POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W WYŻSZEJ SZKOLE ZARZĄDZANIA OCHRONĄ PRACY W KATOWICACH

§ 1

1. Polityka bezpieczeństwa danych osobowych (Polityka) obejmuje całokształt uregulowań dotyczących przetwarzania i ochrony danych osobowych w Wyższej Szkole Zarządzania Ochroną Pracy w Katowicach (WSZOP).
2. Polityka stanowi realizację wymogów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 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 (RODO).

DEFINICJE

§ 2

Użyte w dokumencie pojęcia oznaczają:

1) **Dane osobowe** – wszelkie 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
2) **Przetwarzanie** – operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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
3) **Administrator** – Wyższa Szkoła Zarządzania Ochroną Pracy w Katowicach (WSZOP), zwana również Uczelnią, reprezentowaną przez Rektora
4) **Lokalny administrator** – kierownik jednostki organizacyjnej lub komórki administracji, a w szczególności: Dziekan, Kanclerz, Kwestor, kierownik działu kadr i płac, kierownik promocji i rekrutacji, kierownik administracji, kierownik biblioteki, kierownik sekcji planowania i organizacji studiów
5) **Inspektor ochrony danych (IDO)** – osoba pełniąca funkcję doradczo-nadzorczą w zakresie bezpieczeństwa przetwarzania danych osobowych
6) **Administrator systemu informatycznego (ASI)** – osoba odpowiadającą za funkcjonowanie i bezpieczeństwo systemu informatycznego, zawierającego programy lub bazy danych zastosowane do przetwarzania danych osobowych, również w przypadku dostępu zdalnego i mobilnego do systemu
7) **Podmiot przetwarzający (Procesor)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora
8) **Jednostka** – jednostka organizacyjna lub komórka administracji
9) **Odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią
10) **Zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

11) **Naruszenia ochrony danych osobowych** – naruszenia 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
12) **Wrażliwe dane osobowe** – dane, o których mowa w art. 9 –10 RODO, tj.
    a) tzw. szczególne kategorie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dotyczące stanu zdrowia, seksualności itp.
    b) dane osobowe dotyczące wyroków skazujących i czynów zabronionych.
13) **System informatyczny** – zespół współpracujących ze sobą programów i urządzeń Uczelni zastosowanych w celu przetwarzania danych.
14) **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych wg określonych kryteriów
15) **Marketing bezpośredni** – prezentowanie (za pośrednictwem poczty elektronicznej) oferty edukacyjnej Administratora dotyczącej studiów, kursów, szkoleń, konferencji, wydarzeń kulturalnych (wernisaży, występów artystycznych).

§ 3

Rektor jako reprezentant Administratora zobowiązuje wszystkich pracowników Uczelni oraz osób z nią współpracujących do przestrzegania najwyższych standardów w zakresie ochrony danych osobowych, przy czym dodatkowo:

1) inspektorowi ochrony danych (IDO) powierza funkcje doradcze oraz nadzorcze w skali całej Uczelni
2) Lokalnym administratorom powierza funkcje kontrolne w skali zarządzanej jednostki
3) Administratorowi systemu informatycznego (ASI) powierza funkcje doradcze i kontrolne w zakresie bezpieczeństwa systemu informatycznego.

ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

§ 4

1. **Legalizm, rzetelność i przejrzystość** – przetwarzanie danych osobowych odbywa się zgodnie z prawem, rzetelnie, a także w sposób przejrzysty dla osoby, której dane dotyczą.
2. **Ograniczenie celu** – przetwarzanie danych osobowych, odbywa się wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach.
3. **Minimalizacja danych** – przetwarzanie danych osobowych ogranicza się wyłącznie do niezbędnego celu.
4. **Prawidłowość** – przetwarzanie aktualnych i prawidłowych danych osobowych i podejmowanie działania zmierzające do usunięcia lub sprostowania danych nieprawidłowych.
5. **Ograniczenie przechowywania** – przetwarzanie danych osobowych odbywa się przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane
6. **Integralność i poufność** – przetwarzanie danych osobowych odbywa się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym przetwarzaniem, utratą, zniszczeniem lub uszkodzeniem
7. **Rozliczalność** – zgodne z prawem przetwarzanie danych osobowych musi być możliwe do wykazania przez Administratora.

INSPEKTOR OCHORNY DANYCH

§ 5

1. Rektor wyznacza inspektora ochrony danych (IDO), który podlega mu bezpośrednio i pełni rolę jego pełnomocnika w zakresie bezpieczeństwa informacji.

2. IDO jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych w Uczelni, a w realizacji obowiązków pozostaje niezależny od kierownictwa Uczelni, a także pozostałych pracowników i innych osób współpracujących.
3. Do zadań IDO należy w szczególności:
   1) informowanie pracowników przetwarzających dane osobowe o ochronie danych osobowych, w tym także doradzanie, szkolenie, współpraca z Lokalnymi administratorami
   2) udzielanie upoważnień do przetwarzaniach danych osobowych, w tym określanie zakresu upoważnień do przetwarzania danych i związanym z tym upoważnianiem do posiadania kluczy do pomieszczeń, szaf oraz sejfów
   3) sprawdzanie przestrzegania zasady przetwarzania danych osobowych w poszczególnych jednostkach Uczelni, w szczególności poprzez przeprowadzanie kontroli przestrzegania ochrony danych osobowych przez pracowników Uczelni oraz kierowanie zaleceń pokontrolnych
   4) organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania danych osobowych
   5) ustalanie przyczyny, zakresu i skutków naruszenia ochrony danych osobowych, osób odpowiedzialnych, ustalanie i wdrażanie odpowiednich środków zapobiegawczych przed dalszym naruszeniem albo naruszeniem w przyszłości; ustalanie i wdrażanie odpowiednich środków w celu przywrócenia prawidłowego funkcjonowania systemu ochrony danych
   6) pełnienie funkcji punktu kontaktowego dla osób, których dane przetwarzane są w Uczelni
   7) prowadzenie rejestru czynności przetwarzania danych osobowych
   8) prowadzenie rejestru kategorii czynności przetwarzania danych osobowych
   9) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych
   10) prowadzenie rejestru naruszeń ochrony danych osobowych
   11) podejmowanie decyzji w sprawie udostępniania danych
   12) nadzorowanie procesu rozpatrywania odwołań związanych z przetwarzaniem danych.

LOKALNY ADMINISTRATOR

§ 6

1. Pracownik pełniący funkcje kierownicze wykonuje z urzędu rolę Lokalnego administratora odpowiedzialnego za przestrzeganie zasad dotyczących ochrony danych osobowych w podległej jednostce.
2. Do zadań Lokalnego administratora należy dbałość o wysokie standardy w zakresie przestrzegania zasad ochrony danych osobowych w podległej jednostce, w tym ścisła współpraca z IDO w zakresie:
   1) konsultacji merytorycznej dotyczącej ochrony danych osobowych
   2) udzielania upoważnień do przetwarzania danych przez podległych pracowników
   3) zgłaszania naruszeń dotyczących przetwarzania danych osobowych
   4) zgłaszania problemów związanych z przestrzeganiem ochrony danych osobowych
   5) zgłaszania wniosków/propozycji mających usprawnić system bezpieczeństwa informacji w podległej jednostce, a dotyczących zabezpieczeń (technicznych, organizacyjnych).

ADMINSTRATOR SYSTEMU INFORMATYCZNEGO

§ 7

1. Administrator Systemu Informatycznego (ASI) ściśle współpracuje z IDO, pełni funkcję doradczą i kontrolną w zakresie funkcjonowania bezpieczeństwa systemu informatycznego.
2. Do zadań ASI należy w szczególności:
   1) przeprowadzanie okresowych przeglądów stanu urządzeń i oprogramowania
   2) ochrona danych osobowych w systemach informatycznych, zarchiwizowanych na nośnikach zewnętrznych

3) prowadzenie ewidencji sprzętu komputerowego, laptopów, telefonów komórkowych, aparatów fotograficznych oraz nośników, o których mowa w pkt 2
4) monitorowanie systemu zabezpieczeń, zapory internetowej firewall oraz urządzeń do zasilenia awaryjnego
5) weryfikacja legalności oprogramowania
6) instalacja i konfiguracja nowych programów i urządzeń do przetwarzania danych osobowych
7) wykonywanie i odzyskiwanie kopii zapasowych nośników danych osobowych
8) prowadzenie symulowanych włamań do systemu w celu ustalenia aktualnego poziomu zabezpieczeń
9) nadawanie haseł do systemu informatycznego, kontrolowanie użytkowników programów w zakresie zmian haseł
10) szyfrowanie przesyłanych danych osobowych w ramach zawartych umów powierzenia.

3. Szczegółowy tryb, zakres oraz częstotliwość czynności związanych z realizacją zadań dotyczących bezpieczeństwa systemu informatycznego określają odrębne procedury.

PODMIOTY, KTÓRYCH DANE SĄ PRZETWARZANE W UCZELNI

§ 8

Administrator przetwarza dane osobowe następujących osób fizycznych:
1) studentów (ich rodzin), w tym kandydatów na studia/ studia podyplomowe
2) słuchaczy studiów podyplomowych
3) uczestników kursów, szkoleń, konferencji
4) absolwentów
5) pracowników (ich rodzin), w tym kandydatów do pracy oraz byłych pracowników
6) osób świadczących pracę w innej formie niż stosunek pracy
7) czytelników biblioteki
8) kontrahentów
9) osób zaproszonych do udziału w eventach promocyjnych.

PODSTAWY PRAWNE ORAZ CELE PRZETWARZANIA DANYCH OSOBOWYCH

§ 9

1. Podstawę przetwarzania danych osobowych przez Uczelnię stanowią następujące przesłanki:
   1) realizacja obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 pkt c; art. 9 ust. 2 pkt b RODO)
   2) wykonanie umowy, której stroną jest osoba, której dane dotyczą, lub podjęcie działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust. 1 pkt b RODO)
   3) realizacja celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora (art. 6 ust. 1 pkt f RODO)
   4) zgoda osoby, której dane dotyczą (art. 6 ust. 1 pkt a /art. 9 ust. 2 pkt a RODO).
2. Przetwarzanie danych osobowych kandydatów na studentów/słuchaczy studiów podyplomowych jest niezbędne w celu rejestracji na studia/studia podyplomowe. Przetwarzanie danych osobowych ma związek z realizacją obowiązku prawnego ciążącego na Administratorze i jest niezbędne do zawarcia umowy.
3. Przetwarzanie danych osobowych studentów jest niezbędne w celu realizacji obowiązku prawnego ciążącego na Administratorze (realizacja procesu kształcenia), a także w celu wykonania prawnie uzasadnionych interesów Administratora, a związanych z prowadzeniem ewaluacji jakości kształcenia, marketingiem bezpośrednim. Dane osobowe mogą być także przetwarzane w celu realizacji procesu przyznawania pomocy materialnej, realizacji studiów zagranicznych w ramach Programu Erasmus, udostępniania zbiorów bibliotecznych.
4. Przetwarzanie danych osobowych członków rodzin studentów może być niezbędne w celu realizacji obowiązku prawnego ciążącego na Administratorze związanego z realizacją procesu przyznawania pomocy materialnej.

5. Przetwarzanie danych osobowych uczestników kursów/szkoleń/konferencji jest niezbędne w celu realizacji usługi edukacyjnej/naukowej, a także w celu wykonania prawnie uzasadnionych interesów Administratora związanych z marketingiem bezpośrednim, ewaluacją.
6. Przetwarzanie danych osobowych absolwentów jest niezbędne do wypełnienia obowiązku prawnego związanego z archiwizacją, a także w celu wykonania prawnie uzasadnionych interesów Administratora związanych z badaniem losów absolwentów, marketingiem bezpośrednim.
7. Przetwarzanie danych osobowych kandydatów do pracy jest niezbędne do przeprowadzenia procesu rekrutacyjnego, a następnie realizacji obowiązku prawnego związanego z zatrudnianiem.
8. Przetwarzanie danych osobowych pracowników jest niezbędne do realizacji obowiązku prawnego związanego z zatrudnieniem oraz z uwagi na uzasadniony interes prawny Administratora (np. prezentacja wizerunku pracowników pełniących funkcje reprezentacyjne).
9. Przetwarzanie danych osobowych członków rodzin pracowników może być niezbędne do realizacji obowiązku prawnego związanego z przyznawaniem świadczeń socjalnych.
10. Przetwarzanie danych osobowych osób świadczących pracę w innej formie niż stosunek pracy jest niezbędne do realizacji współpracy i ma związek z realizacją obowiązku prawnego.
11. Przetwarzanie danych osobowych kontrahentów jest niezbędne do realizacji umowy.
12. Przetwarzanie danych osobowych czytelników biblioteki jest niezbędne w celu udostępniania zbiorów bibliotecznych.
13. Przetwarzanie danych osobowych osób zaproszonych do udziału w eventach promocyjnych jest niezbędne do realizacji marketingu bezpośredniego.

OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

§ 10

1. Dane osobowe kandydatów na studia są przetwarzane prze okres prowadzenia rekrutacji, a następnie podlegają archiwizacji przez okres 6 miesięcy.
2. Dane osobowe studentów/słuchaczy studiów podyplomowych są przetwarzane przez okres realizacji usługi edukacyjnej, przez 15 lat przez okres realizacji marketingu bezpośredniego.
3. Dane osobowe studentów członków rodzin studentów są przetwarzane przez okres niezbędny do załatwienia sprawy, realizacji świadczenia pomocy materialnej.
4. Dane osobowe uczestników kursów/szkoleń są przetwarzane przez okres niezbędny do realizacji usługi edukacyjnej, przez 15 lat przez okres realizacji marketingu bezpośredniego.
5. Dane osobowe absolwentów studiów wyższych są archiwizowane przez okres 50 lat.
6. Dane osobowe absolwentów studiów podyplomowych są archiwizowane przez okres 10 lat.
7. Dane osobowe kandydatów do pracy są przetwarzane przez okres rekrutacji, a następnie podlegają archiwizacji przez okres 3 lat, chyba że kandydat na pracownika wyraził zgodę na przetwarzanie jego danych na potrzeby przyszłych rekrutacji w maksymalnym okresie do 3 lat.
8. Dane osobowe pracowników (odpowiednio) są przetwarzane przez okres zatrudnienia, a następnie podlegają archiwizacji przez okres wynikający z obowiązujących przepisów prawa pracy (50 lub 10 lat).
9. Dane osobowe studentów członków rodzin studentów są przetwarzane przez okres niezbędny do załatwienia sprawy, realizacji świadczenia socjalnego.
10. Dane osobowe osób świadczących pracę w innej formie niż stosunek pracy są przetwarzane przez okres niezbędny do realizacji współpracy, a następnie podlegają archiwizacji przez okres 10 lat.
11. Dane osobowe kontrahentów są przetwarzane przez okres współpracy z Administratorem, a następnie podlegają archiwizacji przez okres 10 lat.
12. Dane osobowe czytelników są przetwarzane przez okres realizacji usługi udostępniania zbiorów bibliotecznych.
13. Dane osobowe osób zaproszonych do udziału w eventach promocyjnych są przetwarzane przez okres 15 lat.

OBOWIĄZKI INFORMACYJNE ADMNISTRATORA

§ 11

1. Administrator podaje osobie, której dane będzie przetwarzać informacje o:
   1) nazwie, adresie, danych kontaktowych
   2) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania
   3) kategoriach odbiorców danych osobowych
   4) istnieniu albo braku istnienia wymogu podania danych osobowych oraz konsekwencjach niepodania danych osobowych
   5) zamiarze przekazania danych osobowych do państwa trzeciego
   6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalenia tego okresu
   7) prawie dostępu do danych osobowych, żądania ich sprostowania, uzupełnienia, usunięcia lub ograniczenia przetwarzania danych osobowych, prawie do wniesienia sprzeciwu wobec przetwarzania, prawie do odwołania zgody na dalsze przetwarzanie, prawie do przenoszenia danych, prawie do wniesienia skargi do organu nadzorczego.
2. Administrator przekazuje powyższe informacje w formie pisemnej lub elektronicznej podczas pozyskiwania danych osobowych lub w przypadku zmiany celu przetwarzania danych, którymi już dysponuje.
3. W imieniu Administratora, inspektor ochrony danych (IDO) lub osoba przez niego upoważniona w zwięzłej, zrozumiałej formie prowadzi z osobą, której dane dotyczą, wszelką komunikację (pisemną lub elektroniczną) w sprawie informacji dotyczącej przetwarzania danych osobowych, w tym dotyczących sprostowania, uzupełnienia, usuwania danych osobowych, sprzeciwu wobec dalszego przetwarzania lub odwołania zgody.

PRAWO DOSTĘPU PRZYSŁUGUJACE OSOBIE, KTÓREJ DANE DOTYCZĄ

§ 12

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsc, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   1) cele przetwarzania
   2) kategorie odnośnych danych osobowych
   3) informacje o odbiorcach lub kategoriach odbiorców, którym dane zostaną lub zostały ujawnione
   4) w miarę możliwości planowany okres przechowywania danych osobowych lub kryteria ustalenia tego okresu
   5) informacje o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec przetwarzania
   6) informacje o prawie wniesienia skargi do UODO
   7) informacje o źródle pozyskania danych jeśli dane nie zostały zebrane od Administratora
   8) informacje o ewentualnym zautomatyzowanym podejmowaniu decyzji.
2. Administrator prowadzi z osobą, której dane dotyczą wszelką komunikację w zakresie dotyczącym przetwarzania jej danych. Informacji udziela się na piśmie, a w przypadku korespondencji elektronicznej stosuje się postanowienia § 25.
3. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
4. Wszelkie czynności związane z kopiowaniem dokumentów lub utrwalaniem obrazu dokumentu za pomocą zdjęć fotograficznych przez osobę której dane dotyczą muszą być odnotowane przez pracownika właściwej rzeczowo jednostki organizacyjnej Administratora (np. pracownika dziekanatu lub kasy).
5. Czynności, o których mowa:

1) w ust. 2 prowadzi Lokalny administrator w porozumieniu z IDO
2) w ust. 3 prowadzi pracownik właściwej rzeczowo jednostki organizacyjnej Administratora.

ZABEZPIECZANIE DANYCH OSOBOWYCH

1. POSTANOWIENIA OGÓLNE

§ 13

1. Administrator stosuje odpowiednie środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych, w szczególności zabezpiecza dane przed przetwarzaniem z naruszeniem przepisów prawa, w tym przed:
   1) udostępnieniem osobom nieuprawnionym
   2) utratą, uszkodzeniem lub zniszczeniem.
2. Stosowane środki techniczne i organizacyjne zapewniają w sposób ciągły poufność, integralność, dostępność i odporność systemów przetwarzania, a także zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu naruszenia danych.
3. Administrator prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych.
4. Administrator na bieżąco ocenia skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych.
5. Każda osoba, która w imieniu Administratora przetwarza dane osobowe jest odpowiedzialna za ich ochronę w tym przetwarzanie zgodne z prawem.

§ 14

Przetwarzanie danych osobowych wbrew postanowieniom Polityki prowadzące do naruszenia praw i wolności osób, których dane są przetwarzane, może być uznane za ciężkie naruszenie podstawowych obowiązków służbowych uzasadniające rozwiązanie umowy w trybie natychmiastowym.

§ 15

1. Dane osobowe muszą być:
   1) przetwarzane zgodnie z prawem
   2) przetwarzane przez osoby posiadające odpowiednie upoważnienia oraz przeszkolone w zakresie przetwarzania danych osobowych
   3) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami
   4) merytorycznie poprawne i w razie potrzeby uaktualnione
   5) adekwatne oraz ograniczone do tego, co niezbędne w stosunku do celów, w jakich są przetwarzane
   6) przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania danych osobowych
   7) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
2. Ochronie podlegają dane zgromadzone w jakiejkolwiek formie, w tym w dokumentach, kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w systemach informatycznych.
3. Przetwarzanie danych może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień do przetwarzania danych wynika z zakresu upoważnienia.

2. ZASADY DOPUSZCZENIA DO PRZETWARZANIA DANYCH

A. UPOWAŻNIENIA

§ 16

1. Do przetwarzania danych osobowych mogą być dopuszczone osoby do tego upoważnione.
2. Administrator upoważnia IDO do udzielania upoważnień do przetwarzania danych osobowych, określania zakresu upoważnień, zmiany zakresu oraz uchylania upoważnień.
3. Upoważnienie do przetwarzania danych IDO wydaje z urzędu w ramach zatrudniania nowego pracownika w porozumieniu z Lokalnym administratorem lub na jego wniosek składany drogą elektroniczną w celu zmiany lub uchylenia upoważnienia.
4. IDO upoważnia do przetwarzania danych, o ile przetwarzanie danych osobowych na danym stanowisku jest konieczne.
5. Upoważnienie zawiera imię, nazwisko osoby upoważnionej, stanowisko służbowe, zakres upoważnienia i jest sporządzone w dwóch egzemplarzach, z czego jeden otrzymuje osoba upoważniona, a drugi pozostaje w dokumentacji IDO.
6. Wzór upoważnienia stanowi załącznik nr 1 do Polityki.
7. Rejestr elektroniczny upoważnień do przetwarzania danych osobowych prowadzi ASI.

B. SZKOLENIA

§ 17

1. Osoba upoważniana do przetwarzania danych podlega obowiązkowemu szkoleniu wstępnemu, w ramach którego zostaje zapoznana z powszechnymi przepisami prawa dotyczącymi ochrony danych osobowych oraz przepisami wewnętrznymi, a w szczególności niniejszą Polityką.
2. Wzór karty szkolenia wstępnego, oświadczenia o poufności danych osobowych i tajemnicy służbowej stanowi odpowiednio załącznik nr 2 i 3 do Polityki.
3. Wszyscy pracownicy poddawani są cyklicznym szkoleniom okresowym w zakresie ochrony danych osobowych.

3. ZASADY ZABEZPIECZENIA OBSZARU PRZETWARZANIA DANYCH OSOBOWYCH

§ 18

1. Administrator określa następujący obszar, w którym przetwarzane są dane osobowe:
   1) siedziba Administratora: budynek przy ul. Bankowej 8, 40-007 Katowice
   2) budynek przy ul. Ścigały 9, 40-208 Katowice
   3) budynek przy al. Krzywoustego 9, 40-870 Katowice.
2. Budynki i pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczane w ten sposób że, Administrator:
   1) stosuje monitoring wizyjny budynków oraz terenu wokół budynków
   2) stosuje systemy alarmowe (włamania/przeciwpożarowy) wraz z grupą interwencyjną – profesjonalną usługą podmiotu zewnętrznego
   3) stosuje systemy podtrzymania zasilania w razie awarii zasilania oraz zakłócenia sieci energetycznej serwerów
   4) okna zabezpiecza kratami
   5) ewidencjonuje pobranie i zwrot kluczy.

A. MONITORIG

§ 19

1. Monitoring wizyjny (kamery nie rejestrują dźwięku) budynków oraz terenu wokół budynku Uczelni jest stosowany w celu zapewnienia bezpieczeństwa i porządku oraz ochrony osób i mienia.
2. Nagrania z monitoringu są przetwarzane maksymalnie przez okres 3 miesięcy.
3. Administrator nie udostępnia nagrań z monitoringu, chyba że stanowią one dowód w postępowaniu i wnioskuje o nie organ prowadzący postępowanie (np. w celu ustalenia sprawcy kolizji drogowej).
4. Monitoring wizyjny nie obejmuje pomieszczeń szatni, sanitariatów oraz stołówki studenckiej.
5. Szczegółowe zasady dotyczące monitoringu wizyjnego określa Regulamin Monitoringu Wizyjnego we WSZOP.

B. SYSTEMY ALARMOWE

§ 20

Administrator stosuje zespół urządzeń służących zabezpieczeniu budynków i pomieszczeń przed włamaniem (system alarmu włamania) lub pożarem (system przeciwpożarowy).

C. POLITYKA KLUCZY

§ 21

1. Klucze do budynków i pomieszczeń Uczelni pozostają w dyspozycji pracowników ochrony osób i mienia (Portierzy), którzy stoją na straży bezpieczeństwa mienia Uczelni, z zastrzeżeniem ust. 2.
2. Postanowienie ust. 1 nie dotyczy pomieszczeń, do których – z uwagi na bezpieczeństwo danych osobowych – dostęp może mieć jedynie osoba upoważniona do przetwarzania danych.
3. Do zadań Portierów należy w szczególności:
   1) ewidencjonowanie wszystkich przypadków pobrania i zwrotu kluczy do budynków lub pomieszczeń
   2) wydawanie kluczy do pomieszczeń Uczelni osobom upoważnionym przez IDO na podstawie okresowo aktualizowanego wykazu
   3) kontrola bezpieczeństwa budynku, w tym pomieszczeń Uczelni po zakończeniu pracy, w ramach realizowanego obchodu.
4. Szczegółowy tryb przechowywania i wydawania kluczy określa Polityka kluczy.
5. Kierownik działu kadr i płac jest zobowiązany do niezwłocznego informowania IDO o zmianach personalnych oraz o zmianie lokalizacji miejsc przetwarzania danych osobowych.

4. ZASADY ZABEZPIECZANIA DANYCH OSOBOWYCH NA STANOWISKU PRACY

§ 22

1. Każdy pracownik lub inna osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania szczególnej staranności podczas przetwarzania, tj. zabezpieczenia danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem danych, a także dostępem osób nieupoważnionych.
2. Obowiązek, o którym mowa w ust. 1 polega w szczególności na:
   1) przetwarzaniu tylko tych danych, które są niezbędne do realizacji zadań Administratora lub zostały dobrowolnie podane przez osobę, której dane dotyczą
   2) przechowywaniu dokumentacji zawierającej dane osobowe wyłącznie w przeznaczonych do tego zamykanych szafach
   3) zabezpieczaniu hasłem dostępu sprzętu komputerowego

4) niezapisywaniu danych osobowych na urządzeniach przenośnych (pamięci flash, dyski twarde, płyty CD, DVD itp.), chyba że są zabezpieczone programem szyfrującym i przydzielone w ramach czynności służbowych
5) nieużywaniu prywatnych urządzeń przenośnych
6) nieopuszczaniu stanowiska pracy bez uprzedniego zabezpieczenia danych osobowych, tj. w przypadku czasowego opuszczenia stanowiska lub po zakończeniu pracy
7) nieprzekazywaniu dokumentacji zawierającej dane osobowe osobom do tego nieupoważnionym
8) niepozostawianiu dokumentów zawierających dane osobowe w drukarkach, skanerach, kopiarkach
9) uważnym adresowaniu korespondencji wysyłanej pocztą elektroniczną lub zwykłą
10) niekserowaniu oraz niedrukowaniu dokumentów zawierających dane osobowe poza obszarem Administratora, chyba że Administrator zawarł w tym zakresie umowę powierzenia z procesorem
11) nieprzekazywaniu osobom nieupoważnionym kluczy do pomieszczeń, szafek, biurek, sejfów, w których znajdują się dane osobowe
12) ustawieniu monitora komputera w sposób uniemożliwiający wgląd w przetwarzane dane osobom nieupoważnionym
13) zgłaszaniu naruszeń dotyczących ochrony danych osobowych lokalnemu Administratorowi oraz inspektorowi ochrony danych (IDO)
14) zgłaszaniu ASI wszelkich awarii dotyczących sprzętu komputerowego
15) konsultowanie wszelkich wątpliwości dotyczących przetwarzania ochrony danych osobowych z IDO.

3. Przez osoby upoważnione do przetwarzania danych należy rozumieć pracowników lub inne osoby upoważnione przez IDO do przetwarzania danych osobowych.
4. Osoba, której dane dotyczą może pisemnie upoważnić inną osobę (np. członka rodziny/starostę grupy studenckiej) do załatwienia w jej imieniu sprawy w Uczelni, a więc do przetwarzania jej danych osobowych. Wzór upoważnienia stanowi załącznik nr 4-5 do Polityki.

§ 23

Usługi utrzymania czystości pomieszczeń Uczelni są realizowane poza godzinami pracy z wyłączeniem pomieszczeń archiwum oraz serwerowni, w których usługi te mogą być realizowane wyłącznie podczas obecności pracownika jednostki w czasie jego godzin pracy.

5. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH PODCZAS CZYNNOŚCI SŁUŻBOWYCH

A. PRZEKAZYWANIE DANYCH OSOBOWYCH

§ 24

Informacje zawierające dane osobowe są przekazywane organom administracji państwowej (odbiorcom danych) w ramach realizacji obowiązków prawnych Administratora (np. celem rejestracji pracownika w ZUS, Urzędzie Skarbowym, Systemie Polon). Informacje zawierające dane osobowe mogą być przekazywane:

1) osobie, której te dane dotyczą lub osobie przez nią upoważnionej zgodnie z § 22 ust. 4 Polityki
2) osobie upoważnionej przez IDO w ramach struktury organizacyjnej, w tym zakresu czynności związanych ze stanowiskiem pracy
3) procesorowi na podstawie zawartej z Administratorem umowy powierzenia danych osobowych.

§ 25

1. Z uwagi na brak możliwości identyfikacji tożsamości osoby, informacje zawierające dane osobowe nie mogą być udzielane podczas rozmowy telefonicznej.
2. Informacje zawierające dane osobowe mogą być udzielane za pośrednictwem poczty elektronicznej osobie, której dane dotyczą, wyłącznie na adres e-mail wskazany przez nią w kwestionariuszu Administratora (np. kwestionariusz kandydata do pracy, pracownika, studenta, słuchacza).
3. Podczas wysyłki poczty elektronicznej do większej liczby odbiorców (tzw. wysyłka masowa), nadawca jest zobowiązany do ukrycia adresów odbiorców e-mail, chyba że są to adresy założone przez Administratora do realizacji zadań służbowych (domena: wszop.edu.pl).

B. UDOSTĘPNIANIE DANYCH OSOBOWYCH

§ 26

1. Administrator udostępnia dane osobowe organom prowadzącym postepowanie (sąd, prokuratura, policja, ZUS) na pisemny wniosek wskazujący cel przetwarzania danych.
2. Decyzję o udostępnieniu danych osobowych w imieniu Administratora podejmuje IDO.
3. IDO prowadzi dokumentację danych udostępnionych organom, w tym kopii udostępnionych dokumentów.

C. PUBLIKACJA ZDJĘĆ, INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§ 27

1. Publikacja wyników egzaminów, kolokwiów, list studentów, którzy uzyskali stypendia, w szczególności stypendia socjalne lub specjalne, list rankingowych w ramach projektów UE jest możliwa wyłącznie przy zastosowaniu anonimizacji danych osobowych, a w szczególności imienia i nazwiska.
2. Publiczne ogłoszenie wyników egzaminów jest dopuszczalne gdy osoby, których dane dotyczą wyraziły na to zgodę, w przeciwnym wypadku komisja egzaminacyjna ogłasza wyniki indywidulanie.
3. Dozwolone jest publikowanie danych osobowych osoby, której dane dotyczą bez uzyskania jej zgody na publikację gdy odnoszą się do:
   1) zdjęcia zawierającego wizerunek osoby, który
      a) wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych
      b) stanowi jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza
   2) informacji mających związek z powierzoną funkcją (reprezentacyjną np. Rektor), merytoryczną (sylwetka promotora).
4. Przez publikację, o której mowa w ust. 3 należy w szczególności rozumieć udostepnienie danych w internecie (na stronie internetowej, fb, instagramie, ENSie).

D. REKRUTACJA KANDYDATÓW DO PRACY

§ 28

1. Dokumenty aplikacyjne, które wpływają do Administratora podlegają rejestracji zgodnie z procedurą rejestracji dokumentów aplikacyjnych.
2. Dokumenty aplikacyjne (cv, listy motywacyjne) kandydatów do pracy są przechowywane przez okres realizacji procesu rekrutacji, chyba że kandydaci wyrazili zgodę na uczestnictwo w kolejnych przyszłych rekrutacjach, jednak przez okres nie dłuższy niż 5 lat.

E. KOPIOWANIE/ UTRWALANIA OBRAZU DOKUMENTÓW ZAWIERAJĄCYCH DANE OSOBOWE

§ 29

1. O ile obowiązek przechowywania kopii dokumentów zawierających dane osobowe nie wynika wprost z przepisów prawa, a jest potrzebny do celów dowodowych (np. stanowi podstawę uzyskania prawa do świadczeń z ZFŚS lub do stypendium socjalnego) Administrator przechowuje tylko te kopie dokumentów które uzna za niezbędne, a w pozostałym zakresie żąda dokumentów do wglądu i na ich podstawie przygotowuje notatkę zawierającą wymagane informacje.
2. Postanowienie ust. 1 powinno mieć zastosowanie w szczególności w zakresie dokumentów zawierających wrażliwe dane osobowe (np. orzeczenia/zaświadczenia lekarskie, wyroki sądowe).

§ 30

1. O ile o utrwalenie obrazu za pomocą fotografii dokumentów zawierających dane osobowe zwróci się osoba, której dane dotyczą, fakt dokonania tej czynności musi być odnotowany przez pracownika właściwej rzeczowo jednostki organizacyjnej Administratora (np. pracownika dziekanatu) przez wskazanie daty i rodzaju utrwalonych za pomocą zdjęcia dokumentów.
2. Postanowienie ust. 1 ma także zastosowanie gdy czynność, o której mowa w ust. 1 jest realizowana przez reprezentantów organów prowadzących postepowanie np. Policję.
3. O czynnościach, o których mowa w ust. 1-2 powiadamiany jest IDO.

F. ZASADY REALIZACJI MARKETINGU BEZPOŚREDNIEGO

§ 31

1. Administrator przetwarza dane osobowe (imię, nazwisko, adres e-mail, numer telefonu) w celu realizacji marketingu bezpośredniego skierowanego do:
   1) studenta, absolwenta, słuchacza, uczestnika kursów, szkoleń, konferencji na podstawie prawnie uzasadnionego interesu Administratora
   2) osób zaproszonych do udziału w eventach promocyjnych pod warunkiem uzyskania zgody na przetwarzanie jego danych osobowych do celu marketingu bezpośredniego.
2. Administrator zaprzestaje przetwarzania danych osobowych do celów marketingu bezpośredniego jeśli osoby o których mowa:
   1) w ust. 1 pkt 1 wniosą sprzeciw wobec dalszego przetwarzania
   2) w ust. 1 pkt 2 odwołają wcześniej wyrażoną zgodę.
3. Szczegółowe zasady realizacji marketingu bezpośredniego określa stosowna procedura.

G. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

§ 32

1. Dostęp do systemu informatycznego zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora użytkownika i hasła, które podlega okresowej zmianie.
2. Pierwsze hasło jest nadawane przez ASI.
3. Użytkownik systemu chroni hasło przed dostępem osób trzecich, w przypadku, ujawnienia, wymagana jest zmiana.
4. Przy generowaniu hasła należy stosować duże litery, cyfry i/lub znaki specjalne, minimum osiem znaków, tak aby hasło było kategorii „silne".
5. Do czynności związanych z wykonywaną pracą służy służbowa poczta elektroniczna. Pracownicy nie są upoważnieni do posługiwaniem się adresem prywatnym do załatwiania czynności służbowych.

9

6. Użytkownicy systemu powinni zwrócić szczególna uwagę na poprawność adresu poczty elektronicznej odbiorcy dokumentu.
7. Monitory ekranowe są zabezpieczone wygaszaczami chronionymi hasłem.
8. Po zakończeniu pracy na stanowisku komputerowym wymagane jest wyłączenie listwy zasilającej w którą wyposażone jest stanowisko oraz wykonanie kopii bezpieczeństwa poczty e-mail przez uruchomienie przycisku/ikony „Kopiowanie poczty" znajdującego się na pulpicie.
9. Aktywność użytkowników systemu komputerowego jest monitorowana.
10. Po rozwiązaniu stosunku pracy ASI blokuje, kasuje lub wyłącza dostęp do systemów, konta mobilnego i poczty elektronicznej. Identyfikatory użytkownika nie mogą być przydzielane innej osobie.

§ 33

1. Serwery, na których przechowywane są dane osobowe, znajdują się w odrębnym, zamykanym pomieszczeniu Administratora.
2. Oprogramowanie stosowane na stanowiskach komputerowych jest legalne, posiada ważne licencje i jest na bieżąco aktualizowane.
3. W przypadku podejrzenia wystąpienia wirusa w sieci informatycznej, użytkownik systemu powinien niezwłocznie zgłosić podejrzenie do ASI.
4. Ochrona przed dostępem do danych komputera z sieci publicznej jest realizowana przez zewnętrzną zaporę ogniową Firewall.
5. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe.

§ 34

1. W celu zabezpieczenia przetwarzanych w systemie informatycznym danych osobowych tworzy się kopie zapasowe nośników danych.
2. Archiwizacja danych z serwerów wykonywana jest w cyklach dziennych i tygodniowych na zewnętrzny serwer plików w sieci lokalnej. Dodatkowe kopie bezpieczeństwa na nośnikach magnetycznych optycznych i elektronicznych wykonuje okresowo ASI w ramach swoich obowiązków. Kopie bezpieczeństwa przechowywane są w metalowej szafie w pomieszczeniu ASI.
3. Dostęp do nośników danych posiadają: IDO oraz ASI.
4. Niszczenie nośników kopii zapasowych odbywa się w sposób mechaniczny w obecności co najmniej trzyosobowej komisji, która sporządza protokół zniszczenia.
5. ASI przechowa protokoły usunięcia nośników, o których mowa w ust. 4.

§ 35

1. Przekazywane na zewnątrz nośniki magnetyczne pozbawiane są zapisów zawierających dane osobowe poprzez wymazywanie informacji oraz formatowanie nośnika.
2. Uszkodzone nośniki magnetyczne przed wyrzuceniem są trwale fizycznie niszczone w sposób mechaniczny. Postanowienia § 34 ust. 4-5 stosuje się odpowiednio.

§ 36

1. Pracownik, któremu został przyznany komputer przenośny odpowiada za jego stan techniczny i bezpieczeństwo oraz oprogramowanie i dane osobowe. Na komputerze przenośnym, na którym przetwarzane są dane osobowe wymagana jest instalacja oprogramowania do szyfrowania danych.
2. Nie jest dopuszczalne używanie komputera przenośnego do celów prywatnych.

§ 37

1. Wszystkie awarie urządzeń serwerowych, sprzętu komputerowego, systemu operacyjnego i programów należy zgłaszać bezpośrednio do ASI, który współpracuje z IDO.

2. Szczegółowe zasady przetwarzania danych w systemach informatycznych określają stosowne procedury.

NARUSZENIA PRZETWARZANIA DANYCH OSOBOWYCH

§ 38

1. Osoba przetwarzająca dane osobowe w imieniu Administratora informuje IDO o wszelkich naruszeniach danych osobowych, w szczególności dotyczących niezgodnego z prawem zniszczenia, utracenia, w tym kradzieży albo zagubienia, nieuprawnionego dostępu do danych.
2. Typowe naruszenia przetwarzania danych osobowych dotyczą:
   1) ustnego ujawnienia osobie nieuprawnionej danych osobowych albo zabezpieczeń danych osobowych
   2) zgubienia lub kradzieży dokumentu, komputera, telefonu lub innego nośnika danych zawierającego dane osobowe pracowników, współpracowników, studentów
   3) błędnego wskazanie adresata w korespondencji zawierającej dane osobowe wysłanej pocztą tradycyjną lub elektroniczną
   4) doprowadzenia do nieuprawnionego dostępu do systemu informatycznego, pomieszczenia, komputera, w którym przetwarzane są dane osobowe
   5) stwierdzenia włamania lub próby włamania do budynku, pomieszczenia, szafki, sejfu, w którym przetwarzane są dane osobowe
   6) zapisania i pozostawienia w widocznym miejscu hasła do systemu informatycznego
   7) pozostawienia niezabezpieczonych dokumentów zawierających dane osobowe
   8) niekorzystania z niszczarek dokumentów.
3. Inspektor ochrony danych prowadzi rejestr naruszeń, który zawiera:
   1) okoliczności naruszenia ochrony danych osobowych
   2) kategorię i przybliżoną liczbę osób, których dane dotyczą
   3) kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie
   4) skutki naruszenia ochrony danych osobowych
   5) podjęte działania zaradcze.
4. Administrator zawiadamia organ nadzorujący o naruszeniu ochrony danych osobowych bez zbędnej zwłoki (w miarę możliwości w terminie 72 godzin po stwierdzeniu naruszenia), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
5. Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony jej danych osobowych jeżeli to naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

§ 39

1. Administrator tworzy rejestr czynności przetwarzania danych osobowych.
2. Rejestr czynności przetwarzania danych osobowych (Rejestr) prowadzi IDO w formie elektronicznej.
3. Rejestr zawiera:
   1) kategorie danych osobowych
   2) opis kategorii osób, których dane dotyczą
   3) cele przetwarzania danych
   4) podstawę prawną przetwarzania danych
   5) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione
   6) informacje dotyczące przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej
   7) planowane terminy usunięcia poszczególnych danych.

9

AUDYTY I KONTROLE

§ 40

1. IDO oraz ASI przeprowadzają okresowe kontrole i audyty w zakresie ochrony danych osobowych.
2. W ramach czynności, o których mowa w ust. 1 weryfikowany jest system zabezpieczeń (działanie ochrony antywirusowej) oraz przestrzeganie środków technicznych oraz organizacyjnych w szczególności:
   1) zakres przetwarzanych danych w kontekście upoważnienia do przetwarzania danych oraz posiadania kluczy
   2) zabezpieczanie danych osobowych w zamykanych szafach
   3) sprawdzanie częstotliwości zmian haseł i ich przechowywania
   4) zakres informacji przekazywanych drogą elektroniczną
   5) poprawność publikacji danych osobowych.
3. Po przeprowadzonej kontroli lub audycie sporządza się protokół zawierający zalecenia, w przypadku stwierdzonych naruszeń stosuje się postanowienia § 38 ust. 3-5 Polityki.

POSTANOWIENIE KOŃCOWE

§ 41

1. Lokali administratorzy i IDO zobowiązani są do współdziałania w celu zapewnienia należytego przestrzegania przepisów dotyczących ochrony danych osobowych.
2. Naruszenie Polityki może być uznane za ciężkie naruszenie podstawowych obowiązków dające podstawę do rozwiązania umowy w trybie natychmiastowym, a także uprawniające Administratora do dochodzenia odszkodowania.

§ 42

1. Polityka wchodzi w życie z dniem 7 grudnia 2018 r.
2. Z dniem 1 grudnia 2018 r. traci moc Zarządzenie nr 24/2009/10 Rektora WSZOP z dnia 29 lipca 2010 r. w sprawie wprowadzenia polityki bezpieczeństwa informacji.
3. O ile postanowienia Polityki wymagają uszczegółowienia, Administrator wprowadza zarządzeniem procedury regulujące określoną materię ochrony danych osobowych.

§ 43

Określa się wykaz załączników do Polityki:
1) załącznik nr 1 – upoważnienie do przetwarzania danych osobowych udzielane przez IDO
2) załącznik nr 2 – wzór karty szkolenia wstępnego w zakresie ochrony danych osobowych
3) załącznik nr 3 – wzór oświadczenia o zachowaniu poufności danych osobowych i tajemnicy służbowej
4) załącznik nr 4 – upoważnienie do przetwarzania danych osobowych udzielane przez osobę, której dane dotyczą
5) załącznik nr 5 – upoważnienie do przetwarzania danych osobowych udzielane przez osoby, których dane dotyczą (tzw. upoważnienie zbiorcze)

REKTOR

prof. dr hab. inż. Bohdan Mochnacki

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr.....

Upoważniam Pana/ią: .....

Zatrudnionego/ą na stanowisku: .....

do przetwarzania, w zakresie niezbędnym do realizacji powierzonej funkcji, danych osobowych w następujących zbiorach:

l.p.	typ zbioru (*)	nazwa systemu i/lub modułu, nazwa zbioru	identyfikator	rodzaj uprawnienia (**)	data wygaśnięcia

(*) - (P) papierowa, (E) elektroniczna, (S) system informatyczny
(**) - (WG) wglądu, (W) wprowadzania, (M) modyfikacji, (U) usuwania, (A) archiwizacji i zobowiązuję do przestrzegania Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemami Informacji służącymi do przetwarzania danych osobowych w Wyższej Szkole Zarządzania Ochroną Pracy w Katowicach wprowadzonej Zarządzeniem Rektora WSZOP Nr 24/2009/10 z dnia 29 lipca 2010 roku w sprawie wprowadzenia polityki bezpieczeństwa informacji.
Upoważnienie obowiązuje do dnia odwołania lub wygasa z chwilą ustania zatrudnienia w WSZOP.

Osoba upoważniona:

.....
data i podpis

Inspektor Ochrony Danych:

.....
data i podpis

KARTA SZKOLENIE WSTĘPNEGO
W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

imię i nazwisko osoby i odbywającej szkolenie:	
stanowisko służbowe:	
termin szkolenia wstępnego:	

....

podpis osoby szkolonej *podpis inspektora ochrony danych*

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

I. POSTANOWIENIA OGÓLNE

1. Każdy pracownik lub inna osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania szczególnej staranności podczas przetwarzania, tj. zabezpieczenia danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem danych, a także dostępem osób nieupoważnionych.
2. Obowiązek, o którym mowa w ust. 1 polega w szczególności na:
   1) przetwarzaniu tylko tych danych, które są niezbędne do realizacji zadań Administratora lub zostały dobrowolnie podane przez osobę, której dane dotyczą
   2) przechowywaniu dokumentacji zawierającej dane osobowe wyłącznie w przeznaczonych do tego zamykanych szafach
   3) zabezpieczaniu hasłem dostępu nośników danych (komputery)
   4) nieużywaniu prywatnych urządzeń przenośnych
   5) niezapisywaniu danych na urządzeniach przenośnych (pamięci flash, dyski twarde, płyty CD, DVD itp.), chyba że są zabezpieczone hasłem dostępu i przydzielone w ramach czynności służbowych
   6) nieopuszczaniu stanowiska pracy bez uprzedniego zabezpieczenia danych osobowych, tj. w przypadku czasowego opuszczenia stanowiska lub po zakończeniu pracy
   7) nieprzekazywaniu dokumentacji zawierającej dane osobowe osobom do tego nieupoważnionym
   8) niepozostawianiu dokumentów zawierających dane osobowe w drukarkach, skanerach, kopiarkach
   9) uważnym adresowaniu korespondencji wysyłanej pocztą elektroniczną lub zwykłą
   10) niekserowaniu oraz niedrukowania dokumentów zawierających dane osobowe poza obszarem Administratora, chyba że Administrator zawarł w tym zakresie umowę powierzenia z procesorem
   11) nieprzekazywaniu osobom nieupoważnionym kluczy do pomieszczeń, szafek, biurek, sejfów, w których znajdują się dane osobowe
   12) ustawieniu monitora komputera w sposób uniemożliwiający wgląd w przetwarzane dane osobom nieupoważnionym
   13) zgłaszaniu naruszeń dotyczących ochrony danych osobowych lokalnemu Administratorowi oraz inspektorowi ochrony danych (IDO)
   14) konsultowanie wszelkich wątpliwości dotyczących przetwarzania ochrony danych osobowych z IDO.

II. FORMA PRZEKAZYWANIA DANYCH OSOBOWYCH

1. Informacje zawierające dane osobowe mogą być przekazywane:
   1) osobie, której te dane dotyczą lub osobie przez nią pisemnie upoważnionej
   2) osobie upoważnionej przez IDO
   3) procesorowi na podstawie zawartej z Administratorem umowy powierzenia danych osobowych.
2. Z uwagi na brak możliwości identyfikacji tożsamości osoby, informacje zawierające dane osobowe nie mogą być udzielane podczas rozmowy telefonicznej.
3. Informacje zawierające dane osobowe mogą być udzielane za pośrednictwem poczty elektronicznej osobie, której dane dotyczą, wyłącznie na adres e-mail wskazany przez nią w kwestionariuszu Administratora (np. kwestionariusz kandydata do pracy, pracownika, studenta, słuchacza).
4. Podczas wysyłki poczty elektronicznej do większej liczby odbiorców (tzw. wysyłka masowa), nadawca jest zobowiązany do ukrycia adresów odbiorców e-mail, chyba że są to adresy założone przez Administratora do realizacji zadań służbowych (domena: wszop.edu.pl).

III. PUBLIKACJA ZDJĘĆ, INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

1. Publikacja wyników egzaminów, kolokwiów, list studentów, którzy uzyskali stypendia, w szczególności stypendia socjalne lub specjalne, list rankingowych w ramach projektów UE jest możliwa wyłącznie przy zastosowaniu anonimizacji imienia i nazwiska.
2. Publiczne ogłoszenie wyników egzaminów jest dopuszczalne gdy osoby, których dane dotyczą wyraziły na to zgodę, w przeciwnym wypadku komisja egzaminacyjna ogłasza wyniki indywidulanie.
3. Dozwolone jest publikowanie danych osobowych osoby, której dane dotyczą bez uzyskania jej zgody na publikację gdy odnoszą się do:
   1) zdjęcia zawierającego wizerunek osoby, który:
      a) wykonano w związku z pełnieniem przez nią funkcji publicznych w szczególności politycznych, społecznych, zawodowych
      b) stanowi jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza
   2) informacji mających związek z realizacją czynności reprezentacyjnych/merytorycznych (np. publikacja sylwetki rektora/promotora pracy dyplomowej)

   Przez publikację, o której mowa w ust. 3 należy w szczególności rozumieć udostepnienie danych w internecie (na stronie www., fb, instagramie, ENSie).

Oświadczam, że zapoznałem się z *Polityką Bezpieczeństwa Ochrony danych osobowych w Wyższej Szkole Zarządzania Ochroną Pracy w Katowicach i zobowiązuję się do jej przestrzegania*

.....

podpis osoby szkolonej

imię i nazwisko osoby upoważnionej do przetwarzania danych:	
stanowisko służbowe:	

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI DANYCH OSOBOWYCH ORAZ TAJEMNICY SŁUŻBOWEJ

W związku z wykonywaną pracą w Wyższej Szkole Zarządzania Ochroną Pracy w Katowicach, zobowiązuję się do zachowania w tajemnicy danych do których mam lub będę miał/a dostęp w związku z wykonywaniem czynności służbowych, w tym:

1) danych osobowych oraz sposobów ich zabezpieczania
2) danych mających charakter *know-how* Uczelni, a dotyczących w szczególności:
   - organizacji Uczelni w tym studiów i innych form kształcenia
   - planów rozwojowych Uczelni, w tym przeprowadzanych analiz i wyników
   - strategii marketingowych, w tym metod pozyskiwania kandydatów na studia i inne formy kształcenia oraz raportów rekrutacyjnych
   - interesariuszy, kadry dydaktycznej, w tym warunków współpracy
3) danych dotyczących mienia i gospodarki finansowej Uczelni, a dotyczących w szczególności:
   - budżetu, planów, sprawozdań i raportów finansowych
   - kosztów bieżącej działalności Uczelni, przychodów i inwestycji
   - majątku rzeczowego (baza lokalowa, dydaktyczna).

Przyjmuję do wiadomości, że:

1) niedochowanie ww. zobowiązań może być uznane za ciężkie naruszenie obowiązków i skutkować rozwiązaniem współpracy w trybie natychmiastowym
2) obowiązek zachowania tajemnicy w zakresie danych osobowych, danych mających charakter *know-how* oraz danych dotyczących mienia i gospodarki finansowej Uczelni nie wygasa z chwilą rozwiązania stosunku pracy / ustania współpracy.

Podstawa prawna:

1) art. 6; 9 rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych
2) art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 208 r., poz. 1000)
3) art. 72^1 ustawy z dnia 23 kwietnia 1963 r. kodeks cywilny (tj. Dz.U. z 2017 r., poz. 459 poźn. zm.)
4) art. 266 ustawy z dnia 6 czerwca 1997 r. kodeks karny (tj. Dz. U. z 2017 r., poz. 2204 ze zm.).
5) art. 52 § 1 pkt 1 ustawy z dnia 26 czerwca 1974 r. kodeks pracy w związku z art. 100 § 1 pkt 4 kp (tj. Dz.U. z 2018 r., poz. 10 ze zm.)
6) Polityka Bezpieczeństwa Ochrony Danych Osobowych w Wyższej Szkole Zarządzania Ochroną Pracy w Katowicach.

.....

data i podpis osoby upoważnionej do przetwarzania danych

…….. Katowice, dnia ……..

imię i nazwisko

……

*status: student/słuchacz/pracownik**

UPOWAŻNIENIE

Upoważniam ……

imię i nazwisko, nr dowodu

do przetwarzania moich danych osobowych w celu: odbioru moich dokumentów/ złożenia moich dokumentów/ dokonania opłat* wskazanych poniżej: ……

……

……

……

……

podpis osoby upoważniającej

**niepotrzebne skreślić*

…….. Katowice, dnia ……
kierunek i tryb studiów

……
specjalność, grupa

……
rok akademicki

UPOWAŻNIENIE ZBIOROWE
DLA OSOBY REPREZENTUJĄCEJ GRUPĘ STUDENTÓW

Upoważniamy ……
imię i nazwisko osoby reprezentującej grupę studentów, nr albumu

do przetwarzania danych osobowych w roku akademickim ……..w celu:

- reprezentowania interesów studentów przed władzami uczelni, w tym pobieranie list grup i innych dokumentów niezbędnych w organizacji roku akademickiego, odbioru i złożenia indeksu, uzyskania wpisu, uzyskania listy ocen z zaliczeń,
- reprezentowania grupy we współpracy z Dziekanatem w zakresie wszelkich spraw organizacyjnych i technicznych dot. kształcenia

l.p.	imię i nazwisko studenta	nr albumu	czytelny podpis
1.			
2.			
3.			
…			