

POLITYKA BEZPIECZEŃSTWA INFORMACJI

I. Podstawa prawna:

- 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) obowiązuje w Polsce od dnia 25 maja 2018 roku.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000).

II. Administratorem, czyli podmiotem przetwarzającym Państwa dane osobowe jest Politechnika Śląska z siedzibą w Gliwicach (44-100), przy ul. Akademickiej 2A, reprezentowana przez Rektora, zwana w dalszej części Uczelnią.

Z Administratorem Państwa danych osobowych w Politechnice Śląskiej można skontaktować się mailowo: iod@polsl.pl lub za pośrednictwem poczty tradycyjnej na adres: Politechnika Śląska 44-100 Gliwice ul. Akademicka 2A.

Administrator danych ustala cele i sposoby przetwarzania danych osobowych, a także zobowiązany jest – uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – wdrożyć odpowiednie środki techniczne i organizacyjne, by przetwarzanie danych osobowych odbywało się zgodnie z RODO.

III. Danymi osobowymi są informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny (PESEL), dane o lokalizacji, identyfikator internetowy (adres IP, adres e-mail, login do portalu internetowego) lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Danymi szczególnej kategorii są takie, które dotyczą: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym; podlegają one szczególnym zasadom przetwarzania i ochrony.

Przetwarzanie danych szczególnej kategorii jest dopuszczalne, jeżeli: osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony; przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora; przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem; przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie; przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą; jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;

przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Przetwarzanie danych osobowych to 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.

IV. Uczelnia przetwarza dane osobowe w obszarach związanych m.in. z: działalnością dydaktyczną, działalnością naukowo-badawczą, zarządzaniem zasobami ludzkimi, działalnością na rzecz studentów (pomoc materialna oraz ubezpieczenia studentów, stypendia naukowe), obsługą finansowo-księgową (rachunkowość, rozrachunki z pracownikami, kontrahentami), innymi obszarami działalności (m.in. biblioteką, działaniami marketingowymi, reklamowymi oraz promocyjnymi, korespondencją przychodząca i wychodząca).

Uczelnia przetwarza dane między innymi w zakresie:

- imion i nazwisk;
- dat urodzenia;
- numeru PESEL;
- numeru albumu;
- serii i numeru dokumentu potwierdzającego tożsamość;
- adresu e-mail;
- numeru telefonu;
- wizerunku;
- obywatelstwa;
- szczególne kategorie danych o: stanie zdrowia, stopniu niepełnosprawności; przynależności do związków zawodowych.

Politechnika Śląska przetwarza dane:

- pracowników Uczelni i ich rodzin,
- kandydatów na określone funkcje,
- studentów, doktorantów, słuchaczy studiów podyplomowych, uczestników kursów dokształcających oraz osób ubiegających się o przyjęcie na studia, studia doktoranckie, studia podyplomowe lub kursy dokształcające;
- osób, które uzyskały stopień naukowy doktora lub doktora habilitowanego;
- cudzoziemców podejmujących i odbywających studia, studia doktoranckie i inne formy kształcenia, a także uczestniczące w badaniach naukowych lub pracach rozwojowych;
- studentów i doktorantów, w tym cudzoziemców ubiegających się o stypendia lub świadczenia z zakresu pomocy materialnej;
- czytelników biblioteki;
- osób biorących udział w postępowaniach konkursowych;
- uczestników badań naukowych;
- uczestników konferencji, projektów, seminariów;
- absolwentów.

Dane osobowe przetwarzane są w celach takich, jak:

- przyjęcia kandydatów na studia;
- przyjęcia kandydatów do pracy;
- realizacji procesu dydaktycznego;
- obsługi czytelników bibliotek;

- zatrudnienia pracownika;
- zawierania umów cywilnoprawnych;
- prowadzenia dokumentacji kadrowej;
- prowadzenia spraw bytowo-socjalnych studentów i pracowników;
- nadzoru nad przestrzeganiem zasad bezpieczeństwa i higieny pracy;
- realizacji projektów badawczych;
- przyznawania stypendiów;
- przydziału miejsc w domach studenckich;
- inicjowania i wspierania różnych form działań wolontariackich;
- działań marketingowych, zarządzania ofertą: edukacyjną, naukową, usługową, działalność promocyjna;
- obsługi i realizacji konkursów/konferencji i in.

V. Dane osobowe przetwarzane są w:

- systemach informatycznych;
- pakietach biurowych;
- systemach pocztowych;
- zbiorach tradycyjnych (papierowych).

VI. Podstawy do legalnego przetwarzania danych osobowych określa art. 6 rozporządzenia RODO. Przetwarzanie jest dopuszczalne, gdy:

1. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie jej danych osobowych. Zgoda na przetwarzanie danych osobowych to jedna z przesłanek legalności przetwarzania danych osobowych, rozumiana jako okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalającego na przetwarzanie dotyczących jej danych osobowych. Zgoda na przetwarzanie danych osobowych musi być: dobrowolna, konkretna, świadoma i jednoznaczna. Zgoda na przetwarzanie danych osobowych może przyjąć formę oświadczenia woli, wyrażonego w formie pisemnej lub elektronicznej, np. klauzula zgody dołączona do kwestionariusza osobowego w formie papierowej lub umieszczenie klauzuli zgody w formularzu elektronicznym przy zastosowaniu checkboxa. Zgoda na przetwarzanie danych osobowych musi być wyrażona na jasno określony cel np. zgoda na przetwarzanie danych osobowych w procesie rekrutacji do pracy czy udziału w konkursie, konferencji itp. Na Politechnice Śląskiej na podstawie zgody przetwarzane są m.in. dane następujących kategorii osób: kandydatów do pracy; absolwentów; uczestników badań/projektów; uczestników konferencji/szkoleń/seminariów. Jeżeli dane osobowe przetwarzane są na podstawie zgody, osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody ma być równie proste do realizacji jak jej wyrażenie;

2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze – podstawą prawną są min. przepisy: ustawy Prawo o szkolnictwie wyższym i rozporządzeń wykonawczych do ww. ustawy, ustawy Kodeks pracy, ustawy o bibliotekach, ustawy o narodowym zasobie archiwalnym i archiwach.

4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

VII. Udostępnianie danych osobowych to jedna z form operacji wykonywanych na danych osobowych w ramach przetwarzania tych danych. Uczelnia, administrując danymi, może udostępniać je osobom lub podmiotom uprawnionym do ich otrzymania na podstawie przepisów prawa (organy administracji państwowej, wymiaru sprawiedliwości) lub innym podmiotom w przypadku posiadania przez te podmioty podstaw prawnych do legalnego przetwarzania danych. Politechnika Śląska udostępnia dane osobowe m.in.: zgodnie z ustawą Prawo o szkolnictwie wyższym Ministerstwu Nauki i Szkolnictwa Wyższego; ZUS i KRUS w celu potwierdzenia statusu studenta; potencjalnym pracodawcom na podstawie zgody absolwenta.

VIII. Powierzenie przetwarzania danych osobowych zachodzi wtedy, gdy Uczelnia, administrując danymi, korzysta z usług podmiotów zewnętrznych zwanych procesorami, w zakresie realizacji zadań związanych z przetwarzaniem danych osobowych. Powierzenie przetwarzania danych odbywa się na podstawie umowy lub innych instrumentów prawnych. Umowa powierzenia musi określać cele i kategorie powierzanych danych osobowych. Retencja danych osobowych odbywa się co do zasady przez okres obowiązywania umowy. Umowa powierzenia może mieć postać samodzielnej umowy bądź dodatkowych postanowień do umów o świadczenie usług. Treść umowy powierzenia należy konsultować z Inspektorem Ochrony Danych.

IX. Obowiązek informacyjny to obowiązek Administratora do poinformowania osoby, której dane dotyczą o:

- danych identyfikujących Administratora;
- danych kontaktowych Inspektora Ochrony Danych;
- przysługujących jej prawach;
- celu przetwarzania danych osobowych;
- okresie przechowywania danych osobowych;
- podstawie przetwarzania danych osobowych;
- możliwości złożenia skargi do organu nadzorczego.

Obowiązek informacyjny ma na celu uświadomić osobę, której dane dotyczą, o tym na co się godzi, wyrażając zgodę na przetwarzanie swoich danych osobowych lub gdy przetwarzanie danych odbywa się na podstawie innych przesłanek o przysługujących osobie, której dane dotyczą, prawach. Obowiązek ten jest realizowany najczęściej w postaci klauzul informacyjnych. Obowiązek informacyjny należy spełnić niezależnie od podstawy przetwarzania danych osobowych. Obowiązek informacyjny należy spełnić podczas pozyskiwania danych od osoby, której dane dotyczą, np.: w procesie rekrutacji na studia/do pracy, zapisu uczestników na organizowane wydarzenie, w procesie dotyczącym prowadzenia badań naukowych. Najbezpieczniejszym rozwiązaniem jest umieszczanie klauzul informacyjnych tam, gdzie przetwarzamy dane osobowe.

X. Rozporządzenie RODO wprowadziło zasadę ograniczenia czasowego przechowywania danych osobowych, tzn. że dane nie powinny być przechowywane w nieskończoność. Jeżeli podstawę przetwarzania danych osobowych stanowi zgoda osoby, której dane dotyczą, wówczas dane osobowe mogą być przetwarzane do czasu odwołania zgody. Po odwołaniu zgody, dane mogą być przetwarzane przez okres odpowiadający ew. terminowi przedawnienia roszczeń, jakie może ponosić administrator danych. Jeżeli dane przetwarzane są na podstawie

umowy, wówczas mogą być przetwarzane tak długo, jak jest to niezbędne do wykonania umowy, a po tym czasie przez okres odpowiadający okresowi przedawnienia roszczeń. Jeżeli przepisy określają termin, przez jaki powinny być przechowywane dane osobowe, to należy przechowywać je przez czas wskazany w konkretnym przepisie.

XI. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Przykłady naruszeń:

- zagrożenia w obszarze zasobów ludzkich (ujawnianie danych osobom nieuprawnionym);
- zjawiska naturalne (zjawiska klimatyczne, sejsmiczne, pogodowe);
- utrata podstawowych usług;
- zniszczenia fizyczne (pożar, zalanie, wypadek, zniszczenie urządzeń lub nośników);
- awarie techniczne;
- nieautoryzowane zmiany, nielegalne wykorzystywanie lub nadużywanie zasobów IT;
- infekcja systemu przez szkodliwe oprogramowanie;
- ataki hakerskie;
- fałszywe wiadomości e-mail;
- naruszenia podstaw przetwarzania danych osobowych;
- włamania, wtargnięcia lub inne nieuprawnione wejście na teren Uczelni.

W przypadku podejrzenia/stwierdzenia naruszenia ochrony danych osobowych należy zaprzestać przetwarzanie danych osobowych, poinformować bezpośredniego przełożonego oraz IOD o możliwym naruszeniu ochrony danych osobowych. W zgłoszeniu podejrzenia/stwierdzenia naruszenia należy wskazać:

- datę zdarzenia,
- opis zaistniałego incydentu,
- miejsce wystąpienia incydentu,
- wskazać przyczynę lub potencjalną przyczynę wystąpienia naruszenia,
- ustalić możliwe skutki wynikające z naruszenia,
- opisać dotychczasowe działania w związku z incydemem,
- opisać znane danej osobie sposoby zabezpieczenia danych osobowych.

XII. Na Politechnice Śląskiej stosuje się m.in.:

Zabezpieczenia organizacyjne:

- wyznaczenie inspektora ochrony danych;
- opracowanie i wdrożenie dokumentacji ochrony danych osobowych;
- do przetwarzania danych osobowych dopuszczone zostały osoby do tego upoważnione;
- prowadzenie ewidencji osób upoważnionych;
- przeszkolenie i zaznajomienie pracowników z przepisami ochrony danych osobowych;
- procedura wydawania kluczy do pomieszczeń osobom uprawnionym;
- portiernie monitorujące osoby wchodzące i wychodzące z budynków;
- osoby trzecie w obszarze przetwarzania danych osobowych przebywają w obecności osób upoważnionych;
- osoby upoważnione zobowiązane są do zachowania danych osobowych i sposobów zabezpieczeń w tajemnicy.

Środki ochrony fizycznej:

- drzwi zamykane na klucz;
- drzwi o podwyższonej odporności na włamanie;

- okna zabezpieczone za pomocą krat/rolet;
- systemy alarmowe;
- systemy monitoringu wizyjnego;
- systemy przeciwpożarowe;
- szafy niemetalowe/metalowe zamykane na klucz;
- sejfy, kasy pancerne;
- niszcarki dokumentów.

Środki ochrony w ramach narzędzi programowych:

- rejestracja zmian w systemach;
- określenie praw dostępu do danych;
- identyfikatory użytkowników oraz hasła;
- token.