



Politechnika
Wroclawska

REKTOR

ZARZĄDZENIE WEWNĘTRZNE 55/2020

z dnia 6 lipca 2020 r.

w sprawie organizacji przetwarzania danych osobowych w Politechnice Wrocławskiej
i dokumentacji związanej z tym przetwarzaniem

Na podstawie art. 23 ust. 2 ustawy z dnia z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2020 r., poz. 85 z późn.zm.), w związku z art. 2 oraz art. 3, a także art. 24 ust. 1 i 2 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 Nr 119, str. 1), zwanego dalej RODO, a także w związku z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781), zarządza się, co następuje:

§ 1

1. Rektor odpowiada za przetwarzanie i ochronę danych osobowych w Uczelni, zgodnie z przepisami prawa. Rektor określa i ustanawia szczegółowe zasady przetwarzania danych osobowych obowiązujące w Uczelni.
2. Obowiązki Administratora danych osobowych (którym jest Politechnika Wroclawska) wykonuje właściwy Prorektor wyznaczony przez Rektora.
3. Administrator danych osobowych:
 - 1) określa środki techniczne, informatyczne i organizacyjne, zapewniające ochronę danych odpowiednią do zidentyfikowanych przez administratora zagrożeń;
 - 2) nadzoruje wdrażanie określonych środków w „*Dokumentacji przetwarzania danych osobowych w Politechnice Wrocławskiej*”, zwanej dalej *Dokumentacją*;
 - 3) może wyznaczać zadania określonym osobom oraz stosownie do potrzeb powoływać je do pełnienia funkcji - w szczególności: lokalnych administratorów danych osobowych, administratorów systemów informatycznych.
 - 4) Administratora danych osobowych w Uczelni w realizacji jego zadań wspierają wszyscy pracownicy Uczelni, a w szczególności osoby kierujące działalnością Uczelni w danym obszarze bądź kierujące komórkami/jednostkami organizacyjnymi Uczelni.

§ 2

1. Administrator danych osobowych w Uczelni określa i aktualizuje *Dokumentację*, która jest cyklicznie przeglądana i podlega aktualizacji stosownie do potrzeb w celu zapewnienia jej zgodności wymogom prawa i identyfikowanym na bieżąco zagrożeniom.
2. W skład *Dokumentacji* wchodzi niniejsze Zarządzenie Wewnętrzne, określające sposób organizacji i zakres zadań związanych z przetwarzaniem danych osobowych oraz *Polityka Ochrony Danych Osobowych*. Administrator danych osobowych- stosownie do potrzeb - uzupełnia *Dokumentację* o inne dokumenty, które udostępnia się niezwłocznie po ich określeniu przy pomocy narzędzi komunikacji Uczelni. *Dokumentacja* zawierać może w szczególności następujące elementy:

- 1) wyciągi i regulaminy dotyczące szczegółowych zasad postępowania z danymi osobowymi;
 - 2) instrukcje szczegółowe (w tym instrukcje zarządzania poszczególnymi systemami informatycznymi);
 - 3) rejestry, wykazy i ewidencje;
 - 4) formularze i wzory upoważnień lub oświadczeń;
 - 5) zalecenia i rekomendacje sporządzone przez Administratora danych osobowych w Uczelni lub przez Inspektora Ochrony Danych;
 - 6) przyjęte do stosowania zbiory „dobrych praktyk” dotyczące przetwarzania danych oraz procedury;
 - 7) wzory umów lub wzory klauzul dotyczących przetwarzania, powierzania i ochrony danych osobowych.
3. Z uwagi na potrzebę zachowania bezpieczeństwa danych osobowych *Dokumentacja* nie stanowi informacji publicznej udostępnianej na wniosek. Administrator danych osobowych może jednak wskazać elementy *Dokumentacji* mające charakter jawny i mogące zostać ujawnione.

§ 3

1. Administrator danych osobowych wyznaczył Inspektora Ochrony Danych (IOD), do którego należą zadania wynikające z powszechnie obowiązujących przepisów prawa i inne zadania w obszarze ochrony danych osobowych powierzone mu zgodnie z tymi przepisami, a w szczególności:
 - 1) identyfikowanie procesów przetwarzania danych przez Administratora danych osobowych i sprawdzanie ich zgodności z prawem;
 - 2) informowanie Administratora danych i osób przetwarzających dane osobowe o obowiązkach spoczywających na nich z mocy prawa unijnego i krajowego – w tym poprzez redagowanie strony www poświęconej tym zagadnieniom;
 - 3) doradzanie w sprawach związanych z ochroną danych osobowych – m.in. na etapie projektowania rozwiązań organizacyjnych i technicznych związanych z przetwarzaniem danych osobowych w sporządzaniu umów powierzenia przetwarzania danych osobowych, klauzul informacyjnych i klauzul zgody itp.;
 - 4) rekomendowanie działań, mających zapewnić zgodność przetwarzania danych z przepisami prawa;
 - 5) uczestniczenie w informowaniu osób, których dane dotyczą w razie potrzeby zawiadomienia ich o naruszeniu ochrony ich danych osobowych;
 - 6) współdziałanie w ocenie skutków dla ochrony danych oraz wspieranie Administratora danych osobowych poprzez konsultowanie takich kwestii jak:
 - a) zasadność przeprowadzenia oceny skutków dla ochrony danych,
 - b) metodyka oceny skutków dla ochrony danych,
 - c) potrzeba oceny skutków dla ochrony danych przez podmiot zewnętrzny,
 - d) środki stosowane w celu ograniczenia skutków naruszenia praw i interesów osób, których dane dotyczą,
 - 7) oceny prawidłowości przeprowadzonej oceny ryzyka prowadzenie Rejestru Czynności Przetwarzania i Rejestru Kategorii Przetwarzania oraz nadzór nad Rejestrem Naruszeń Ochrony Danych Osobowych, zgodnie z regulacjami wewnętrznymi Administratora danych osobowych,
 - 8) udział w analizie ryzyka przetwarzania danych osobowych z uwzględnieniem charakteru, zakresu i celów przetwarzania;
 - 9) zgłaszanie przypadków naruszeń ochrony danych osobowych do PUODO i gromadzenie potrzebnej do tego celu dokumentacji naruszeń ochrony danych osobowych (dotyczącej okoliczności, skutków i podjętych działań zaradczych);

- 10) pełnienie funkcji punktu kontaktowego dla osób, których dane są przetwarzane na Politechnice Wrocławskiej oraz dla PUODO;
 - 11) szkolenia pracowników z zakresu ochrony danych osobowych oraz zapoznanie osób przetwarzających dane z dokumentacją obowiązującą na Politechnice Wrocławskiej.
2. Kierownicy J/KO są odpowiedzialni za zarządzanie procesami przetwarzania danych osobowych w swoich jednostkach/komórkach. Do szczególnych obowiązków kierowników J/KO należy:
- 1) zapewnienie, aby podlegli pracownicy, którzy przetwarzają dane osobowe, zostali upoważnieni do przetwarzania danych osobowych w zakresie wymaganym ze względu na te czynności, jakie wykonują z danymi;
 - 2) bieżące nadzorowanie przebiegu czynności przetwarzania w swojej jednostce/komórce;
 - 3) zgłaszanie IOD:
 - a) zmian dotyczących czynności przetwarzania danych osobowych, które wymagają aktualizacji danych zawartych w *Rejestrze czynności przetwarzania*,
 - b) informacji o planowanych do wdrożenia nowych systemach/aplikacjach informatycznych, bądź planowanych zmianach funkcjonalności w istniejących systemach/aplikacjach informatycznych, jeżeli będą w nich przetwarzane dane osobowe;
 - 4) zgłaszanie każdej zauważonej nieprawidłowości przy przetwarzaniu danych osobowych oraz współpracowanie przy wyjaśnianiu okoliczności wystąpienia takich zdarzeń zgodnie z procedurą ustaloną przez administratora danych osobowych;
 - 5) zapoznanie podległych pracowników (i innych osób - np. współpracowników) z zasadami przetwarzania i ochrony danych w danej J/KO;
 - 6) występowanie do dyrektora Działu Informatyzacji (lub wyznaczonych przez niego odpowiednich administratorów) o nadanie, zmianę lub cofnięcie uprawnień odpowiednich do zakresu upoważnienia pracownika (w systemie informatycznym);
 - 7) określanie i konsultowanie z radcami prawnymi uczelni oraz IOD podstaw prawnych (tzw. „przesłanek”) przetwarzania danych osobowych i przygotowania właściwej klauzuli informacyjnej;
 - 8) stosowanie się do zaleceń zewnętrznego administratora danych osobowych, w przypadku, gdy ten administrator powierza uczelni przetwarzanie danych na podstawie umowy powierzenia.
3. Dyrektor Działu Spraw Osobowych odpowiada za:
- 1) włączenie do akt osobowych nadanych upoważnień do przetwarzania danych osobowych oraz oświadczeń o zachowaniu tajemnicy danych osobowych i sposobów ich zabezpieczania wraz z aktami osobowymi pracowników (oraz odpowiednio - z umowami zlecenia/cywilnoprawnymi);
 - 2) udostępnianie w wymagających tego przypadkach danych osobowych pracowników we właściwym i tylko minimalnym zakresie oraz tylko uprawnionym odbiorcom, zgodnie z procedurą ustaloną przez administratora danych osobowych.
4. Kierownik Jednostki zarządzającej systemami informatycznymi :
- 1) jest odpowiedzialny za zapewnienie systemom i narzędziom informatycznym wykorzystywanym do przetwarzania danych osobowych w Uczelni:
 - a) opieki technicznej,
 - b) wsparcia i administrowania przy wykorzystaniu środków organizacyjnych, technicznych i informatycznych niezbędnych dla zapewnienia bezpieczeństwa danych,
 - c) ciągłości ich przetwarzania na poziomie odpowiadającym potrzebom Uczelni,
 - d) zgodności tych systemów i narzędzi z wymogami prawa.

- 2) współpracuje w innymi jednostkami w zakresie zapewnienia i monitorowania bezpieczeństwa systemów informatycznych przetwarzających dane osobowe;
- 3) współpracuje z Zespołem Administratora Danych ds. zgodności z RODO w zakresie opracowania i wdrażania ogólnouczelnianych zasad i standardów bezpiecznego przetwarzania danych osobowych przy pomocy środków informatyki – w tym urządzeń, aplikacji i struktury sieciowej.

§ 4

Tracą moc:

- 1) Zarządzenie Wewnętrzne 35/2017 z dnia 30 marca 2017 roku w sprawie organizacji przetwarzania danych osobowych w Politechnice Wrocławskiej i dokumentacji związanej z tym przetwarzaniem;
- 2) Pismo Okólne 8/2007 z dnia 23 kwietnia 2007 roku w sprawie wprowadzenia w Politechnice Wrocławskiej sposobu prowadzenia dokumentacji dotyczącej przetwarzania danych osobowych oraz instrukcji dotyczącej trybu zapoznawania się osób fizycznych z ich danymi osobowymi;
- 3) Pismo Okólne 21/2015 w sprawie Rejestru zbiorów danych i obowiązku aktualizacji danych o zbiorach danych osobowych przetwarzanych w Uczelni.

§ 5

Zarządzenie niniejsze wchodzi w życie z dniem ogłoszenia.

Prof. dr hab. inż. Cezary Madryas