przełożonym**.
8. **Osoba uprawniona – osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.**
9. **Użytkownik uprzywilejowany** – osoba posiadająca najwyższy stopień uprawnień do zarządzania systemem informatycznym.

§ 4

1. **ADO** może upoważnić inną osobę, zatrudnioną w **WSM** do wykonywania określonych czynności, leżących w zakresie realizacji zadań Administratora.
2. Kontrola prawidłowości wykonywania czynności, o których mowa w ust. 1, należy do **ADO** lub osoby uprawnionej.
3. Osoba, o której mowa w ust. 1, informuje **IODO** lub osoby uprawnione o podjętych przez siebie czynnościach.

Rozdział 2

Procedury związane z zarządzaniem systemem informatycznym służącym do przetwarzania danych osobowych w WSM

§ 1

Nadawanie uprawnień i wyrejestrowywanie użytkowników.

1 Nadawanie i rejestrowanie uprawnień

1) Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie upoważniony do przetwarzania danych osobowych, zarejestrowany jako użytkownik w tym systemie przez administratora systemu na wniosek kierownika działu kadr lub kierownika działu.

Administrator systemu jest obowiązany upoważnić co najmniej jednego pracownika działu informatyki do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 14 dni.

Rejestracja użytkownika, o której mowa w ppkt 1), polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do ewidencji użytkowników systemu.

Administrator systemu albo upoważniony pracownik, o którym mowa w ppkt. 2), przekazuje do działu kadr informację o identyfikatorze, który został nadany użytkownikowi.

2 Wyrejestrowywanie uprawnień

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek kierownika działu kadr.
2) Wyrejestrowanie, o którym mowa w ppkt. 1), może mieć charakter czasowy lub trwały.
3) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4) Wyrejestrowanie czasowe musi nastąpić w przypadku:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych.

Wyrejestrowanie czasowe może nastąpić w przypadku:

a) wypowiedzenia umowy o pracy,
b) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.

Wyrejestrowanie trwałe następuje w przypadku rozwiązania lub wygaśnięcia stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.

Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

2. W celu zarządzania metodami oraz środkami uwierzytelniania mają zastosowanie *(załącznik nr **1**)*:
   a) „Procedura uwierzytelniania użytkownika w systemie informatycznym"
   b) „Procedura rejestrowania /wyrejestrowania użytkownika z systemu informatycznego".

3. W celu rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym mają zastosowanie następujące procedury (załącznik nr 2):

   1. Procedura rozpoczęcia pracy w systemie informatycznym
   2. Procedura zawieszenia/odwieszenia pracy w systemie informatycznym
   3. Procedura zakończenia pracy w systemie informatycznym

4. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych ma zastosowanie

procedura postępowania w sytuacjach naruszenia ochrony danych osobowych.

1. **Procedura postępowania w sytuacjach naruszenia ochrony danych osobowych**
    1. Na fakt naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:
        1. Stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem).
        2. Wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach).
        3. Różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych).
        4. Jakości komunikacji w sieci telekomunikacyjnej (gwałtowne opóźnienia lub przyśpieszenia wykonywanych czynności).
        5. Stwierdzenie obecności w systemie nowego oprogramowania bądź oprogramowania niewiadomego pochodzenia
        6. Pojawienie się w systemie nowych procesów.
        7. Inne sytuacje nadzwyczajne.
    2. W przypadku podejrzenia naruszenia zabezpieczenia systemu informatycznego użytkownik niezwłocznie powiadamia bezpośredniego przełożonego oraz **IODO**.
    3. **IODO** niezwłocznie wszczyna postępowanie wyjaśniające.
    4. Wyniki postępowania wyjaśniającego są zapisywane w formie notatki służbowej, jeżeli **IODO** stwierdzi faktyczne naruszenie zabezpieczenia systemu informatycznego.
    5. Treść notatki **IODO** przekazuje do wiadomości Administratorowi.

5. W celu zabezpieczenia danych i programów służących do przetwarzania danych osobowych ma zastosowanie poniższa

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1. Kopie zapasowe są tworzone codziennie przez Dział Informatyki WSM po zakończeniu dnia pracy. Kopie pełnie wykonywane są nie rzadziej niż raz na tydzień, kopie zapasowe dzienne mogą być kopiami przyrostowymi.
2. Nośniki z kopiami zapasowymi są przechowywane w pomieszczeniach Działu Informatyki pod nadzorem **IODO**.
3. Kopie zapasowe są tworzone w cyklu miesięcznym nie rzadszym niż tygodniowy. Po tym okresie nośniki są kasowane i ponownie wykorzystywane do tworzenia kopii zapasowych.
4. Kopie zapasowe są okresowo sprawdzane pod kątem ich dalszej przydatności.
5. Na koniec każdego miesiąca Dział Informatyki tworzy kopię miesięczną na nośnikach trwałych
6. Kopie miesięczne są przechowywane przez okres co najmniej 5 lat.
7. Po okresie przechowywania kopie miesięczne podlegają komisyjnej likwidacji poprzez ich fizyczne zniszczenie. W komisji likwidacyjnej biorą udział **IODO** i/lub **ASI**.

Rozdział 3

Inne uregulowania związane z przetwarzaniem danych osobowych w Wyższej Szkole Menedżerskiej

§ 1

1. W celu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego Wyższa Szkoła Menedżerska wykorzystuje:
    1. Oprogramowanie antywirusowe na serwerze mailowym.
    2. Oprogramowanie na stacjach roboczych.
    3. Oprogramowanie ograniczające niepożądany ruch w sieci.
    4. Fizyczne rozdzielenie sieci zawierającej dane osobowe od sieci ogólnodostępnej.
    5. Logiczny podział sieci uwzględniający komórki organizacyjne.

2. Aktualizacja wyżej wymienionego oprogramowania jest automatyczna. Bazy wirusów są aktualizowane niezwłocznie po opublikowaniu nowej bazy wirusów.

§ 2

1. Systemy informatyczne oraz nośniki informacji służące do przetwarzania danych eksploatowane w WSM podlegają okresowym przeglądom i konserwacjom.
2. Do dokonywania przeglądów i konserwacji uprawniony jest Dział Informatyki pod nadzorem **IODO**.
3. W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem w celu naprawy innemu podmiotowi pozbawiane są zawartości.
4. W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są uszkadzane w sposób uniemożliwiający odczytanie danych.
5. Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem **IODO** lub **ASI**.

§ 3

Wszelkie wydruki zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie czasu ich przydatności są niszczone przy użyciu niszczarek lub przez wyspecjalizowane firmy posiadające odpowiednie certyfikaty.

§ 4

1. Wykorzystywanie sieci komputerowej w celach innych niż wyznaczone przez **Władze WSM** jest zabronione.

2. Zabroniona jest także samowolna instalacja oprogramowania na stacjach roboczych przez użytkowników

Rozdział 4

Postanowienia końcowe

§ 1

1. Niniejsza Instrukcja przeznaczona jest dla użytkowników i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.
2. Wykonanie postanowień Instrukcji ma na celu wprowadzenie jednolitego systemu zarządzania systemem informatycznym w WSM.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się i stosować do zasad i procedur określonych niniejszym dokumentem.
4. Naruszenie zasad i procedur określonych w niniejszym dokumencie może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
5. Naruszenie zasad i procedur określonych w niniejszym dokumencie może być potraktowane jako nienależyte wykonanie umowy w rozumieniu Kodeksu cywilnego.
6. Nośniki informacji w rozumieniu § 5 pkt 5 lit. a rozporządzenia 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*) są przechowywane w pomieszczeniach Działu Informatyki.

REKTOR
prof. zw. dr hab. Paweł Czarnecki

Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym

Procedura uwierzytelniania użytkownika w systemie informatycznym

1. Niepowtarzalny identyfikator oraz pierwsze hasło jest przydzielone użytkownikowi przez **ASI** po nadaniu uprawnień do przetwarzania danych osobowych.
2. Pierwsze hasło jest przekazane przez **ASI** użytkownikowi systemu w formie pisemnej.
3. Użytkownik po otrzymaniu pierwszego hasła jest zobowiązany do niezwłocznej jego zmiany .
4. Bezpośredni dostęp do danych użytkownik uzyskuje po podaniu identyfikatora i właściwego hasła.
5. Hasła w systemie informatycznym musza być przechowywane w postaci zaszyfrowanej .
6. Hasła użytkowników uprzywilejowanych pozostają do wyłącznej wiadomości wybranych pracowników Działu Informatyki WSM. Ich pisemna wersja przechowywana jest zaklejonej kopercie w sejfie Kanclerza WSM.
7. Osobą odpowiedzialną za rejestrowanie oraz wyrejestrowywanie użytkowników jest ASI bądź osoba spośród pracowników Działu Informatyki WSM przez ASI do tego upoważniona.
8. Hasła administratorów systemów informatycznych przechowywane są w szafie pancernej Kasy WSM i ich awaryjne użycie odnotowywane jest każdorazowo przez ABI w specjalnym rejestrze .

Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego

1. Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez **ASI**, gdy uzyskują lub tracą prawo dostępu do systemu, zgodnie z procedurą nadawania/cofania uprawnień do przetwarzania danych osobowych.
2. Identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez **ASI**.
3. Ustanie stosunku pracy powoduje wyrejestrowanie użytkownika przez ASI. Odchodzący pracownik wypełnia kartę obiegową w wyznaczonych komórkach organizacyjnych.

   Podstawą wypełnienia karty obiegowej przez ASI jest trwałe usunięcie użytkownika z systemu.
4. Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie .

Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym

Procedura rozpoczęcia pracy w systemie informatycznym

2. W celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania hasła dostępu do systemu.
3. Podczas pierwszego uwierzytelniania w systemie użytkownik ma obowiązek zmiany hasła.
4. Hasło składa się co najmniej z 6 znaków. Jego długość jest uzależniona od poziomu bezpieczeństwa i zasad stosowanych w odpowiednich systemach informatycznych.
5. Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 30 dni kalendarzowych.
6. Zabrania się wpisywania hasła lub jego zmiany w obecności innych osób.
7. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.
8. W przypadku zagubienia hasła użytkownik musi skontaktować się z **ASI** w celu uzyskania nowego hasła.
9. Użytkownikowi nie wolno udostępniać swoich haseł innym osobom.

Procedura zawieszenia/odwieszenia pracy w systemie informatycznym

2. W celu zawieszenia pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wyrejestrowania się z systemu.
3. W przypadku konieczności odejścia od stanowiska pracy, po wyrejestrowaniu się z systemu użytkownik jest zobowiązany zablokować pulpit.
4. W celu ponownego uwierzytelnienia w systemie użytkownik odblokowuje pulpit i rozpoczyna pracę w systemie informatycznym zgodnie z procedurą rozpoczęcia pracy w systemie informatycznym.
5. Zabrania się pozostawiania stanowiska komputerowego z uruchomionym systemem bez kontroli pracującego na nim użytkownika.

Procedura zakończenia pracy w systemie informatycznym

2. W celu zakończenia pracy w systemie informatycznym użytkownik wyrejestrowuje się z programu służącego do obsługi danych osobowych.
3. Użytkownik zamyka sesję użytkownika w systemie operacyjnym (wylogowuje się) i o ile jest to konieczne, wyłącza komputer.

Wyższa Szkoła Menedżerska
w Warszawie

Załącznik 3 do
Zarządzenia Rektora WSM nr 2/05/2018 z dnia 22 maja 2018 r.

Regulamin korzystania z firmowej poczty elektronicznej i sieci Internet przez pracowników Wyższej Szkoły Menedżerskiej w Warszawie oraz osoby z nim współpracujące

§ 1. Definicje i skróty

W treści niniejszej Instrukcji zastosowanie mają definicje zawarte w rozdziale 1 Polityki Bezpieczeństwa Danych Osobowych oraz definicje i skróty wyszczególnione poniżej:

1. Uczelnia lub WSM – oznacza Wyższą Szkołę Menedżerską w Warszawie;
2. Regulamin – oznacza niniejszy Regulamin;
3. Poczta elektroniczna WSM (system poczty elektronicznej) – oznacza usługę teleinformatyczną, służącą do wymiany wiadomości zarówno z adresatami w WSM, jak również z adresatami w innych, zewnętrznych systemach poczty elektronicznej;
4. Internet – oznacza wszelkie zasoby informacyjne ogólnoświatowej sieci teleinformatycznej Internet, do których może mieć dostęp pracownik Użytkownik lub inna osoba, której takie uprawnienia nadano;
5. Użytkownik – oznacza pracownika WSM, który zgodnie z przepisami Regulaminu otrzymał prawo dostępu do korzystania z systemu poczty elektronicznej WSM i/lub dostępu do Internetu, a także inną osobę, której takie uprawnienia nadano w związku z zawartą z WSM umową;
6. Administrator poczty elektronicznej WSM – oznacza pracownika Działu IT odpowiedzialnego za zarządzanie systemem poczty elektronicznej Wyższej Szkoły Menedżerskiej w Warszawie.

7. Komputer – oznacza stację roboczą zainstalowaną w siedzibie WSM (tzw. desktop), komputer przenośny (laptop), a także każdego innego rodzaju sprzęt mobilny służący umożliwiający łączenie się siecią z Internet.

§ 2. Zakres Regulaminu.

Regulamin określa ogólne zasady korzystania z systemu poczty elektronicznej oraz sieci Internet. Regulamin precyzuje również zakres i uprawnienia kontrolne WSM dotyczące służbowej korespondencji Użytkowników oraz korzystania z sieci Internet.

§ 3. Procedura przyznawania firmowego adresu poczty elektronicznej.

1. Adres poczty elektronicznej nowo zatrudnionego pracownika WSM, na wniosek jego bezpośredniego przełożonego, tworzy Administrator poczty elektronicznej WSM według następującego wzorca: imię.nazwisko@wsm.warszawa.pl , np. *jan.nowak@wsm.warszawa.pl*
2. Administrator poczty elektronicznej WSM przekazuje Użytkownikowi informacje niezbędne do pierwszego logowania i w razie potrzeby przeprowadza instruktaż korzystania z poczty elektronicznej.
3. Użytkownik zobowiązany jest do zachowania hasła do poczty w poufności. W przypadku rozmyślnego, bądź przypadkowego ujawnienia hasła osobom trzecim, pracownik WSM powinien niezwłocznie poinformować o tym fakcie Administratora poczty elektronicznej lub innego pracownika Działu IT.
4. Możliwy jest zdalny dostęp do systemu poczty elektronicznej (spoza siedziby WSM). Dostęp taki posiadają wszyscy pracownicy w WSM pełniący funkcje kierownicze lub pracujący na stanowiskach samodzielnych. Pozostałym pracownikom ww. uprawnienia nadaje osoba kierująca daną jednostką organizacyjną, kierując się potrzebami w zakresie zapewnienia pracownikowi możliwości prawidłowego toku realizacji powierzonych zadań służbowych, również poza siedzibą Uczelni. W przypadku Użytkowników nie będących pracownikami WSM, uprawnienia takie nadaje Kanclerz WSM.
5. Nadanie uprawnień do zdalnego dostępu do firmowej poczty elektronicznej następuje w drodze pisemnego powiadomienia o tym fakcie Kierownika Działu IT, który prowadzi rejestr osób, którym taki dostęp przyznano.
6. Prawo wglądu do rejestru określonego w ustępie 5 posiada również IOD.
7. Przed uruchomieniem dostępu do systemu poczty elektronicznej, każdy Użytkownik zobowiązany jest zapoznać się z przepisami niniejszego Regulaminu i potwierdzić ten

fakt na piśmie. Za zaznajomienie Użytkownika z tymi przepisami oraz odebranie od niego pisemnego oświadczenia, sporządzonego według wzoru stanowiącego Załącznik nr 1 do niniejszego Regulaminu, odpowiedzialny jest pracownik Działu Spraw Personalnych.

§ 4. Zasady korzystania z firmowej poczty elektronicznej przez Użytkowników.

1. Poczta elektroniczna z adresem zawierającym oznaczenie domeny „wsm.edu.pl" znajduje się w wyłącznej dyspozycji Wyższej Szkoły Menedżerskiej w Warszawie.
2. Informacje przekazywane za pomocą poczty elektronicznej podlegają takim samym zasadom poufności, jakim podlega pisemna korespondencja służbowa.
3. Poczta elektroniczna WSM może być monitorowana przez upoważnione osoby w taki sposób, który nie narusza tajemnicy korespondencji i prawa do prywatności, w rozumieniu odnośnych przepisów prawa (art. 267 kk, art. 47 Konstytucji RP). Prawo do prowadzenia czynności związanych z monitorowaniem poczty elektronicznej WSM mają wyłącznie osoby wskazane imiennie przez Rektora WSM.
4. Adres poczty elektronicznej WSM powinien być wykorzystywany wyłącznie w celu prowadzenia korespondencji związanej z działalnością Uczelni (korespondencja służbowa).
5. Nie dopuszcza się możliwości używania poczty elektronicznej WSM w celach prywatnych.
6. Użytkownikom firmowej poczty elektronicznej WSM zabrania się za pomocą poczty:
    a. reprezentować, wydawać opinii lub w inny sposób zajmować stanowiska w imieniu Uczelni, jeżeli nie są do tego właściwie upoważnieni,
    b. wysyłać wiadomości fałszując informację o jej nadawcy lub treści.
7. Użytkownicy zobowiązani są do regularnego odczytywania otrzymywanych wiadomości, a jeżeli wiadomość wymaga udzielenia odpowiedzi, odpowiedź powinna być wysłana w terminie określonym przepisami prawa lub wewnętrznymi regulacjami obowiązującymi w WSM.
8. Użytkownicy powinni zachować szczególną ostrożność w przypadku otrzymania wiadomości pocztowych pochodzących od nieznanych nadawców. W przypadku uzasadnionej wątpliwości co do pochodzenia lub zawartości wiadomości pocztowych, w celu podjęcia dalszych działań, Użytkownik powinien się zwrócić się o pomoc do Administratora poczty elektronicznej.
9. Wszystkie informacje, które nie są publicznie dostępne, a z którymi Użytkownik zapoznał się w trakcie wykonywania obowiązków służbowych powinny być wysyłane

wyłącznie na adres osób, które są znane nadawcy, są służbowo zainteresowane sprawą i posiadają uprawnienia do jej otrzymania.

10. Użytkownicy mają prawo zdalnego logowania się do konta poczty elektronicznej Wyższej Szkoły Menedżerskiej w Warszawie z komputerów innych, niż urządzenia służbowe, jednak należy powstrzymywać się od korzystania z usług tzw. „kafejek internetowych", „hot spotów", i innych tego rodzaju źródeł dostępu do sieci Internet.

11. Użytkownicy poczty elektronicznej WSM są zobowiązani do:

    a. stosowania ogólnie przyjętych zasad i form grzecznościowych w wymienianych wiadomościach pocztowych,

    b. sprawdzania autentyczności nadawcy w przypadku wątpliwości, co do autentyczności wiadomości, np. poprzez próbę kontaktu z nadawcą, przy pomocy innych środków komunikacji.

    c. załączania na końcu wiadomości swojej wizytówki, zawierającej co najmniej: imię i nazwisko, stanowisko służbowe, nazwę jednostki organizacyjnej WSM, numer telefonu i adres e-mail,

12. Nadawca wiadomości poczty elektronicznej nie powinien zakładać, że jego przesyłka została przeczytana przez adresata w momencie jej dostarczenia, jeżeli przed jej wysłaniem nie ustawił stosownych reguł powiadamiania (o otrzymaniu i odczycie wiadomości).

13. Wiadomość wysłana pocztą elektroniczną nie jest bezpieczna. Może być przechwycona i odczytana lub zmodyfikowana przez osobę nieuprawnioną, chyba, że wiadomość jest zaszyfrowana (chroniona przed odczytaniem) lub podpisana elektronicznie (chroniona przed modyfikacją).

14. Usunięcie wiadomości poczty elektronicznej ze skrzynki Użytkownika nie oznacza jej fizycznego unicestwienia. Wiadomości są archiwizowane przez elektroniczne systemy sporządzania kopii zapasowych i mogą być odtwarzane.

15. W rejestrach zdarzeń systemu poczty elektronicznej zapisywane są informacje o czasie przysłania i wysłania każdej wiadomości pocztowej oraz adresie jej nadawcy i odbiorcy.

16. Administrator systemu poczty elektronicznej UFG, ze względu na przysługujące mu uprawnienia jest w stanie odczytać zawartość każdej wiadomości pocztowej, jeżeli wiadomość nie jest zaszyfrowana.

17. Za zgodą Kierownika Działu IT, Administrator systemu poczty elektronicznej WSM ma prawo nakładać ograniczenia i restrykcje na ten system lub na poszczególnych Użytkowników, jeżeli jest to niezbędne do prawidłowego funkcjonowania całego systemu pocztowego w Uczelni, informując o tym zainteresowane osoby.

18. Użytkownik nie powinien odpowiadać na tzw. „spam", czego skutkiem może być nasilenie otrzymywania tego rodzaju wiadomości. Przesyłki, które Użytkownik uzna za spam, należy przesyłać na adres Administratora systemu poczty elektronicznej.

§ 5. Zasady korzystania z dostępu do sieci Internet.

1. Użytkownik może korzystać z Internetu wyłącznie z wyznaczonego stanowiska, skonfigurowanego zgodnie z regulacjami obowiązującymi w WSM.
2. Dostęp do Internetu w czasie godzin pracy powinien być wykorzystywany jedynie do realizacji obowiązków pracowniczych, dydaktycznych oraz pozyskiwania informacji przydatnych w pracy zawodowej i służących samokształceniu.
3. Użytkownik może okazjonalnie korzystać z dostępu do Internetu w celach prywatnych, jeżeli czynność ta nie zakłóca realizacji obowiązków służbowych Użytkownika.
4. Użytkownik powinien dołożyć należytej staranności podczas korzystania z Internetu. Za właściwe korzystanie z Internetu odpowiada Użytkownik stanowiska, z którego łączy się z Internetem. W szczególności Użytkownik tego stanowiska odpowiada za:
    a. treści wysyłane do Internetu,
    b. decyzje dotyczące pozyskiwania treści z Internetu.
5. W przypadku wystąpienia problemów związanych z korzystaniem z Internetu, Użytkownik powinien się zwrócić do pracownika Działu IT.
6. Użytkownikom korzystającym z sieci Internet zabrania się:
    a. reprezentować, wydawać opinii lub w inny sposób zajmować stanowiska w imieniu Uczelni, jeżeli nie są do tego właściwie upoważnieni,
    b. przeglądać stron internetowych o charakterze rozrywkowym, szczególnie uczestniczyć we wszelkiego rodzaju grach on-line,
    c. przeglądać stron zawierających treści sprzeczne z prawem,
    d. pozyskiwać znacznej ilości danych, w szczególności poprzez zapisywanie na stanowisku, z którego łączy się z Internetem plików multimedialnych o znacznej objętości, jeżeli nie jest to uzasadnione obowiązkami służbowymi,
    e. pozostawiać stanowiska komputerowego z uaktywnionym oprogramowaniem utrzymującym łączność Internetem.
7. W Dziale IT zbierane są informacje o zasobach internetowych, do których Użytkownik miał dostęp.

§ 6. Odpowiedzialność Użytkowników korzystających z firmowej poczty elektronicznej Wyższej Szkoły Menedżerskiej w Warszawie i sieci Internet.

1. Wykorzystywanie poczty elektronicznej oraz korzystanie z sieci Internet niezgodnie z zasadami określonymi w niniejszym Regulaminie może stanowić podstawę nałożenia na pracownika WSM kary porządkowej, lub innych środków dyscyplinujących określonych przepisami prawa pracy, Regulaminu Pracy WSM oraz innych wewnętrznych regulacji obowiązujących w Uczelni. W stosunku do Użytkowników niebędących pracownikami Uczelni, złamanie zasad określonych w niniejszym Regulaminie może stanowić podstawę do natychmiastowego rozwiązania stosownej umowy, bez zachowania okresu wypowiedzenia (umowy zlecenia, o dzieło, itp.).

2. Postanowienia zawarte w ust. 1 powinny znaleźć swoje odzwierciedlenie w treści wszystkich umów zawieranych z zewnętrznymi podmiotami, które będą korzystać z dostępu do poczty elektronicznej WSM.

3. O naruszeniu zasad określonych w niniejszym Regulaminie przez pracowników WSM Kierownik Działu IT informuje bezpośredniego przełożonego danego pracownika. W przypadku Użytkownika niebędącego pracownikiem WSM, ww. informacja przekazywana jest Kanclerzowi.

4. Kierujący poszczególnymi jednostkami organizacyjnymi Uczelni odpowiedzialni są za poinformowanie podległych pracowników o zasadach określonych w niniejszym Regulaminie.

§ 7. Zakres i uprawnienia kontrolne WSM dotyczące korespondencji przesyłanej za pomocą poczty elektronicznej WSM oraz korzystania z dostępu do sieci Internet.

1. Z uwagi na konieczność zapewnienia ochrony interesów i bezpieczeństwa Uczelni, WSM zastrzega sobie możliwość wglądu w korespondencję przesyłaną z wykorzystaniem firmowego konta poczty elektronicznej, jak również w działania Użytkowników w zakresie dostępu do sieci Internet.

2. Kierownik Działu IT, nie rzadziej, niż dwa razy w roku, przeprowadza przegląd z zakresu przestrzegania zasad określonych w niniejszym Regulaminie, a w szczególności zasad określonych w §§ 4 i 5. Wyniki tych przeglądów przekazywane są Rektorowi w postaci pisemnych raportów.

§ 8. Postanowienia końcowe.

1. Przepisy *Instrukcji* określonej w ust. 1 powinny wejść w życie nie później, niż w terminie 30 dni od wejścia w życie niniejszego Regulaminu.

REKTOR
prof. zw. dr hab. Paweł Czarnecki

Załącznik nr 1.

Oświadczenie Użytkownika

Oświadczam, iż przyjmuję do wiadomości postanowienia **„Regulaminu korzystania z firmowej poczty elektronicznej i sieci Internet przez pracowników Wyższej Szkoły Menedżerskiej w Warszawie oraz innych użytkowników"** i zobowiązuję się do przestrzegania zasad i obowiązków określonych w Regulaminie. Przyjmuję zarazem do wiadomości, że naruszenie przeze mnie zasad i obowiązków w nim określonych, skutkować może zastosowaniem wobec mnie właściwych przepisów porządkowych prawa pracy, włącznie z rozwiązaniem umowy o pracę z winy leżącej po stronie pracownika.

Oświadczam zarazem, że wyrażam zgodę na prowadzenie czynności kontrolnych w zakresie korzystania przeze mnie z dostępu do sieci Internet oraz prawidłowości wykorzystywania firmowej poczty elektronicznej WSM.

Z tytułu prowadzonych czynności kontrolnych, realizowanych zgodnie z zasadami określonymi w przepisach ww. Regulaminu, nie będę wnosić obecnie, jak również po rozwiązaniu łączącego mnie z WSM stosunku prawnego, żadnych roszczeń.

.....

(miejscowość i data)

.....

(podpis pracownika)

.....

(podpis osoby odbierającej oświadczenie).

Wyższa Szkoła Menedżerska
w Warszawie

Instrukcja postępowania w sytuacji stwierdzenia przypadków naruszenia bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie

Załącznik nr 4 do zarządzenia Rektora WSM w Warszawie
nr 2/05/2018 z dnia 22 maja 2018 r.

Dokument przygotował: Dyrektor Centrum Administracyjno – technicznego inż. Dariusz Grabiec
Wersja dokumentu: 1/2018
Dokument zatwierdził: J.M. Rektor Prof. dr hab. Paweł Czarnecki MBA dr h.c.
Wprowadzono do stosowania Zarządzeniem Rektora nr 2/05/2018 w dniu: 22 maja 2018 r.

Spis treści

I. Wprowadzenie

1. Niniejsza Instrukcja jest aktem wykonawczym w odniesieniu do „Polityki Bezpieczeństwa Danych Osobowych". Wprowadza się ją w celu określenia na czym mogą polegać poszczególne rodzaje naruszeń bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie (WSM) i w jaki sposób oraz na jakiej podstawie zatrudnione w nim osoby powinny kwalifikować (rozpoznawać) określone zdarzenia jako potencjalne naruszenie bezpieczeństwa informacyjnego.
2. Celem Instrukcji jest określenie wymaganego sposobu postępowania wszystkich osób odpowiedzialnych za właściwe zabezpieczenie przetwarzanych w WSM danych, w szczególności Inspektora Ochrony Danych (IOD), w sytuacji gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informacyjnego w obszarze przetwarzania danych,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie bezpieczeństwa danych,
   - stwierdzono naruszenie bezpieczeństwa fizycznego pomieszczeń, kartotek lub szaf, w których przechowywane są nośniki danych, w szczególności danych osobowych.
3. Instrukcja wprowadza również obowiązujące w WSM zasady dokumentowania zdarzeń dotyczących naruszenia bezpieczeństwa informacyjnego, a także procesu ich analizy pod kątem konieczności zgłoszenia faktu ich zaistnienia do Organu nadzorczego oraz osoby, której dane dotyczą.
4. Inspektor Ochrony Danych, we współpracy z Administratorem Systemu Informatycznego, podejmuje niezbędne działania zapewniające odporność sieci oraz systemów informatycznych na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne zjawiska naruszające dostępność, integralność i poufność przetwarzanych danych osobowych oraz bezpieczeństwo związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci.
5. Każdy pracownik Uczelni biorący udział w przetwarzaniu danych osobowych jest odpowiedzialny za bezpieczeństwo tych danych. Na każdym pracowniku ciąży zarazem obowiązek zgłaszania do przełożonych lub bezpośrednio do IOD wszelkich stwierdzonych przez siebie naruszeń zasad bezpieczeństwa informacyjnego oraz zdarzeń mogących prowadzić do naruszenia bezpieczeństwa, w tym zwłaszcza zaobserwowanych podatności

na naruszenia. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną.

6. Dla stwierdzonych przypadków naruszenia zasad bezpieczeństwa danych osobowych należy zapewnić możliwość uzyskania danych niezbędnych do przeprowadzenia postępowania wyjaśniającego pod kątem określenia skutków naruszenia, ustalenia odpowiedzialności i sformułowania wniosków.

II. Definicje

W treści niniejszej Instrukcji zastosowanie mają definicje zawarte w rozdziale 1 Polityki Bezpieczeństwa Danych Osobowych PBDO), a także:

1. **Zdarzenie związane z bezpieczeństwem informacyjnym** – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie PBDO, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacyjnym i prowadzić w konsekwencji do naruszenia ochrony danych osobowych;
2. **Incydent bezpieczeństwa** – pojedyncze zdarzenie lub seria niepożądanych oraz niespodziewanych zdarzeń związanych z bezpieczeństwem informacyjnym, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacyjnemu;
3. **Raport** – pisemny raport dot. naruszenia bezpieczeństwa informacyjnego;
4. **Rejestr** – Rejestr naruszeń bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie.

III. Rodzaje naruszeń bezpieczeństwa informacyjnego

1. Najbardziej typowe źródła zagrożeń bezpieczeństwa informacyjnego, szczególnie istotne z punktu widzenia przetwarzania danych osobowych, wyszczególniono w rozdziale 15 PBDO.
2. Dla potrzeb niniejszej Instrukcji wyróżnia się następujące główne rodzaje naruszeń bezpieczeństwa informacyjnego:
   a. naruszenie dostępności systemu informacyjnego;

b. naruszenie integralności systemu informacyjnego;
c. naruszenie poufności systemu informacyjnego.

3. Naruszenie dostępności systemu informacyjnego występuje wtedy, gdy użytkownik tego systemu nie jest w stanie wykonać autoryzowanej, zgodnej z dokumentacją funkcji użytkowej.
4. Naruszenie integralności systemu informacyjnego występuje wtedy, gdy postać lub treść danych (informacji) niezbędnych do wykonania legalnej funkcji użytkowej nie spełnia autoryzowanych wymagań lub, gdy wykonanie legalnej funkcji przebiega niezgodnie z autoryzowaną procedurą. Ten rodzaj naruszenia przejawiać się może również w przypadku dokonywania nieautoryzowanych modyfikacji lub niszczenia danych.
5. Naruszenie poufności systemu informacyjnego wystąpi wtedy, gdy dane (informacje) zostaną przypadkowo lub świadomie, udostępnione lub w inny sposób ujawnione nieautoryzowanym osobom, podmiotom lub procesom.
6. Niezależnie od określonych w przepisach ust. 3 – 5 rodzajów naruszeń, za naruszenie bezpieczeństwa informacyjnego w WSM uznane będzie również pozyskiwanie danych ze źródeł prawnie niedopuszczalnych.

IV. Zasady postępowania w przypadku naruszenia ochrony danych osobowych

1. Postępowanie w przypadkach naruszenia Polityki Bezpieczeństwa Danych Osobowych

   Każdy pracownik Uczelni biorący udział w przetwarzaniu danych osobowych jest odpowiedzialny za zapewnienie bezpieczeństwa tych danych. Na każdym pracowniku ciąży zarazem obowiązek zgłaszania do przełożonych lub bezpośrednio do IOD wszelkich stwierdzonych przez siebie naruszeń zasad bezpieczeństwa informacyjnego oraz zdarzeń mogących prowadzić do jego naruszenia, w szczególności zaobserwowanych podatności na naruszenia. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika w sposób bezpośredni ustnie, drogą telefoniczną lub pocztą elektroniczną.

   Dla stwierdzonych przypadków naruszenia zasad bezpieczeństwa danych osobowych należy zapewnić możliwość uzyskania danych niezbędnych do przeprowadzenia postępowania wyjaśniającego pod kątem określenia skutków naruszenia, ustalenia odpowiedzialności i sformułowania wniosków.

2. Za symptomy wskazujące na potencjalną możliwość naruszenia bezpieczeństwa informacji, w tym bezpieczeństwa danych osobowych można uznać:
   - ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
   - wygląd aplikacji inny niż normalnie,
   - inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
   - znaczne spowolnienie działania systemu informatycznego,
   - pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
   - ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
   - ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
   - włamanie lub próby włamania do szafek, w których przechowywane są, w postaci elektronicznej lub papierowej, nośniki danych osobowych,
   - zagubienie bądź kradzież nośnika danych osobowych,
   - kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
   - fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,
   - podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym,
   - podejrzenie, iż dane osobowe przetwarzane są w zakresie przekraczającym uzasadnioną potrzebę do realizacji określonego celu (nadmiarowość).

3. Zgłaszanie naruszenia (incydentu) ochrony danych osobowych Organowi nadzorczemu
   W przypadku wystąpienia incydentu, który może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je Organowi

nadzorczemu. Do zgłoszenia przekazanego Organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie każdorazowo musi być poprzedzone analizą ujawnionego incydentu, za przeprowadzenie której odpowiedzialny jest IOD we współpracy z ASI.

W zakres analizy incydentu bezpieczeństwa wchodzi realizacja co najmniej niżej wymienionych czynności:

- zabezpieczenie wszelkich znamion i dowodów związanych z zaistniałym incydentem,
- szczegółowy opis naruszenia, wskazujący w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- ocenę możliwych konsekwencji naruszenia praw lub wolności osób fizycznych;
- wyszczególnienie zastosowanych lub możliwych do zastosowania środków w celu zaradzenia lub choćby zminimalizowania ewentualnych skutków naruszenia.

Inspektor Ochrony Danych dokonuje wstępnej kwalifikacji każdego analizowanego przypadku, a następnie formułuje do Administratora (Rektora) wniosek w sprawie dokonania zgłoszenia do Organu nadzorczego lub odstąpienia od tej czynności w danym przypadku. Wniosek składany jest z całością zgromadzonego materiału w sprawie.

IOD w imieniu Administratora, dokumentuje i ewidencjonuje wszelkie naruszenia ochrony danych osobowych, z uwzględnieniem okoliczności każdego naruszenia, jego skutków oraz podjętych środków zaradczych. Dokumentacja ta musi pozwolić Organowi nadzorczemu na zweryfikowanie przestrzegania wymogów prawnych związanych z dokonywaniem zgłoszeń.

Za monitorowanie przestrzegania obowiązku zgłaszania naruszenia ochrony danych osobowych Organowi nadzorczemu odpowiedzialny jest Inspektor Ochrony Danych. Monitorowanie jest wynikiem stałej oceny ryzyka, prowadzonej przez IOD oraz stanowi również wynik innych analiz, w tym audytów bezpieczeństwa informacyjnego.

4. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

   Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, chyba że wystąpią przypadki wskazane w prawie wyłączające konieczność zawiadomienia.

Za przejawy wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych można uznać w szczególności:

- przetwarzanie danych osobowych prowadzące do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych,
- przetwarzanie mogące skutkować dyskryminacją, kradzieżą tożsamości, lub oszustwem, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, znaczną szkodą gospodarczą lub społeczną,
- możliwość narażenia osoby, której dane dotyczą pozbawienia przysługujących jej praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
- przetwarzanie dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Czynności związane z przeprowadzeniem pogłębionej analizy i kwalifikacji każdego tego rodzaju przypadku są realizowane zgodnie z zasadami określonymi w pkt. 3. Administrator, w przypadku stwierdzenia takiej konieczności, podejmuje inne niezbędne działania mające zapobiec materializacji negatywnych skutków związanych z naruszeniem praw osób, których to dotyczy.

V. Dokumentowanie naruszeń bezpieczeństwa informacyjnego

1. Najczęściej możliwe do zrealizowania się w Wyższej Szkole Menedżerskiej w Warszawie formy naruszeń bezpieczeństwa informacyjnego zamieszczono w tabeli, stanowiącej Załącznik nr 1 do niniejszej Instrukcji. Wykaz nie ma charakteru zamkniętego i w okresach nie krótszych niż pół roku podlega przeglądowi i aktualizacji, za przeprowadzenie której odpowiedzialny jest IOD.
2. Powzięcie przez uprawnionego użytkownika systemu informatycznego Wyższej Szkoły Menedżerskiej w Warszawie informacji o zaistniałym, bądź podejrzeniu zaistnienia Incydentu bezpieczeństwa, związanego w szczególności z naruszeniem przepisów dot. ochrony danych osobowych, nakłada na niego obowiązek powstrzymania się od dalszego przetwarzania tych danych i niezwłocznego powiadomienia osób wymienionych w rozdziale IV pkt. 1.
3. Po dokonaniu wstępnej analizy i kwalifikacji zaistniałego zdarzenia użytkownik jest obowiązany udokumentować ten fakt, poprzez sporządzenie Raportu, korzystając z wzoru

stanowiącego Załącznik nr 2 do niniejszej Instrukcji. Raport sporządzony w postaci elektronicznej bądź papierowej, jest następnie bez zbędnej zwłoki przekazywany do IOD, do którego należy podjęcie dalszych niezbędnych w tym zakresie czynności. Do czynności tych w szczególności zaliczyć można:

- zabezpieczenie dowodów zdarzenia,
- minimalizacja negatywnych skutków zdarzenia,
- wyjaśnienie wszelkich możliwych okoliczności zdarzenia.

4. W przypadku wystąpienia naruszenia bezpieczeństwa informacyjnego IOD wg własnej oceny może natychmiast powiadomić o takim zdarzeniu Rektora oraz podjąć dodatkowe działania związane ze sporządzeniem szczegółowej dokumentacji stwierdzonego naruszenia.
5. W sytuacji gdy naruszenie bezpieczeństwa informacyjnego związane jest z funkcjonowaniem systemu informatycznego, IOD współpracuje ściśle w tym zakresie z ASI. Wyniki ustaleń dokonanych przez ASI dokumentowane są w odrębnej notatce.
6. Dane zawarte w „Raporcie o naruszeniu bezpieczeństwa informacyjnego" oraz w treści notatki sporządzonej ewentualnie przez ASI, stanowią podstawę do dokonania wpisu w Rejestrze, wzór którego określono w Załączniku nr 3. Za prowadzenie Rejestru odpowiedzialny jest IOD.
7. IOD, na podstawie analizy zawartości Rejestru, a także w oparciu o inne pozyskane przez siebie informacje, sporządza i przedstawia Rektorowi raz na pół roku ogólną informację o stanie bezpieczeństwa informacyjnego Wyższej Szkoły Menedżerskiej w Warszawie, wraz ze stosownymi wnioskami. Odrębną część tej informacji stanowi opis stanu przestrzegania przepisów dotyczących ochrony danych osobowych. Wszystkie wskazane w niniejszym punkcie czynności stanowić winny również podstawę wszelkich poczynań w zakresie zarządzania ryzykiem informacyjnym w WSM.

VI. Uprawnienia Inspektora Ochrony Danych

1. W celu eliminowania negatywnych skutków naruszenia bezpieczeństwa informacyjnego w Wyższej Szkole Menedżerskiej w Warszawie, Inspektor Ochrony Danych ma prawo do podejmowania wymagających tego działań, a w szczególności:
   - żądania podania przez pracowników dodatkowych wyjaśnień w związku z zaistniałym zdarzeniem,

- korzystania z pomocy konsultantów,
- nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

2. Odmowa udzielenia wyjaśnień lub brak współpracy z IOD traktowana będzie jako poważne naruszenie podstawowych obowiązków pracowniczych.

VII. Postanowienia końcowe

1. Nieprzestrzeganie zasad i trybu postępowania określonych w niniejszej Instrukcji stanowi poważne naruszenie podstawowych obowiązków pracowniczych, które skutkować może możliwością nałożenia kary porządkowej przewidzianej przepisami kodeksu pracy. W przypadku osoby zatrudnionej na innej podstawie niż stosunek pracy możliwym będzie nałożenie kary przewidzianej treścią zawartej z nią umowy.
2. Osobą uprawnioną do określania wykładni przepisów niniejszej Instrukcji jest IOD. W przypadku utrzymującej się, mimo wyjaśnień IOD, różnicy w rozumieniu tych przepisów, ostatecznej wykładni dokonuje Rektor.
3. W przypadku wystąpienia sytuacji, która nie została przewidziana przepisami niniejszej Instrukcji, użytkownik ma oprawo zwrócić się do IOD z wnioskiem o określenie na piśmie sposobu wymaganego postępowania.

REKTOR
prof. zw. dr hab. Paweł Czarnecki

IX. Załączniki

Załącznik nr 1

Tabela form naruszeń bezpieczeństwa informacyjnego

Kod naruszenia	Formy naruszeń	Sposób postępowania
A	**Forma naruszenia bezpieczeństwa informacyjnego przez pracownika zatrudnionego przy przetwarzaniu danych**	
A.1	**W zakresie wiedzy**	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IOD.
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IOD.
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką informację mógł pozyskać np. z obserwacji lub dokumentacji.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IOD.
A.2	**W zakresie sprzętu i oprogramowania**	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do informacji chronionych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport i powiadomić IOD.
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych, w szczególnie danych osobowych, przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska pracy przy komputerze. Pouczyć osobę, która dopuściła się takiej sytuacji. Sporządzić raport i powiadomić IOD.
A.2.3	Pozostawienie w miejscu niezabezpieczonym, a w szczególności miejscu widocznym, zapisanego hasła dostępu do systemu informatycznego.	Zabezpieczyć notatkę z hasłami w sposób uniemożliwiający jej odczytanie. Sporządzić raport i powiadomić IOD.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami WSM.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały osoby nieuprawnione wykonane. Przerwać działanie programów. Sporządzić raport i powiadomić IOD.

A.2.5	Samodzielne instalowanie oprogramowania.	Pouczyć osobę wykonującą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne WSM w celu odinstalowania programów. Sporządzić raport i powiadomić IOD.
A.2.6	Modyfikowanie parametrów systemu i aplikacji	Wezwać osobę wykonującą wymienioną czynność, aby jej zaniechała. Sporządzić raport i powiadomić IOD.
A.2.7	Odczytywanie zewnętrznych nośników danych przed sprawdzeniem ich oprogramowaniem antywirusowym.	Pouczyć osobę wykonującą wymienioną czynność, aby stosowała się do wymogów bezpieczeństwa obowiązujących w tym zakresie.. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport i powiadomić IOD.
A.3	**W zakresie dokumentów i obrazów zawierających dane osobowe**	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport i powiadomić IOD.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych pracownika. Spowodować poprawę zastanej sytuacji. Sporządzić raport i powiadomić IOD.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym odczytanie ich treści.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawniona osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały dane, w szczególności dane osobowe - sporządzić raport i powiadomić IOD.
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych odrębnymi procedurami.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Sporządzić raport i powiadomić IOD.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Sporządzić raport i powiadomić IOD.
A.4	**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych**	
A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy służący do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.4.2	Wpuszczanie do pomieszczeń służbowych osób nieznanych i	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich

	dopuszczanie ich do kontaktu ze sprzętem komputerowym.	tożsamość. Powiadomić przełożonych. Sporządzić raport i powiadomić IOD.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów, gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne. Sporządzić raport i powiadomić IOD.
A.5	**W zakresie pomieszczeń, w których znajdują się serwery i urządzenia sieci**	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach dostępnych publicznie (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość z pomocą pracowników ochrony. Powiadomić służby informatyczne WSM. Sporządzić raport i powiadomić IOD.
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach serwerowni lub węzłów sieci informatycznej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne WSM. Sporządzić raport i powiadomić IOD.
B	**Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych**	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie IOD oraz służby informatyczne WSM. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu	Powiadomić niezwłocznie służby informatyczne WSM i IOD. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie służby informatyczne WSM oraz IOD. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne WSM oraz IOD. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Powiadomić niezwłocznie służby informatyczne WSM oraz IOD. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z obowiązującymi w tego rodzaju przypadkach procedurami. Powiadomić IOD i sporządzić raport.

C	**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem**	
C.1	Próba uzyskania hasła uprawniającego do dostępu do systemów, w których przetwarzane są dane osobowe, w ramach świadczenia pomocy technicznej.	Powiadomić IOD i sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych, przy użyciu identyfikatora i hasła użytkownika.	Powiadomić IOD i sporządzić raport.

Załącznik nr 2
Wzór raportu o naruszeniu bezpieczeństwa informacyjnego.

Raport o naruszeniu bezpieczeństwa informacyjnego

Sporządzający raport:

Nazwisko i imię .....
Stanowisko i funkcja .....
Jednostka organizacyjna, pokój, nr telefonu .....

Kod formy naruszenia (wg tabeli) .....

1. Miejsce, dokładny czas i data stwierdzonego naruszenia (budynek, piętro, nr pokoju, godzina, itp.) :
   .....
   .....

2. Osoby powodujące naruszenie bezpieczeństwa informacyjnego:
   .....
   .....

3. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony bezpieczeństwa informacyjnego:
   .....
   .....

4. Informacje o danych, które zostały lub mogły zostać ujawnione:
   .....
   .....

5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem:
   .....
   .....

6. Krótki opis wydarzenia związanego z naruszeniem bezpieczeństwa informacyjnego (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):
   .....
   .....
   .....
   .....
   .....
   .....

....
data podpis

Załącznik nr 3

Wzór „Rejestru naruszeń bezpieczeństwa informacyjnego w WSM”

Lp	Czas trwania naruszenia			Osoba / źródło informacji o naruszeniu	Kategoria i liczba osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Miejsce naruszenia	Sposób naruszenia	Opis charakteru naruszenia	Opis skutków naruszenia	Przyczyna naruszenia przez	Osoba/jednostka odpowiedzialna za naruszenie	Podjęte działania	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy informowano IODO ? Jeśli tak to w jakim dniu i godzinę zgłoszono	Czy informowano osobę, której dotyczy naruszenie ?	Monitoring działań naprawczych
	Data i godzina rozpoczęcia naruszenia	Data i godzina stwierdzenia naruszenia	Data naruszenia (okres, którego dotyczy)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18