Polityka Ochrony
Danych Osobowych

Spis treści

Rozdział I - Postanowienia ogólne

§ 1

1. Polityka ochrony danych osobowych w Politechnice Wrocławskiej określa zasady stosowane przez Uczelnię, w celu spełnienia wymagań 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 (ogólne rozporządzenie o ochronie danych) – Dz. Urz. UE L 119 z dnia 04.05.2016 r. i reguły dotyczące procedur zapewnienia bezpieczeństwa przetwarzanych danych osobowych.
2. Polityka ma zastosowanie do wszystkich danych osobowych przetwarzanych w Uczelni w ramach procesów przetwarzania danych osobowych.
3. Obowiązek ochrony danych osobowych przetwarzanych w Uczelni dotyczy wszystkich osób, które mają do nich dostęp. Na ten obowiązek nie mają wpływu zajmowane stanowisko, miejsce wykonywania pracy, charakter stosunku pracy bądź stosunku cywilnoprawnego łączącego zobowiązanego z Uczelnią.
4. Każda osoba, która ma dostęp do danych osobowych, może je przetwarzać wyłącznie na podstawie otrzymanego upoważnienia.
5. Politykę uzupełniać może dokumentacja dotycząca szczegółowych sposobów postępowania z danymi osobowymi w Uczelni. Dokumentacja jest aktualizowana na bieżąco i może ulegać zmianom stosownie do potrzeb Uczelni. Osoby mające dostęp do danych osobowych są zobowiązane do zapoznawania się z dokumentacją oraz do stosowania opisanych tam zasad.
6. Polityka zachowuje zgodność z innymi wewnętrznymi regulacjami z obszaru bezpieczeństwa informacji i systemów informatycznych obowiązującymi w Uczelni.
7. Rektor Politechniki Wrocławskiej zatwierdza zmiany niniejszej Polityki i jej aktualizacje w drodze Zarządzenia Wewnętrznego. Uzupełniające Politykę dokumenty zatwierdzać może (i udostępniać w sposób zwyczajowo przyjęty w Uczelni) osoba wykonująca zadania Administratora danych osobowych wyznaczona przez Rektora.

§ 2

Występujące w niniejszej Polityce zwroty oznaczają:

1. **Administrator danych osobowych (ADO)** - Politechnika Wrocławska z siedzibą we Wrocławiu przy Wybrzeżu Wyspiańskiego 27, reprezentowana przez Rektora (zwana też dalej: Uczelnią). Z przedstawicielami Administratora danych osobowych zapewnia się kontakt przy pomocy formularza na stronie pwr.edu.pl/kontakt.

2. **Dane osobowe** – wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 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.

3. **Dane osobowe szczególne** – kategorie danych określone w art. 9 RODO, w tym: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

4. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora danych osobowych na podstawie art. 37 RODO, która realizuje zadania monitorowania przestrzegania przepisów o ochronie danych osobowych w Uczelni, określone w art. 39 RODO oraz poleceń Administratora danych osobowych.

5. **Jednostka/komórka organizacyjna (J/KO)** – jednostka bądź komórka organizacyjna wynikająca z przyjętej w Uczelni struktury organizacyjnej.

6. **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.

7. **Osoba upoważniona** – osoba upoważniona do przetwarzania danych osobowych przez Administratora danych osobowych (lub przez wskazaną do tego osobę), mająca dostęp do danych, przetwarzanych w systemie informatycznym lub w dokumentacji papierowej.

8. **Podmiot przetwarzający** – podmiot, któremu Uczelnia powierza czynności przetwarzanie danych osobowych w swoim imieniu - w szczególności zawierając umowę powierzenia zgodnie z art. 28 RODO.

9. **Procesor / podmiot przetwarzający** - podmiot (osoba fizyczna lub prawna, organ publiczny), któremu powierzono do przetwarzania dane osobowe w celu określonym przez administratora.

10. **Profilowanie** – oznacza dowolną formę 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.

11. **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

12. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych.

13. **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 (ogólne rozporządzenie o ochronie danych);

14. **UODO** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018, poz. 1000).

15. **Zespół Administratora Danych ds. zgodności z RODO** - zespół powołany na Uczelni, którego celem jest zapewnienie by przetwarzanie danych osobowych, za które odpowiada Politechnika Wrocławska (jako Administrator danych osobowych, współadministrator lub podmiot przetwarzający) odbywało się zgodnie z przepisami RODO.

Rozdział II - Organizacja systemu ochrony danych osobowych w Politechnice Wrocławskiej

§ 3

Podstawowe zasady przetwarzania danych osobowych

1. Wszyscy pracownicy Uczelni są zobowiązani do przestrzegania zasad przetwarzania danych osobowych określonych w Polityce, do reagowania na zauważone nieprawidłowości (np. porzucenie wydruków zawierających dane osobowe, pozostawienie

niezabezpieczonych akt zawierających dane osobowe, niezabezpieczenie pomieszczeń, szaf zawierających akta osobowe itp.) i do zgłaszania takich sytuacji IOD.

2. Każdy pracownik już w trakcie czynności związanych z przyjmowaniem do pracy powinien zostać pouczony o obowiązkach związanych z przetwarzaniem danych (o ile występuje na jego stanowisku pracy) takich jak:
   a) zapoznanie się i przestrzeganie niniejszej Polityki;
   b) ubieganie się o upoważnienie do przetwarzania danych osobowych (z celem i zakresem odpowiadającym obowiązkom i zadaniom pracownika);
   c) ochrony danych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą treści lub nieuprawnionym udostępnieniem;
   d) usuwania z miejsc przetwarzania danych osobowych osób postronnych, jeśli nie ma tam właściwego nadzoru;
   e) niszczenia tylko zbędnych i nie podlegających archiwizacji dokumentów zawierających dane osobowe - najlepiej z użyciem niszczarki;
   f) użytkowania systemów informatycznych, zgodnie z zasadami ustalanymi przez ich administratorów i nieujawniania swoich haseł;
   g) zachowania ostrożności przy przekazywaniu danych osobowych i obowiązku ustalenia, czy osoba, która chce dostać dane jest do tego uprawniona;
   h) posługiwania się przy przetwarzaniu wyłącznie narzędziami i metodami zatwierdzonymi przez Uczelnię;
   i) zachowania szczególnej ostrożności w podróży służbowej, czy w transporcie dokumentów, komputerów i nośników zawierających dane osobowe (także w obrębie kampusu);
   j) usuwania nośników, wydruków i kopii z urządzeń wielofunkcyjnych (nie wolno zostawiać ich bez nadzoru);
   k) przy opuszczeniu miejsca pracy – o zabezpieczeniu dokumentów, nośników czy systemu informatycznego z danymi osobowymi (zasady „czystego biurka” i „czystego ekranu”);
   l) zgłaszania dostrzeżonych nieprawidłowości i naruszeń bezpieczeństwa danych osobowych, przy czym niezwłoczne zgłoszenie naruszenia stanowić będzie okoliczność, uwzględnianą przy ustalaniu odpowiedzialności za uchybienia.
3. Co do zasady zabronione jest przenoszenie danych (szczególnie w postaci papierowej) poza odpowiednio chronione, czy przygotowane do przetwarzania danych obiekty Uczelni. Nie powinno też dochodzić do przesyłania niezabezpieczonych danych osobowych poza systemy informatyczne, nadzorowane przez Administratora danych osobowych. Uzasadnione wyjątki od powyższych zasad (przy zachowaniu minimalnych niezbędnych środków ostrożności) stanowią:
   a) przekazywanie dokumentów/danych osobowych pomiędzy jednostkami organizacyjnymi Uczelni w różnych lokalizacjach;
   b) sytuacje wynikające ze specyfiki realizowanych zadań (np. dostarczenie dokumentacji na rozprawy sądowe);

c) wykonywanie pracy zdalnej na polecenie Administratora danych osobowych przy zastosowaniu wymogów stawianych przez pracodawcę.

4. Akta osobowe pracownika, który przetwarza dane osobowe powinny zawierać m.in. dowody (w formie pisemnej) potwierdzające, że został on upoważniony do przetwarzania danych osobowych i zobowiązał się do nieograniczonego w czasie zachowania tajemnicy co do treści danych osobowych i sposobów ich ochrony.
5. W ramach instruktażu stanowiskowego pracownikowi należy wskazać, gdzie pracodawca udostępnia politykę i procedury (dotyczące danych osobowych), stosowane w Politechnice Wrocławskiej. Jeśli pracownik ma mieć dostęp do danych, należy określić zakres jego upoważnienia - odpowiednio do jego zadań. Bezpośredni przełożony zapewnia, żeby pracownik został zobowiązany do zachowania tajemnicy danych osobowych przed uzyskaniem dostępu do danych.
6. Powyższe zmiany stosuje się również do pracowników zatrudnionych już w chwili wejścia w życie niniejszej Polityki (a wydane im upoważnienia zachowują ważność, o ile nie zachodzi potrzeba ich zaktualizowania bądź uzupełnienia).

§ 4

Upoważnienie do przetwarzania danych osobowych

1. Wszystkie osoby, które wykonują czynności związane z przetwarzaniem danych osobowych w Uczelni, w ramach wykonywania zadań służbowych na stanowiskach pracy lub prac zleconych, muszą być upoważnione do przetwarzania danych osobowych oraz złożyć oświadczenie o zachowaniu tajemnicy danych oraz sposobów ich zabezpieczenia (wzór upoważnienia oraz oświadczenia znajduje się na stronie https://pwr.edu.pl/ochrona-danych-osobowych).
2. W celu uzyskania upoważnienia do przetwarzania danych osobowych osoba wnioskująca musi wypełnić wzór upoważnienia, który po akceptacji przełożonego przekazywany jest do zatwierdzenia do właściwego Prorektora. Po nadaniu (podpisaniu) upoważnienia jego skan trafia do rejestru pełnomocnictw i upoważnień a oryginał do akt osobowych. Osoba upoważniona może uzyskać w Dziale Spraw Osobowych poświadczoną za zgodność kopię upoważnienia. Upoważnienie udzielone w imieniu Administratora danych osobowych jest digitalizowane i włączane do uczelnianego rejestru pełnomocnictw i upoważnień prowadzonego przez Biuro Organizacyjne. Oryginał jest zwracany do Działu Spraw Osobowych, gdzie jest przechowywany w aktach osobowych pracownika. Gdy upoważnienie dotyczy osoby niebędącej pracownikiem, winno być załączane do akt studenckich, lub dokumentacji związanej z odpowiednią umową cywilnoprawną czy projektową, ale nie może być brakowane i należy je zachować w celu zapewnienia Uczelni rozliczalności na wypadek kontroli w zakresie zgodności przetwarzania danych z przepisami.

3. Każda osoba upoważniana do przetwarzania danych osobowych ma obowiązek zapoznać się z dokumentacją dotycząca tego przetwarzania, które ma realizować, w szczególności z niniejszą Polityką ochrony danych osobowych oraz procedurami, które ją uzupełniają.
4. Każda osoba upoważniana do przetwarzania danych osobowych ma obowiązek odbycia szkolenia z zasad ochrony danych osobowych w uczelni. Szkolenia przeprowadza IOD lub inne osoby wg. planu uzgodnionego z Działem Spraw Osobowych. Dopuszcza się możliwość realizacji szkolenia w formie e-learningowej.

Rozdział III - Realizacja obowiązków przy przetwarzaniu danych osobowych

§ 5

1. Zobowiązuje się osoby odpowiedzialne za zaplanowanie nowych działań, dostarczenie, rozwój lub zmiany systemów informatycznych, do uwzględniania na wczesnym etapie planowania, wymogów związanych z ochroną treści danych. W tym celu osoby:
   a) planujące wykorzystanie danych osobowych w działalności Politechniki Wrocławskiej,
   b) projektujące nowe rozwiązania organizacyjne czy informatyczne - dotyczące danych osobowych,
   c) planujące realizację projektów badawczych i naukowych z wykorzystaniem danych, pozwalających pośrednio lub bezpośrednio ustalić tożsamość osób badanych,

   zobowiązane są włączyć w powyższe działania IOD i zapoznać się z jego stanowiskiem co do zgodności z prawem przewidywanego przetwarzania danych osobowych przed podjęciem decyzji o przetwarzaniu danych.
2. Osoby, o których mowa w ust. 1 powyżej w swoich działaniach zapewniają:
   a) aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania (zasada ograniczenia celu),
   b) zidentyfikowanie odpowiednich przesłanek dla planowanych czynności (z katalogu w art. 6, 9 lub 10 RODO),
   c) aby przetwarzanie danych odbywało się nie dłużej niż jest to niezbędne dla osiągnięcia celów przetwarzania (zasada ograniczenia przechowywania danych) i tylko w zakresie w jakim jest to niezbędne do jego osiągniecia (zasada minimalizacji danych),
   d) zastosowanie odpowiednich środków technicznych i organizacyjnych, aby zabezpieczyć dane osobowe,
   e) sposoby dokumentowania działań, które Uczelnia winna zabezpieczyć dla rozliczenia się z wykonania swoich obowiązków,
   f) określenie zadań, kompetencji i uprawnień dla osób realizujących to przetwarzanie,

g) zaplanowanie tego w jaki sposób wykonane będą obowiązki informacyjne z art. 13 i 14 RODO, jeśli dane osobowe będą zbierane od początku lub jeśli przewiduje się użycie już posiadanych danych w nowych celach.

3. Przełożeni osób przetwarzających dane osobowe, mają obowiązek zachowania należytej staranności związanej z tym przetwarzaniem, przez co rozumie się m.in.:
   a) sprawdzenie czy są spełnione podstawy prawne na pozyskiwanie danych osobowych, zgodnie z art. 6 RODO lub art. 9-10 RODO;
   b) sprawdzenie, czy przetwarzanie danych osobowych odbywa się dla określonych, zgodnych z prawem celów realizowanych w Uczelni;
   c) sprawdzenie, czy dane osobowe zbierane są w zakresie adekwatnym do celów w jakich będą przetwarzane w uczelni;
   d) nadzorowanie wykonywania obowiązków informacyjnych oraz dokumentowania tych czynności i możliwości realizowania praw osób, których dane będą przetwarzane.
4. W przypadku, gdy podstawą przetwarzania jest zgoda osoby, której dane dotyczą, należy dodatkowo zapewnić warunki dobrowolnego jej pozyskania oraz powiadomić każdą taką osobę o prawie do odwołania takiej zgody.
5. Osoby, które wykonują zadania związane ze zbieraniem danych osobowych są zobowiązane do wykonywania obowiązków informacyjnych określonych w art. 13 i 14 RODO. Obowiązkiem takich osób jest udzielanie odpowiednich informacji o przetwarzaniu danych w zakresie określonym przez RODO oraz dokumentowanie (zachowanie dowodów), że ten obowiązek został spełniony.
6. Jeżeli przed wejściem w życie niniejszej Polityki nie ustalono przesłanek i nie stosowano odpowiednich klauzul (zgody/informacyjnych), wówczas za uzupełnienie tych uchybień odpowiada przełożony osób, przetwarzających dane osobowe. Zaleca się przy tym m.in. wykorzystanie materiałów udostępnianych na stronie internetowej Uczelni: https://pwr.edu.pl/ochrona-danych-osobowych oraz konsultacji z IOD.

§ 6

1. Dane osobowe zbierane w ramach procesów realizowanych w Uczelni są przetwarzane przez czas określony przez właściwe przepisy prawa lub wewnętrzne przepisy kancelaryjno-archiwalne.
2. Za określenie odpowiednich czasów retencji danych osobowych w procesach przetwarzania danych w Uczelni odpowiada kierownik J/KO odpowiedzialnej za proces zbierania danych. Uwzględnić powinien on przy tym przepisy, określające obowiązki archiwizacyjne i postanowienia Instrukcji Kancelaryjnej Uczelni.
3. Dane osobowe, dla których okres przetwarzania nie wynika z obowiązujących przepisów prawa i dla których nie jest możliwe określenie z góry tego okresu w wewnętrznych przepisach kancelaryjno archiwalnych, są przetwarzane tylko tak długo, jak długo istnieje ściśle konkretny i uzasadniony prawnie cel przetwarzania zgodnie z przesłankami art. 6 ust. 1 RODO.

4. Ustanie celu i brak przesłanek (o których mowa powyżej) przetwarzania danych wymagają niezwłocznego zaprzestania przetwarzania i usunięcia danych.
5. Dane osobowe przetwarzane tylko i wyłącznie w oparciu o przesłankę zgody na przetwarzanie danych osobowych są usuwane zawsze niezwłocznie po wycofaniu takiej zgody, zgodnie z odpowiednią procedurą ustalaną przez administratora danych osobowych. Usunięcie danych osobowych można wyjątkowo zastąpić anonimizacją danych, tylko jeśli całkowite usunięcie danych byłoby niemożliwe, bez poniesienia istotnego uszczerbku dla obowiązków administratora (w szczególności dla prawnych obowiązków dokumentacyjnych i służących wykazaniu rozliczalności).
6. Każda J/KO Uczelni odpowiedzialna za określony proces lub procesy przetwarzania danych osobowych ma obowiązek dokonania przeglądu przynajmniej raz do roku przetwarzanych przez nią danych osobowych, prowadzonych w formie papierowej jak i elektronicznej. Przegląd taki obejmuje co najmniej:
   a) sprawdzenie, czy dane osobowe, dla których upłynął okres przechowywania wynikający z przepisów prawa lub wewnętrznych przepisów kancelaryjno-archiwalnych zostały usunięte,
   b) sprawdzenie, czy w odniesieniu do danych osobowych, których czas przechowywania nie został określony przez właściwe przepisy prawa lub wewnętrzne przepisy kancelaryjno-archiwalne, nadal istnieje podstawa prawna oraz cel przetwarzania danych osobowych.
7. W przypadku ustalenia w trakcie przeglądu, że okres przetwarzania danych osobowych upłynął i nie ma podstawy prawnej lub celu w dalszym przetwarzaniu danych osobowych, takie dane osobowe powinny zostać zanonimizowane. Przez anonimizowanie danych z nośników papierowych rozumie się trwałe ich ukrycie (np. zamazanie). W przypadku nośników elektronicznych oraz systemów informatycznych anonimizowanie polegać może w szczególności na trwałym usunięciu danych, nieodwracalnej zmianie lub zaszyfrowaniu.
8. Szczegółowe zasady niszczenia nośników i wydruków oraz usuwania lub anonimizacji danych w systemach informatycznych, opisane są w ustalonej przez administratora procedurze. Za realizację procedur niszczenia wydruków odpowiada przełożony osób przetwarzających dane (w tym zwłaszcza przechowujących dane). Za realizację procedur dotyczących niszczenia nośników oraz anonimizacji, pseudonimizacji, usuwania danych z systemów informatycznych, czy niszczenia nośników informatycznych pochodzących z systemów zarządzanych przez Dział Informatyzacji odpowiada dyrektor Działu Informatyzacji lub kierownik jednostki organizacyjnej, która zarządza własnymi systemami przetwarzającymi dane osobowe.

§ 7

1. Udostępnienie danych jest jedną z form ich przetwarzania a podstawy takiego udostępnienia określa art. 6 ust. 1 RODO. Do szczególnych obowiązków osób, które

w imieniu Uczelni udostępniają dane osobowe (przekazują je jakiemukolwiek podmiotowi zewnętrznemu czy osobie trzeciej) należy jednoznaczne ustalenie podstaw prawnych pozwalającego na taką czynność - a szczególnie sprawdzenie czy:

a) przepis prawa nakazuje udostępnienie danych;
b) zgoda osoby, której te dane dotyczą pozwala na udostępnienie danych innemu podmiotowi;
c) przewidziano taką czynność w umowie zawartej z odbiorcą danych;
d) wniosek o udostępnienie danych pochodzi od podmiotu uprawnionego i wskazuje prawidłową podstawę prawną do takiej czynności.

Wątpliwości co do podstaw udostępnienia, czy co do zgłoszenia tej czynności do Rejestru należy konsultować z IOD. IOD może dodatkowo konsultować się z radcą prawnym Działu Prawnego Uczelni.

§ 8

1. Powierzenie przetwarzania danych osobowych oznacza, że administrator danych wybiera podmiot przetwarzający (procesora), który w imieniu administratora ma wykonać określone czynności z danymi osobowymi i który stwarza gwarancje, że czynności te będą zgodne z prawem i nie naruszą bezpieczeństwa osób, których te dane dotyczą.
2. Uczelnia w umowie powierzenia przetwarzania może być (odpowiednio do okoliczności w danym przypadku) administratorem albo procesorem:
   a) Uczelnia jest administratorem, gdy to ona decyduje o celach i sposobach przetwarzania danych i wybiera procesora, który przetwarza dane dla niej i w jej imieniu. Uczelnia odpowiada wówczas za wybór bezpiecznego procesora, za nałożenie na niego odpowiednich obowiązków ochrony danych i za to czy procesor gwarantuje wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie było bezpieczne i zgodne z prawem.
   b) Uczelnia jest procesorem, gdy przetwarza dane dla innego administratora i wówczas sama może podlegać obowiązkom na nią nakładanym przez innego administratora.
3. Powierzenie przetwarzania wymaga zawarcia umowy w formie pisemnej pomiędzy administratorem a podmiotem przetwarzającym (procesorem). Umowa powierzenia powinna zawierać co najmniej elementy wymienione w art. 28 ust. 3 RODO. Umowa taka nie może być zawierana dla pozoru i powinna uwzględniać rozsądne wymagania administratora danych osobowych oraz możliwości Uczelni w tym zakresie (jak np. posiadane zabezpieczenia techniczne i informatyczne, możliwości organizacyjne, potrzebne nakłady finansowe itd.).
4. Dopuszcza się powierzenie danych przez Uczelnię tylko takim procesorom, którzy są w stanie zagwarantować taki poziom bezpieczeństwa i zastosować takie środki organizacyjne i techniczne jakich zastosowania wymaga się od Uczelni. Gwarancje takie powinny być jednym z podstawowych kryteriów uzasadniającym wybór podmiotu, który dla Uczelni ma wykonywać prace czy usługi, wymagające przetwarzania danych

osobowych. Zapewnienia procesora należy w miarę możliwości weryfikować. Jednostka inicjująca zawarcie umowy powierzenia przetwarzania odpowiada za udokumentowanie, że wybrała taki podmiot przetwarzający, który zapewni poziom bezpieczeństwa przetwarzania danych osobowych niezbędny dla ochrony interesów Administratora danych osobowych.

5. Spełnianie przez procesora wymagań stawianych przez Uczelnię należy w uzasadnionych przypadkach (szczególnie w razie wątpliwości co do zapewnień procesora) udokumentować w formie pisemnej przed podpisaniem umowy powierzenia i zachować takie dowody dla celów ewentualnej kontroli. Spełnianie przez procesora wymagań, stawianych przez Uczelnię potwierdzają w szczególności wyniki audytów, certyfikaty oraz inne dokumenty potwierdzające taki poziom przygotowania procesora do przetwarzania danych osobowych, jaki odpowiada oczekiwaniom Uczelni.
6. Jeżeli Uczelnia dalej powierza przetwarzanie danych, które uprzednio już wcześniej powierzono do przetwarzania samej Uczelni, to powierzenie takie musi nałożyć na następnego procesora co najmniej te same obowiązki ochrony danych jak te, które przyjęła uprzednio sama Uczelnia - w szczególności dotyczy to obowiązku wdrożenia środków technicznych i organizacyjnych, niezbędnych do zapewnienia bezpiecznego przetwarzania danych.
7. Kierownicy J/KO, które w ramach przetwarzania danych osobowych przewidują skorzystanie z podwykonawcy (procesora), określają w umowie powierzenia z tym procesorem te same obowiązki ochrony danych, jakie dotyczą Uczelni w tym zakresie. Jeżeli Uczelnia ma być procesorem to umową powierzenia można przyjąć tylko takie obowiązki ochrony danych, które Uczelnia realnie może wykonać. Za wykonywanie obowiązków ochrony danych przyjętych przez Uczelnię w umowie powierzenia odpowiada kierownik J/KO, która to przetwarzanie ma realizować.
8. Przy powierzeniu danych osobowych procesorowi w drodze zawarcia umowy rejestrowanej w Centralnym Rejestrze Umów, należy uzasadnić wybór danego procesora, co zostaje odnotowane w dokumentacji sprawy w CRU. Uzasadnienie wymaga opinii IOD.

§ 9

1. Jeżeli Administrator danych osobowych nie ustali i nie zatwierdzi uprzednio odpowiedniego katalogu podstaw do takiego przekazywania danych, każdą podstawę prawną przekazania danych osobowych do podmiotu znajdującego się w państwie trzecim (poza UE) ustala się wspólnie z IOD. IOD może dodatkowo konsultować się z radcą prawnym Działu Prawnego Uczelni
2. IOD może ustalić wzory zapisów umów w ramach, których dojść ma do transferu danych do państwa trzeciego lub organizacji międzynarodowej.

Rozdział IV - Zabezpieczenia fizyczne i techniczne zastosowane w Uczelni w celu ochrony danych osobowych

§ 10

1. Uczelnia wdraża środki techniczne (w tym informatyczne) i organizacyjne, które pozwalają minimalizować ryzyko związane z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. W celu zapewnienia bezpieczeństwa przetwarzania danych w Uczelni stosuje się między innymi następujące rozwiązania:
   a) w budynkach Uczelni funkcjonują portiernie, z których pobierane są klucze do pomieszczeń. Pobranie i zwrot klucza odnotowywane jest w książce kluczy. Szczegółowe zasady zabezpieczenia mienia oraz wydawania kluczy do pomieszczeń zostały określone w regulacjach wewnętrznych Uczelni.
   b) w Uczelni stosuje się monitoring wizyjny w obrębie obiektów oraz otoczenia. Zakres stosowania oraz techniczne i organizacyjne aspekty monitoringu zostały uregulowane regulacjach wewnętrznych Uczelni.
   c) wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
3. Nadzorowanie i koordynowanie wdrażania i stosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemach teleinformatycznych, należy do Zespołu Bezpieczeństwa Informacji w WCSS. Służą temu w szczególności takie działania jak:
   a) identyfikacja i analiza zagrożenia oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych;
   b) systematyczne określanie potrzeb w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe odpowiednio do stanu wiedzy informatycznej w tym zakresie;
   c) wyznaczanie strategii zabezpieczania systemów informatycznych, określanie procedur bezpieczeństwa i standardów zabezpieczeń;
   d) monitorowanie i zapewnianie ciągłości działania systemu informatycznego oraz baz danych;
   e) cykliczne przeglądy fizycznych zabezpieczeń pomieszczeń serwerowni i węzłów sieci komputerowej;
   f) bieżący nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   g) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych.

4. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych w systemach informatycznych zostają opisane we wdrażanej przez Uczelnię Polityce Bezpieczeństwa Informacji.
5. Kierownicy J/KO określają zabezpieczania techniczne i organizacyjne środki bezpieczeństwa, chroniące dane (przetwarzane w podległych im J/KO), które są następnie uwzględniane w Rejestrze czynności przetwarzania.
6. Dobór środków technicznych i organizacyjnych, dotyczących przetwarzania i zabezpieczania danych osobowych w Uczelni, realizowany jest w oparciu o analizę ryzyka.
7. W przypadku planowania w Uczelni takich procesów przetwarzania danych osobowych, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania obowiązkowo należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (zgodnie z art. 35 RODO).
8. IOD uprawniony jest do wskazania procesów przetwarzania, dla których należy przeprowadzać ocenę skutków.
9. Ocena skutków przetwarzania danych przeprowadzana jest przez Zespół Administratora Danych ds. zgodności z RODO, IOD oraz jednostki/komórki organizacyjnej, nadzorującej merytorycznie obszar, w której czynność przetwarzania danych jest/będzie wykonywana, którzy tworzą Zespół oceniający.
10. Raport z oceny skutków dla danego procesu przetwarzania danych sporządza się w formie pisemnej. Jeżeli dokonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, których Administrator nie może zminimalizować dostępnymi środkami, to przed rozpoczęciem przetwarzania niezbędne będzie przeprowadzenie konsultacji z Prezesem Urzędu Ochrony Danych Osobowych w trybie określonym w ustawie o ochronie danych osobowych.
11. W przypadku konieczności przeprowadzenia konsultacji, o których mowa powyżej, IOD przygotowuje odpowiedni wniosek o konsultacje i wspólnie z odpowiednim Kierownikiem J/KO reprezentują Administratora danych osobowych w tym postępowaniu.

Rozdział V - Prowadzenie Rejestru czynności przetwarzania

§ 11

1. IOD prowadzi Rejestr Czynności Przetwarzania.
2. IOD opierając się na informacjach otrzymywanych od Kierowników J/KO a także samodzielnie identyfikuje wiodące obszary działalności Uczelni, związane z przetwarzaniem danych osobowych w Uczelni, przypisując do nich określone kategorie czynności przetwarzania danych na podstawie zgłoszeń od kierowników J/KO Uczelni.

3. Kierownicy J/KO mają obowiązek na bieżąco informować IOD o procesach przetwarzania danych osobowych, realizowanych w podległych im J/KO (szczególnie o planowanych, nowych czynnościach oraz o istotnych zmianach w zakresie tych czynności). W szczególności należy informować o zmianach w zakresie:
   a) celu przetwarzania danych;
   b) okresu przetwarzania tych danych w ramach realizowanych u nich czynności;
   c) planowanego terminu usunięcia poszczególnych kategorii danych;
   d) kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   e) odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   f) technicznych i organizacyjnych środków stosowanych przy przetwarzaniu.
4. IOD okresowo dokonuje przeglądów procesów przetwarzania danych w celach aktualizacji prowadzonych rejestrów.

Rozdział VI - Postępowanie w sytuacji naruszenia ochrony danych

§ 12

1. Każdej osobie (w tym także osobie spoza Uczelni i osobie, której dane dotyczą) Uczelnia zapewnia możliwość zasygnalizowania dostrzeżonych nieprawidłowości w zakresie przetwarzania danych osobowych. Uczelnia przyjmuje zgłoszenia takich nieprawidłowości, które mogą dotyczyć każdej informacji (nie tylko danych osobowych) i traktuje je jako incydenty bezpieczeństwa informacji. Incydent taki może zostać zakwalifikowany jako Naruszenie Ochrony Danych Osobowych.

2. Jeżeli pracownik Uczelni stwierdza, że w jego ocenie określone zdarzenie lub zaniechanie naraża dane osobowe na niebezpieczeństwo, powinien zgłosić to niezwłocznie w przyjęty przez Administratora danych osobowych sposób (przez wybór odpowiednich pól w formularzu na stronie: **https://zbi.wcss.pl/zglos**). Pracownik informuje o zdarzeniu także swojego przełożonego. Przełożony wyjaśnia z pracownikiem okoliczności zdarzenia i zapewnia utrwalenie informacji o miejscu, czasie i innych okolicznościach zdarzenia. Przełożony może też za pracownika zgłosić to zdarzenie w sposób określony powyżej. Wątpliwości w tym zakresie należy konsultować z IOD.

3. Niezwłoczne zasygnalizowanie nieprawidłowości przez pracownika Uczelni jest podstawą do ograniczenia jego odpowiedzialności, gdyby się okazało, że przyczynił się on do powstania tych nieprawidłowości swoim zachowaniem lub zaniechaniem.

4. Pracownicy Zespołu Bezpieczeństwa Informacji w WCSS udostępniają w systemie OTRS mechanizm, służący do przyjmowania, rejestracji i obsługi zgłoszeń z formularza na stronie, o której mowa w ust. 2 powyżej. Pracownicy ci także wstępnie kwalifikują otrzymane zgłoszenia i przekazują do wyjaśnienia właściwym administratorom, właścicielom danego procesu lub IOD, który w razie potrzeby dokonuje kwalifikacji

zgłoszenia jako Naruszeń Ochrony Danych Osobowych i koordynuje dalsze czynności w tej sprawie.

5. IOD przedstawia w razie potrzeby zalecenia dotyczące dalszego postępowania z tym naruszeniem – w szczególności zgłoszenia przed uprawnionym organem nadzorczym oraz poinformowania osób, których dotyczą dane objęte skutkami naruszenia.

Rozdział VII - Rozliczalność zgodności realizacji obowiązków z RODO

§ 13

1. W celu weryfikacji zastosowanych w Uczelni środków technicznych i organizacyjnych, zapewniających przetwarzanie danych osobowych zgodnie z RODO, wykonuje się ich systematyczne przeglądy.
2. Monitorowanie ochrony danych osobowych prowadzone jest:
   a) na bieżąco przez Kierowników J/KO, w których przetwarzane są dane osobowe/na bieżąco przez osobę zarządzającą Uczelnią;
   b) poprzez sprawdzenia okresowe i doraźne (szczególnie w razie wystąpienia naruszenia ochrony danych), wykonywane przez IOD lub na jego prośbę;
   c) podczas audytów wewnętrznych, przeprowadzanych przez inne upoważnione podmioty i audytorów - po poinformowaniu o nich IOD.
3. IOD okresowo analizuje zgodność dokumentacji przetwarzania danych osobowych, przyjętej w Uczelni z przepisami o ochronie danych osobowych, zgłasza wnioski w zakresie zmian dokumentacji oraz nadzoruje jej aktualizację.

Rozdział VIII - Odpowiedzialność karna za naruszenie zasad ochrony danych

§ 14

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w art. 107 – 108 UODO oraz w art. 130, 266 - 269, 287 Kodeksu karnego.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w pkt 1, naruszenie zasad ochrony danych osobowych może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i może skutkować odpowiedzialnością pracownika na podstawie przepisów prawa pracy.
3. Przy ocenie stopnia zawinienia osoby odpowiedzialnej za naruszenie zasad ochrony danych osobowych bierze się pod uwagę czy osoba ta sygnalizowała zauważone nieprawidłowości i czy uczestniczyła w usuwaniu skutków takiego naruszenia (co prowadzi do ograniczenia odpowiedzialności takiej osoby).

Rozdział IX - Postanowienia końcowe

§ 15

1. Polityka jest dokumentem wewnętrznym i może podlegać udostępnieniu jako informacja publiczna.
2. Kierownicy J/KO odpowiadają za zapoznanie z treścią Polityki swoich pracowników i współpracowników – ze szczególnym uwzględnieniem osób przetwarzających dane osobowe i/lub zabiegających o wydanie im upoważnienia do przetwarzania.

§ 16

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz UODO.
2. Pracownicy (ale również i współpracownicy) Uczelni zobowiązani są do bezpośredniego stosowania zasad określonych w Polityce.