Zarządzenie Nr 7/2018
Rektora Politechniki Łódzkiej
z dnia 24 maja 2018 roku

w sprawie wdrożenia dokumentacji ochrony danych osobowych
w Politechnice Łódzkiej

Na podstawie art. 66 ust.1 i 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (j.t. Dz. U. z 2017 r. poz. 2183 ze zm.) oraz § 15 ust. 1, 2 i 3 Statutu Politechniki Łódzkiej, art. 24 ust. 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 (ogólnego rozporządzenia o ochronie danych), Dz.U.UE.L.2016.119.1 zarządzam, co następuje:

§ 1

Spełniając obowiązki wynikające z przepisów prawa wprowadzam do użytku służbowego:
1. Politykę ochrony danych osobowych w Politechnice Łódzkiej stanowiącą załącznik nr 1 do Zarządzenia
2. Wytyczne – standardy ochrony danych osobowych w Politechnice Łódzkiej stanowiące załącznik nr 2 do Zarządzenia.

§ 2

1. Uprawnienia do nadawania upoważnień do przetwarzania danych osobowych posiadają:
   1) właściwy Prorektor - pracownikom jednostek mu podległych i nadzorowanych;
   2) kierownicy jednostek administracji podstawowej - podległym im pracownikom, w tym pracownikom tych jednostek;
   3) Dyrektor Biura Rektora - pracownikom bezpośrednio podległym Rektorowi i pracownikom Biura;
   4) Kanclerz - pracownikom jednostek administracji kanclerskiej;
   5) Kwestor zastępca kanclerza- pracownikom podległych jednostek;
   6) kierownik Działu Projektów - osobom zatrudnionym w projektach, w tym studentom uczestniczącym w projektach.
2. Upoważnienia do przetwarzania danych osobowych prowadzone są wyłącznie w formie elektronicznej, stanowiącej dokumentację podstawową.
3. Nadane dotychczas upoważnienia zachowują swą ważność do czasu koniecznej ich aktualizacji.
4. Inspektor Ochrony Danych prowadzi centralną ewidencję osób upoważnionych do przetwarzania danych osobowych.

§ 3

Dokumentacja, o której mowa w §1 jest dostępna w wersji nieedytowalnej i ograniczona tylko do pracowników Politechniki Łódzkiej po zalogowaniu się przez nich do dedykowanego systemu informatycznego, w którym jest ona zamieszczona.

§ 4

Nadzór nad realizacją postanowień wynikających z dokumentów, o których mowa w §1 oraz aktualizowanie ich treści powierzam Inspektorowi Ochrony Danych.

§ 5

Traci moc Zarządzenie Nr 09/2017 Rektora Politechniki Łódzkiej z dnia 30 maja 2017 roku w sprawie wdrożenia dokumentacji opisującej sposób przetwarzania danych osobowych w Politechnice Łódzkiej.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 25 maja 2018 r.

Rektor
Politechniki Łódzkiej
Prof. dr hab. inż. Sławomir Wiak

Załącznik nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Polityka ochrony danych osobowych w Politechnice Łódzkiej

Rozdział 1
Postanowienia ogólne
§ 1

Celem Polityki ochrony danych osobowych, zwanej dalej „Polityką" w Politechnice Łódzkiej, zwanej dalej PŁ, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka została opracowana w oparciu o wymagania zawarte w:

- rozporządzeniu 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 (ogólnego rozporządzenia o ochronie danych), Dz.U.UE.L.2016.119.1 (dalej RODO)
- ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 100)
- ustawie z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (tj. Dz.U. z 2017 poz. 2183 z późn zm.

oraz wymaganiom zawartym w normach z zakresu:

- ochrony danych identyfikujących osobę z serii ISO/IEC 29100;
- zarządzania bezpieczeństwem informacji z serii ISO/IEC 27000;
- zarządzania ryzykiem z serii ISO/IEC 31000.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, techniczne oraz poprzez użytkowników proporcjonalnie i adekwatnie do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności w PŁ.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w PŁ rozumiane jest jako zapewnienie ich poufności, integralności, prawidłowości, przejrzystości, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

    1) **poufność danych** – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
    2) **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
    3) **rozliczalność danych** – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
    4) **integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
    5) **dostępność informacji** – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

6) **zarządzanie ryzykiem** – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

1. Administratorem danych osobowych jest Politechnika Łódzka, a w jej imieniu Jego Magnificencja Rektor.
2. Administrator danych osobowych powołał Inspektora Ochrony Danych (dalej IOD). Dane kontaktowe IOD publikowane są na stronie Uczelni w sposób umożliwiający bezpośredni kontakt interesariuszy wewnętrznych i zewnętrznych w kwestiach związanych z przetwarzaniem danych osobowych.
3. IOD jest zobowiązany do zachowania w tajemnicy informacji uzyskiwanych podczas wykonywania swoich zadań.
4. IOD podlega bezpośrednio Rektorowi.
5. Rektor zapewnia wsparcie dla IOD w wykonywaniu zadań zapewniając mu zasoby niezbędne do wykonywania zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
6. IOD , w miarę możliwości, jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych oraz zapewnia wsparcie dla wszystkich osób, których dotyczy obowiązek przetwarzania danych osobowych.

Rozdział 2
Definicje

§ 6

1. Przez użyte w Polityce określenia należy rozumieć:

1) **administrator danych osobowych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – tu: Politechnika Łódzka;
2) **inspektor ochrony danych** – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych - pracownik Politechniki Łódzkiej wskazany przez jej Rektora oraz zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych;
3) **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
4) **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);
5) **PUODO**- Prezes Urzędu Ochrony Danych Osobowych;
6) **dane osobowe** –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;
7) **przetwarzane danych** – operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany;
8) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
9) **NND**- system informatyczny nadzoru nad dokumentami
10) **administrator systemu informatycznego** – osoba lub osoby, odpowiedzialne za administrowanie systemami informatycznymi;
11) **kierownik jednostki** – rozumiany jako Rektor, Prorektor, Kanclerz, Dziekan, Kierownik Katedry lub Dyrektor Instytutu oraz kierownik w ogólnouczelnianych, międzywydziałowych i pozawydziałowych jednostkach PŁ.

Rozdział 3
Zakres stosowania
§ 7

1. W PŁ przetwarzane są dane osobowe:

    1) kandydatów do pracy, dane osób zatrudnionych na umowę o pracę, dane osób - stron umów cywilnoprawnych, dla których celem przetwarzania jest w szczególności wykonywanie zadań odnoszących się do zatrudniania pracowników i innych osób oraz prowadzenie i przechowywanie akt osobowych pracowników . Dane tego zasobu osobowego są przetwarzane na podstawie obowiązku prawnego wynikającego z przepisu art. 22 Kodeksu Pracy ciążącego na PŁ jako pracodawcy lub podpisanej umowy cywilnoprawnej.
    2) kandydatów na studia, studentów, słuchaczy studiów podyplomowych, uczestników konferencji, szkoleń i kursów, które wchodzą w skład jednego ogólnouczelnianego zasobu „studentów i absolwentów" jako osób uczących się w PŁ. Przetwarzanie danych osobowych osób uczących się odbywa się w celach związanych z rekrutacją na studia, a następnie kształceniem w różnych formach, w szczególności w celu realizacji zadań uczelni wskazanych w prawie właściwym dla szkolnictwa wyższego i nauki oraz w innych ustawach szczegółowych związanych z odbywaniem studiów wyższych oraz w rozporządzeniach wykonawczych do tych ustaw;
    3) osób zewnętrznych (nie zatrudnionych) związane z realizacją usług w ramach procesów biznesowych lub organizacyjnych, np. kontrahenci, klienci, podwykonawcy, przedsiębiorcy. Przetwarzane są one w oparciu o umowę wiążącą Strony;
    4) zasoby danych osobowych zebrane w bazach:
        - osób niepełnosprawnych;
        - użytkowników biblioteki głównej i wydziałowych;
        - osób korzystających z miejsc zakwaterowania w osiedlu akademickim i ośrodkach wypoczynkowych;
        - beneficjentów stypendiów oraz osób korzystających z Zakładowego Funduszu Świadczeń Socjalnych;
        - osób fizycznych, których dane są przedmiotem badań naukowych;
        - uczestników projektów i programów realizowanych ze środków unijnych i krajowych;
        - monitoringu wizyjnego wykorzystywanego w celu zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę;
        - innych osób, jeśli wynika to z zadań i jest prawnie dopuszczalne.

2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej. Dane agregowane są w:
    - informatycznych bazach danych, dedykowanych systemach;
    - rejestrach znajdujących się w plikach (Excel, Word, PDF), które są zapisywane na dyskach lokalnych i sieciowych lub na zewnętrznych nośnikach elektronicznych;
    - archiwach papierowych - dedykowane ewidencje uporządkowane pod względem dostępności danych, w tym w archiwum;
    - dane znajdujące się w dokumentach papierowych – listy imienne z danymi osobowymi, zestawy nieuporządkowane pod względem dostępności danych, znajdujące się w pomieszczeniach różnych jednostek organizacyjnych.

3. Polityka zawiera uregulowania dotyczące wprowadzonych zabezpieczeń organizacyjnych, technicznych i fizycznych zapewniających ochronę przetwarzanych danych osobowych.
4. W PŁ prowadzone są czynności przetwarzania danych osobowych, w szczególności:
    - zbieranie różnymi kanałami oraz wprowadzanie i utrwalanie w systemie informatycznym; ewidencji lub kartotece papierowej,
    - organizowanie, zestawianie i agregowanie oraz porządkowanie, adaptowanie lub modyfikowanie;
    - pobieranie i przeglądanie;

- ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, w tym w obiegu wewnętrznym;
- wykorzystywanie poprzez dopasowywanie lub łączenie;
- wykonywanie kopii zapasowych;
- ograniczanie, usuwanie lub niszczenie;
- przechowywanie i archiwizowanie;
- realizacja żądań i wniosków o udostepnienie danych osobowych;
- powierzanie danych do przetwarzania na zlecenie podmiotom przetwarzającym;
- udzielanie informacji na wniosek osób dotyczący przetwarzania ich danych, uwzględnienie składanych sprzeciwów wobec przetwarzania danych, informowanie o naruszeniach bezpieczeństwa;
- obsługa wniosków dotyczących realizacji praw osób, których dane dotyczą.

5. IOD z pełnomocnictwa Rektora prowadzi **rejestr czynności przetwarzania danych osobowych**.

§ 8

1. Zakresy ochrony danych osobowych określone przez Politykę oraz inne z nią związane dokumenty mają zastosowanie do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
   3) wszystkich pracowników, studentów i innych osób mających dostęp do informacji podlegających ochronie.

Rozdział 4
Obowiązki i kompetencje w zakresie ochrony danych osobowych kierownictwa i osób dopuszczonych do przetwarzania danych

§ 9

1. Administrator danych osobowych jest zobowiązany do:
   1) wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z obowiązującymi aktami prawnymi. Jeśli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez PŁ polityki ochrony danych;
   2) przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania wdraża takie środki, jak np. pseudonimizacja, jako procesu odwracalnego, co oznacza, że dane zaszyfrowane można odczytać za pomocą odpowiedniego klucza;
   3) chroni prawa osób, których dane dotyczą przez wdrożenie niezbędnych zabezpieczeń w formie środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by dane osobowe nie były domyślnie udostępniane nieokreślonej liczbie osób fizycznych bez interwencji danej osoby;
   4) dokonując oceny bezpieczeństwa uwzględnia w szczególności ryzyko wiążące się 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 w PŁ;
   5) zapewnia, by każda osoba fizyczna, działająca z upoważnienia administratora, która ma dostęp do danych osobowych przetwarzała je wyłącznie na polecenie administratora, co oznacza, że posiada upoważnienie do przetwarzania danych osobowych.

§ 10

1. Uprawnienia do nadawania upoważnień do przetwarzania danych osobowych posiadają:

   1) właściwy Prorektor - pracownikom jednostek mu podległych i nadzorowanych;

2) kierownicy jednostek administracji podstawowej - podległym im pracownikom, w tym pracownikom tych jednostek;
3) Dyrektor Biura Rektora - pracownikom bezpośrednio podległym Rektorowi i pracownikom Biura;
4) Kanclerz - pracownikom jednostek administracji kanclerskiej;
5) Kwestor zastępca kanclerza- pracownikom podległych jednostek;
6) Kierownik biura projektów - osobom zatrudnionym w projektach, w tym studentom uczestniczącym w projektach.

2. Uprawnione powyżej osoby nadają upoważnienia, dokonują zmian lub odwołują je we współpracy z IOD, który doradza w tym zakresie i weryfikuje zasadność podjętych decyzji o nadanie upoważnienia.
3. Osoby upoważnione do przetwarzania danych osobowych przetwarzają je wyłącznie na polecenie Rektora. Upoważnienie daje formalną możliwość dostępu do danych osobowych zgodnego z zakresem służbowych obowiązków i poprzedza nadanie uprawnień użytkownikowi systemu informatycznego.
4. Upoważnienia nadawane są w formie dokumentu elektronicznego w systemie NND, który to system potwierdza zapoznanie się osoby z treścią upoważnienia oraz podpisanie oświadczenia o zachowaniu danych w tajemnicy.
5. Procedura elektronicznego nadawania i odwoływania upoważnień dostępna jest w **NND** – załącznik nr 1.
6. Treść upoważnienia zawiera wzór dostępny w załączniku zamieszczonym w **NND**.

Rozdział 5
Zadania Inspektora Ochrony Danych
§ 11

1. Do najważniejszych obowiązków Inspektora Ochrony Danych należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych, w tym informowanie Rektora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów prawa europejskiego lub ustawy o ochronie danych oraz zapewnienie odpowiedniego wsparcia;
2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki i innymi dokumentami wewnętrznymi;
3) monitorowanie przestrzegania przepisów o ochronie danych oraz Polityki, w tym podziału obowiązków przy przetwarzaniu danych, podejmowanie działań zwiększających świadomość, organizowanie i prowadzenie szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
4) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania zaleceń;
5) współpraca z organem nadzorczym (PUODO);
6) zgłaszanie naruszenia ochrony danych do PUODO i zawiadamianie osoby o naruszeniu oraz prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
7) prowadzenie centralnej ewidencji osób upoważnionych do przetwarzania danych osobowych;
8) opracowywanie zapisów do klauzul zgód i informacyjnych;
9) sprawdzanie (audyty) działań jednostek pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
10) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
11) obsługa wniosków o realizację praw osób, których dane dotyczą.

Rozdział 6
Zadania administratora systemu informatycznego
§ 12

1. Funkcja Administratora Systemu Informatycznego (ASI) powierzana jest przez kierownika jednostki najczęściej informatykowi, którego zadaniem jest nadzór nad zgodnym z prawem funkcjonowaniem systemu informatycznego, w ramach którego przetwarzane są dane osobowe.

2. Wśród zadań przypisanych do pełnienia funkcji ASI można wymienić: administrowanie serwerami i innymi urządzeniami służącymi do przetwarzania danych osobowych, konfigurowanie kont użytkowników i realizowanie wniosków o nadawanie im uprawnień, czy też nadzór nad wykonywaniem kopii zapasowych.
3. Szczegółowe zadania ASI oraz zakres odpowiedzialności określa kierownik jednostki, który wyznaczył go do pełnienia tej funkcji.

Rozdział 7
Obowiązki osób zarządzających procesami w zakresie przetwarzania danych osobowych
§ 13

1. Rektor wyznacza zarządzających – właścicieli procesów przetwarzania danych osobowych odpowiedzialnych za realizację celów procesu oraz monitorowanie jego aktualności i zgodności z prawem. Opis treści i wizualizacja czynności w procesie dostępna jest w **NND**:
   1) przetwarzanie danych osobowych osób uczących się – **Prorektor ds. Studenckich**- załączniki od 2 do 8;
   2) przetwarzanie danych osobowych pracowniczych - Kierownik Działu Osobowego- załączniki od 9 do 29;
   3) proces nadawania upoważnień do przetwarzania danych osobowych oraz uprawnień w systemach informatycznych – **IOD** jako monitorujący zgodność z przepisami;
   4) proces testowania, mierzenia i oceny skuteczności środków technicznych mających zapewnić bezpieczeństwo przetwarzania;
   5) proces uwierzytelniania oraz zasady związane z ich zarządzaniem i użytkowaniem, stosowane metody i środki- załącznik 30;
   6) proces rozpoczynania, zawieszania i kończenia pracy użytkowników systemu informatycznego, w którym przetwarzane są dane osobowe- załącznik 31;
   7) proces tworzenia i przechowywania kopii zapasowych oprogramowania i plików zawierających dane osobowe- załącznik 32;
   8) proces obsługi wniosków osoby, której dane dotyczą w sprawie realizacji przysługujących praw w RODO – **IOD**- załącznik 33;
   9) proces przetwarzania danych osobowych przedsiębiorców, kontrahentów, klientów, przedstawicieli przemysłu- **Kwestor**;
   10) proces przetwarzania danych dotyczących naliczania i wypłaty wynagrodzeń, stypendiów i staży- **Kwestor**;
   11) proces przetwarzania danych finansowo księgowych – **Kwestor**- załącznik 34;
   12) proces monitorowania zgodności przetwarzania z przepisami RODO, sprawdzenia i opracowanie sprawozdania – **IOD**- załącznik 35;
   13) proces reagowania na incydenty godzące w bezpieczeństwo przetwarzania danych – **IOD**- załącznik 36.

2. Do obowiązków zarządzających - właścicieli procesów przetwarzania danych osobowych należy w szczególności:
   1) identyfikowanie zagrożeń dla danych przetwarzanych w procesie, w tym szacowanie ryzyka przy uwzględnianiu wielkości prawdopodobieństwa i siły oddziaływania (skutków);
   2) monitorowanie zgodności wnioskowanych uprawnień pracownikom przetwarzającym dane w procesie z uzyskanym zakresem dostępu do zasobu danych osobowych i wykonywania konkretnych czynności przetwarzania;
   3) w konsultacji z kierownikiem jednostki oraz IOD podejmowanie decyzji o udostępnianiu danych osobowych przetwarzanych w danym procesie;
   4) we współpracy z IOD opiniowanie wniosków dotyczących praw należnych osobie, której dane dotyczą o możliwości ich zrealizowania;
   5) tworzenie standardu zabezpieczenia obszaru przetwarzania, w którym przechowywane są dane osobowe przetwarzane w procesie przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;

bieżące przeglądanie praw dostępu użytkowników systemu informatycznego używanego w procesie do przetwarzania danych osobowych oraz wskazywanie kierownikom jednostek na konieczność modyfikacji zakresu uprawnień w systemie w przypadku zmiany zadań użytkowników.

Rozdział 8
Warunki powierzenia przetwarzania danych podmiotowi przetwarzającemu
§ 14

1. Do powierzenia dochodzi wtedy, gdy na zlecenie PŁ inny podmiot dokonuje operacji na danych osobowych należących do uczelni jako ich administratora. Kierownik jednostki może korzystać z usług wyłącznie takiego podmiotu przetwarzającego, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, w szczególności posiada wiedzę fachową, wiarygodność i zasoby.
2. Relacje pomiędzy PŁ a podmiotem przetwarzającym są wyraźnie określone w pisemnej umowie powierzenia którą należy opracować i podpisać w każdym przypadku, gdy jednostka korzysta z usługi podmiotu zewnętrznego (outsourcing) związanej z przetwarzaniem danych osobowych. W takim przypadku kierownik jednostki opracowuje projekt umowy powierzenia korzystając ze wzoru (załącznik 37), po czym przekazuje IOD do wglądu projekt umowy powierzenia wraz z podpisaną umowę usługi. IOD po sprawdzeniu przekazuje projekt umowy powierzenia do konsultacji z Działem Prawnym.
3. Umowa powierzenia określa przedmiot i czas przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą oraz obowiązki i prawa administratora. Zastrzec należy w umowie, że na żądanie PŁ podmiot przetwarzający pomaga mu w zapewnieniu przestrzegania obowiązków wynikających z dokonania oceny skutków dla ochrony danych. Ponadto umowa powinna stanowić, że podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie PŁ, a osoby upoważnione do przetwarzania danych zobowiązać należy do zachowania tajemnicy. W umowie należy zastrzec obowiązek podmiotu przetwarzającego zgłoszenia do PŁ wystąpienia naruszenia ochrony danych osobowych po jego stronie.
4. Powierzenie przetwarzania danych szczególnych kategorii nie różni się od powierzenia przetwarzania danych zwykłych.

Rozdział 9
Warunki współadministrowania
§ 15

1. Współadministrowanie ma miejsce w sytuacji, gdy co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, np. konkretne spółki celowe funkcjonujące w PŁ.
2. Proces współadministrowania wymaga w drodze wspólnych uzgodnień określenia zakresów odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów RODO oraz ustawy o ochronie danych osobowych. W uzgodnieniach należy ustalić czy podmioty są administratorami, czy wspólnie określili cele przetwarzania danych, czy wspólnie ustanowili sposoby i środki techniczno-organizacyjne przetwarzania danych osobowych oraz czy sprecyzowany został podział obowiązków i zakres odpowiedzialności.

Rozdział 10
Określenie zasad szkolenia personelu – informowanie o potrzebach szkoleniowych
§ 16

1. Kierownik jednostki jest zobowiązany zapewnić nowo przyjmowanym pracownikom , których zakres zadań jest związany z przetwarzaniem danych osobowych przeprowadzenie instruktażu wstępnego oraz stanowiskowego. Lista imienna osób przeszkolonych przekazywana jest sukcesywnie do wiadomości IOD, a jej drugi egzemplarz pozostaje w jednostce.
2. Kierownik jednostki przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje dotyczące celu, zakresu oraz sposobu zastosowania monitoringu w PŁ ustalonego w regulaminie pracy oraz wskazuje na konieczność indywidulanego zaznajomienie się z zasadami ochrony danych osobowych i obowiązkami z tego zakresu opisanymi w Polityce, w tym także w formie webinarium dostępnym na platformie WIKAMP.

3. IOD prowadzi dokumentację szkolenia indywidualnego oraz organizowanego centralnie dla personelu uczestniczącego w operacjach przetwarzania.
4. IOD opracowuje materiały informacyjne na temat zagadnień zgłoszonych przez kierowników jednostek.

Rozdział 11
Analiza ryzyka dla oceny skutków przetwarzania danych osobowych
§ 17

1. Przeprowadzenie oceny skutków dla ochrony danych wymagane jest wyłącznie w przypadku, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych w celu oszacowania źródła, charakteru, specyfiki i powagi ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z przepisami RODO.
2. Ocena skutków winna mieć miejsce, gdy w operacji przetwarzania dochodzi do istotnej zmiany, kiedy np. została wprowadzona do użytku nowa technologia, której podatność na zagrożenia bezpieczeństwa wcześniej nie została sprawdzona, dane osobowe są wykorzystywane w innym celu lub też właściciel procesu zdecydował o rozpoczęciu transferu danych do państwa trzeciego w rezultacie nowej operacji przetwarzania.
3. Nieprzeprowadzenie oceny skutków dla ochrony danych, gdy przetwarzanie podlega takiej ocenie, nieprawidłowe przeprowadzenie oceny skutków dla ochrony danych lub brak konsultacji z PUODO, gdy jest to wymagane mogą skutkować nałożeniem administracyjnej kary pieniężnej.
4. Wykaz rodzajów przetwarzania, w przypadku których ocena skutków dla ochrony danych jest obowiązkowa prowadzi Prezes Urzędu Ochrony Danych Osobowych.
5. Opis środków zabezpieczeń przyjętych w PŁ jako adekwatnych do zagrożeń dla ochrony danych osobowych wskazane w analizie ryzyka znajdują się w standardach ochrony danych osobowych- załącznik nr 2 do Zarządzenia Rektora Nr 7/ 2018 w sprawie wdrożenia dokumentacji ochrony danych osobowych w Politechnice Łódzkiej.

Rozdział 12
Kanały komunikacji
§ 18

1. Ustala się następujące trzy kanały komunikacji służbowej pracowników ze studentami:

   1) system poczty elektronicznej PŁ (SPE) z zachowaniem zasady, że wszelka komunikacja służbowa odbywa się wyłącznie pomiędzy skrzynkami służbowymi pracowników i skrzynkami studenckimi w ramach SPE;
   2) Platforma WIKAMP, szczególnie zalecana do prezentowania studentom ocen z poszczególnych aktywności śródsemestralnych oraz wymiany/archiwizacji wszelkich opracowań powstających w ramach procesu dydaktycznego;
   3) Wirtualny Dziekanat.
2. Powyższe kanały wykorzystywane są do wszelkiej komunikacji służbowej pomiędzy pracownikami i studentami, ze szczególnym uwzględnieniem korespondencji wymagającej przetwarzania danych osobowych (np. publikowanie ocen, omawianie prac dyplomowych i innych opracowań, zbieranie, przechowywanie i dyskutowanie innych dokumentów zawierających dane osobowe).

Rozdział 13
Korzystanie z poczty elektronicznej SPE
§ 19

1. System poczty elektronicznej SPE jest przeznaczony wyłącznie do prowadzenia korespondencji służbowej, stąd listy elektroniczne wysyłane za pośrednictwem poczty traktowane są jako korespondencja służbowa konieczna do wykonywania zadań i obowiązków służbowych.

2. Regulacje dotyczące korzystania z poczty SPE znajdują się w dokumencie pod nazwą „Zasady funkcjonowania SPE" i publikowane są na stronie Centrum Komputerowego przez Dyrektora Centrum Komputerowego.
3. W Politechnice Łódzkiej obowiązuje jednolity System Poczty Elektronicznej (SPE). Korzystanie do przesyłania korespondencji służbowej z innych systemów poczty elektronicznej, w tym z użyciem lokalnych pod-domen domeny p.lodz.pl odbywa się z zapewnieniem niezaprzeczalności wysyłania i odbioru oraz bezpieczeństwa przesyłania danych pomiędzy serwerami pocztowymi.
4. Kierownik jednostki przed zwolnieniem pracownika, w momencie rozliczania się z jednostką pozyskuje od niego zgodę na piśmie dotyczącą zamiaru dalszego korzystania z poczty elektronicznej przez byłego pracownika, bez prawa wysyłania listów ze skrzynki służbowej. Brak oświadczenia powoduje zamknięcie lub zablokowanie konta.
5. Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej) w sposób nie naruszający tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

Rozdział 14
Standardy ochrony danych osobowych
§ 20

1. PŁ jako administrator danych stosuje wytyczne- standardy ochrony danych osobowych przyjęte jako adekwatne do oceny ryzyka w Politechnice Łódzkiej **według załączonego dokumentu**.

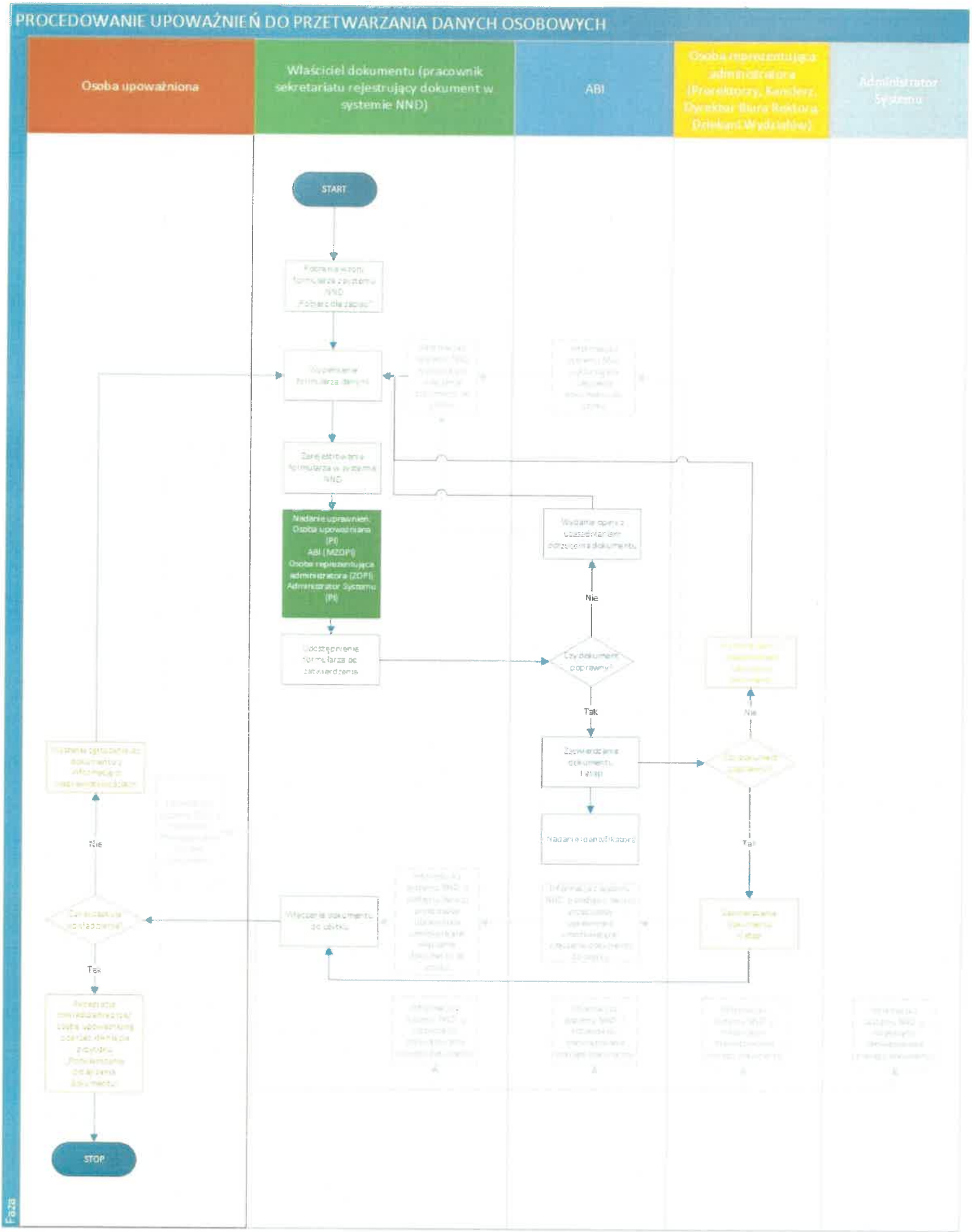
Rozdział 15
Postępowanie z kluczami
§ 21

1. Przechowywanie dokumentów zawierających dane osobowe w pomieszczeniach zabezpieczonych drzwiami zwykłymi zamykanymi na klucze różnego typu, wyposażonymi jeśli potrzeba w samozamykacze, stanowi minimalny standard zapewniający ochronę danym osobowym, gdzie dane osobowe są odczytywane, wpisywane, modyfikowane, niszczone lub przechowywane.
2. Administratorzy budynków prowadzą wykaz pomieszczeń stanowiących obszar przetwarzania zawierający adres budynku, piętro oraz numery pomieszczeń. Oznaczenie takich pomieszczeń w sposób wyróżniający je od pozostałych jest uzasadnione i zależy od decyzji kierownika jednostki. Dostęp do takich pomieszczeń jest ewidencjonowany.
3. Postępowania z kluczami do pomieszczeń obszaru przetwarzania odbywa się **według wzoru**.

Rozdział 16
Postanowienia końcowe
§ 22

1. Regulacje dotyczące systemów informatycznych określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
2. Na stronie http://adm.edu.p.lodz.pl znajdują się dokumenty dotyczące ochrony danych osobowych, w tym także wzory zgód, klauzul, komunikatów itp., których treść należy brać pod uwagę przy rozważaniu kwestii sposobów i metod postępowania przy przetwarzaniu danych osobowych oraz organizowania ochrony danych w jednostce.
3. W przypadku zmian w przepisach o ochronie danych osobowych lub w dokumentach wewnętrznych, Inspektor Ochrony Danych dokonuje przeglądu niniejszego dokumentu. Zmiany wprowadzane są w formie arkusza zmian, bez konieczności podpisywania nowego zarządzenia Rektora.

Rektor
Politechniki Łódzkiej
Prof. dr hab. inż. Sławomir Wiak



Załącznik Nr 1 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Załącznik Nr 2 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Proces przetwarzania danych osobowych osób uczących się w PŁ

Wprowadzenie

Politechnika Łódzka jako administrator danych osobowych jest odpowiedzialna za przetwarzanie danych osobowych kandydatów na studia, studentów studiów pierwszego, drugiego i trzeciego stopnia - zwanych dalej studentami, słuchaczy studiów podyplomowych oraz absolwentów, określając cele przetwarzania oraz zakres danych adekwatnych i niezbędnych do zrealizowania tych celów.

Przetwarzanie danych osobowych osób uczących się odbywać się będzie w celach związanych z rekrutacją na studia, a następnie kształceniem w różnych formach, w szczególności w celu realizacji zadań uczelni wskazanych w prawie właściwym dla szkolnictwa wyższego i nauki oraz w innych ustawach szczegółowych związanych z odbywaniem studiów wyższych oraz w rozporządzeniach wykonawczych do tych ustaw.

Zmiana celu przetwarzania lub zakresu zbieranych danych wymaga konsultacji z Inspektorem Ochrony Danych (IOD) oraz uzyskania zgody Prorektora właściwego odpowiednio do spraw Studenckich lub do spraw Kształcenia.

Proces przetwarzania obejmuje kategorie danych osobowych kandydata na studia, studenta, słuchacza studiów podyplomowych wchodzących w skład jednego ogólnouczelnianego zasobu studentów i absolwentów; w dalszej części opisu procesu „student i/lub absolwent". Zasobem tym zarządza Prorektor ds. Studenckich. Dane z tego zasobu mogą być wykorzystywane tylko do czynności związanych z działalnością dydaktyczną prowadzoną przez Politechnikę Łódzką.

Wszędzie tam, gdzie jest to możliwe i uzasadnione oceną ryzyka, dane osobowe osób uczących się będą anonimizowane lub poddawane pseudonimizacji oznaczającej niemożność przypisania danych konkretnemu studentowi/doktorantowi bez użycia dodatkowych informacji.

Administracja rektorska, wydziałowa i jednostek oraz kanclerska zapewnią zgodność przetwarzania danych osobowych pozostających w ich dyspozycji, wykonując czynności określone przez przepisy 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 (ogólnego rozporządzenia o ochronie danych), Dz.U.UE.L.2016.119.1, (dalej RODO), ustawę o ochronie danych osobowych oraz wewnętrzną Politykę bezpieczeństwa danych osobowych.

1. Przesłanki umożliwiające zgodne z prawem przetwarzanie danych osobowych:

1.1. Każda czynność związana z użyciem danych osobowych osób uczących się, w tym m.in. zapisywanie, kopiowanie czy przechowywanie w formie papierowej lub cyfrowej dokonywana jest w oparciu o artykuł 6 RODO „Zgodność przetwarzania z prawem".

1.2. Zasadniczą przesłanką przetwarzania danych osobowych osób uczących się – studentów i absolwentów jest obowiązek prawny ciążący na Politechnice jako administratora danych podmiotu publicznego, wynikający z art. 6 ust 1 lit. c RODO.

1.3. Zgoda jako przesłanka uprawniająca do przetwarzania danych osobowych stanowi jedną z równoważnych przesłanek spośród wszystkich przewidzianych w art. 6 RODO. Pozyskiwanie zgody przez jednostki organizacyjne Politechniki Łódzkiej jako uczelni publicznej może mieć miejsce w wyjątkowych sytuacjach, przy zachowaniu rzeczywistego i wolnego wyboru oraz zapewnieniu możliwości wycofania zgody pamiętając, że kierownik jednostki dokumentuje wszelkie czynności związane z pozyskiwaniem zgody, np. kiedy, w jakich okolicznościach i komu udzielona została zgoda oraz w jaki sposób spełniono obowiązek informacyjny wobec osoby udzielającej zgody.

1.4. Dział Spraw Studenckich dysponuje wzorami klauzuli informacyjnej, treści zgody na przetwarzanie danych osobowych zawartych w dokumentach oraz treścią zgody na przetwarzanie wizerunku.

2. Czynności przetwarzania danych osobowych kandydatów na studia

2.1. Uchwały Senatu Politechniki w sprawie zasad przyjęć na studia poszczególnych stopni dla określonych kierunków precyzują zakres danych osobowych kandydatów. Sekcja Rekrutacji gromadzi dane osobowe wpisane do dokumentów wymaganych od kandydata na studia i odpowiada za ochronę danych podczas rekrutacji.

2.2. Kandydat na studia jest zapoznawany z tekstem klauzuli informacyjnej, która po podpisaniu umieszczana jest w jego teczce jako odrębny dokument potwierdzający ten fakt, ważny przez cały okres kształcenia studenta.

2.3. Pakiety dokumentów kandydatów, którzy nie uzyskali pozytywnego wyniku kwalifikacji, brakowane są w archiwum protokolarnie po upływie okresu 5 lat od przekazania przez dziekanaty za zgodą Archiwum Państwowego.

2.4. Wyniki postępowania rekrutacyjnego są jawne.

3. Czynności przetwarzania danych osobowych studentów i absolwentów

3.1. Wydziały, Instytuty, Katedry oraz jednostki pozawydziałowe, kiedy to jest niezbędne, odbierają w trakcie studiów od studentów oświadczenie na piśmie, w którym student wymienia z imienia i nazwiska osobę upoważnioną do otrzymywania wszelkich informacji o nim, wymienia również zakres danych jego dotyczących, który może być udostępniony lub oświadcza, że nie należy udostępniać jego danych nikomu .

3.2. Jednostki organizacyjne dokumentujące przebieg studiów wydają na wniosek studenta lub absolwenta odpisy lub wyciągi z dokumentacji upoważnionej osobie lub wysyłają pocztą na wskazany adres za zwrotnym poświadczeniem odbioru. W przypadku braku upoważnienia pozyskanego w trybie wskazanym w punkcie 3.1, osoby wnioskujące o udostępnienie informacji o statusie studenta (członkowie rodzin, bliscy, itp.) muszą okazać w dziekanacie lub sekretariacie jednostki upoważnienie wystawione przez studenta lub absolwenta potwierdzone notarialnie, stanowiące podstawę do udzielania informacji oraz wydawania wnioskodawcom dokumentów określonych rozporządzeniem w sprawie dokumentacji przebiegu studiów.

3.3. Jednostki organizacyjne uczelni, które przetwarzają dane osobowe dzieci oraz osób starszych pozyskują klauzulę zgody oraz realizują obowiązek informacyjny w momencie zbierania danych. Kierownicy tych jednostek konsultują tekst zgody i treść klauzuli informacyjnej z Inspektorem Ochrony Danych, po czym przechowują je w jednostce.

3.3.1. W przypadku Łódzkiego Uniwersytetu Dziecięcego, podstawą zbierania i przechowywania danych osobowych jest zgoda rodzica lub opiekuna prawnego dziecka. W celu weryfikacji wieku dziecka zasadne jest pozyskiwanie w momencie rekrutacji numeru PESEL dziecka. Oświadczenie o uczestnictwie w zajęciach w Uniwersytecie precyzuje informacje przekazane do wiadomości rodzica/opiekuna.

3.3.2. W przypadku Uniwersytetu Trzeciego Wieku podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą a zakres danych winien być adekwatny do celu uczenia.

3.4. Nie wykorzystuje się danych dziecka ani danych osób starszych do celów marketingowych i do tworzenia profili osobowych. Podobnie nie wykorzystuje się rzeczywistych danych studenta bądź absolwenta do rekomendowania zasadności wyboru określonego kierunku studiów

3.5. Politechnika Łódzka w związku z funkcjonowaniem systemu biblioteczno informacyjnego może przetwarzać określone w jej statucie dane osobowe osób korzystających z tego systemu. Stąd deklaracja wypełniana przez zakładającego konto w bibliotece (wzór w bibliotece zał. 5) nie może zawierać więcej danych, zwłaszcza pozyskiwanie numeru PESEL jest nieuprawnione.

3.6. Organizator konkursu z udziałem studentów, zwłaszcza gdy konkurs jest sponsorowany przez Przedsiębiorcę musi odebrać od uczestników konkursu oświadczenie o zachowaniu praw autorskich dotyczących pracy konkursowej, zezwolenia na wykorzystanie wizerunku oraz zgody na przetwarzanie danych w celach organizacji, przeprowadzenia i udostępnienia informacji o wynikach konkursu. Stosowne wzory zapewnia Inspektor Ochrony Danych.

3.7. Jednostki prowadzące szkolenia komercyjne zbierają dane osobowe uczestników w zakresie adekwatnym do celu szkolenia. Czynności przetwarzania prowadzi się w szczególności w oparciu o umowę usługi edukacyjnej określającej warunki odpłatności za udział w takim szkoleniu. Treść umowy uzgadniana jest z działem prawnym PŁ. Uczestnicy szkolenia podpisują zapoznanie się z treścią klauzuli informacyjnej, którą przechowuje się w dokumentacji szkolenia.

3.8. Pozyskiwanie przez Politechnikę od swoich absolwentów informacji o ich karierach zawodowych oraz od studentów poszukujących pracy, praktyki lub stażu powinno następować jedynie za dobrowolną zgodą studentów i /lub absolwentów.

3.9. Informowanie studentów o wynikach egzaminów, kolokwiów, zaliczeń i sprawdzianów odbywa się z poszanowaniem konstytucyjnego prawa do prywatności. Oceny poddane pseudonimizacji doprowadza się do wiadomości studentów. Wskazane jest korzystanie z dostępnych narzędzi informatycznych platformy WIKAMP.

3.10. Akta zawierające dane osobowe studentów/absolwentów będą przechowywane przez okres zgodny z Jednolitym Rzeczowym Wykazem Akt PŁ z zapewnieniem prawa dostępu do tych danych.

4. Czynności przetwarzania danych osobowych w Samorządzie Studenckim

4.1. Przetwarzanie danych osobowych przez Samorząd uczelniany i wydziałowy jest uzasadnione w przypadkach:

4.1.1. zbierania danych osobowych studentów w zakresie imię i nazwisko i kierunek studiów, numer albumu i wydział w celu przeprowadzenia wyborów do Samorządu;

4.1.2. zbieranie danych osobowych studentów ubiegających się o zakwaterowanie w związku z koniecznością ustalenia pierwszeństwa w przyznawaniu miejsca w domu studenckim;

4.1.3. Przewodniczący Samorządu Studenckiego jest odpowiedzialny za zapewnienie poprawnej ochrony powyższych danych osobowych zebranych i przechowywanych w pomieszczeniu Samorządu.

5. Czynności przetwarzania danych osobowych przez Wydziałowe Komisje Stypendialne oraz Odwoławcze Komisje Stypendialne jest uzasadnione w przypadku wnioskowania studenta o pomoc materialną oraz o stypendia, o których mowa w ustawie prawo o szkolnictwie wyższym. Zakres danych osobowych niezbędnych komisjom określa regulamin pomocy materialnej.

6. Czynności przetwarzania danych osobowych w zakresie ich udostępniania
   6.1. Rozpatrzenie wniosku o udostępnienie informacji o studencie i/lub absolwencie wraz z przygotowaniem odpowiedzi należy do obowiązków kierownika jednostki - adresata wniosku. Przy podejmowaniu decyzji należy pamiętać, że udostepniający odpowiada za ewentualne skutki udostępnienia, bądź za skutki bezprawnej odmowy udostępnienia. Odpowiedź w sprawie udostępnienia włączana jest do teczki studenta i/lub absolwenta. Kopia lub skan jest przesyłany mailowo do Inspektora Ochrony Danych w celu ujęcia w ogólnouczelnianym rejestrze udostępnień.
   6.2. Postępowanie w przypadku wpływu do PŁ pism zawierających żądania udostępnienia danych osobowych cudzoziemców:
      6.2.1. informacje o studentach cudzoziemcach studiujących w PŁ mogą być przekazywane uprawnionym organom administracji w kwestii aktualnego statusu studenta cudzoziemca czasowo zamieszkującego RP
      6.2.2. po rozliczeniu semestru Prorektor ds. Kształcenia realizuje obowiązek zawiadomienia wojewody, który udzielił studentowi zezwolenia na pobyt w RP o skreśleniu cudzoziemca z listy studentów, ale także o niezaliczeniu roku studiów w określonym terminie. Centrum Współpracy Międzynarodowej analizuje po zakończeniu semestru przesłane przez wydziały zbiorcze informacje dotyczące rejestracji studentów cudzoziemców na kolejny semestr i w terminie do dwóch tygodni od zakończenia semestru opracowuje pismo informujące wojewodę w tej sprawie. Projekty odpowiedzi konsultowane są z działem prawnym PŁ.

7. Postępowanie w przypadku żądania potwierdzenia wiarygodności dyplomów i informacji o przebiegu studiów

   7.1. absolwent studiów PŁ posiada wiarygodny dyplom ukończenia studiów wraz z suplementem do dyplomu. Dokumenty te dostarczają pełny zakres informacji dotyczący uznawania jego kwalifikacji akademickich oraz zawodowych w kraju i zagranicą. Są one również potwierdzeniem ukończenia studiów wyższych na określonym kierunku, a suplement zawiera opis rodzaju, poziomu, kontekstu, treści i statusu pomyślnie ukończonych studiów

   7.2. podmioty rekrutacyjne typu head hunter oraz działy HR otrzymując od kandydata do pracy do wglądu powyższe dokumenty posiadają pełną wiedzę o tytule zawodowym i niezbędne informacje do potwierdzenia jego kwalifikacji zawodowych. Każde podważanie wiarygodności przedstawionych dokumentów zgodnych z ministerialnym wzorem oraz sygnowanych godłem RP skutkować winno złożeniem przez dany podmiot zawiadomienia o możliwości popełnienia przestępstwa.

   7.3. dziekanaty i sekretariaty nie mają obowiązku, by angażować pracowników do wykonywania dodatkowej pracy na rzecz podmiotów, które podnosząc dobro kandydata do pracy kwestionują wiarygodność przedstawionych dokumentów i żądają ich potwierdzania.

   7.4. udzielając odpowiedzi pamiętać należy, że mamy do czynienia z udostępnianiem informacji podmiotom często prywatnym z pogranicza wywiadowni gospodarczych czy też białego wywiadu. Odpowiedzi należy udzielać w języku polskim

8. Papierowe wersje dokumentów zawierających dane osobowe pozyskiwane w opisywanym procesie, w tym m.in. oświadczenia, klauzule informacyjne, treści zgód, kopie i skany należy

odwzorowywać do wersji elektronicznego dokumentu i przechowywać do momentu zrealizowania celu przetwarzania.

Opracował: Zespół ds. RODO, 28 luty 2018r., wersja 12 marca b.r.

Załącznik Nr 3 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Klauzula dot. przetwarzania danych osobowych kandydatów na studia, studentów wszystkich stopni oraz uczestników studiów doktoranckich

Zgodnie z art. 13 ust. 1 i ust. 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 (ogólnego rozporządzenia o ochronie danych), Dz.U.UE.L.2016.119.1, informuję, że:

1) administratorem Twoich danych osobowych jest Politechnika Łódzka, adres siedziby: ul. Żeromskiego 116, 90-924 Łódź;

2) administrator wyznaczył inspektora ochrony danych, kontakt mailowy: rbi@adm.p.lodz.pl, tel. 426312039;

3) Twoje dane osobowe będą przechowywane przez okres niezbędny do zrealizowania celu przetwarzania w ramach realizacji procesu kształcenia w Politechnice Łódzkiej, w tym dla archiwizacji;

4) posiadasz prawo do żądania od administratora dostępu do Twoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych;

5) masz prawo wniesienia skargi do organu nadzorczego, którym w Polsce jest Prezes Urzędu Ochrony Danych Osobowych, adres siedziby: ul. Stawki 2, 00-193 Warszawa, gdy uznasz, że przetwarzanie Twoich danych osobowych narusza przepisy rozporządzenia wskazanego na wstępie;

6) podanie przez Ciebie danych osobowych jest wymogiem ustawowym;

7) decyzje podejmowane wobec Ciebie i Twoich danych osobowych nie będą podejmowanie w sposób zautomatyzowany, w tym nie zastosujemy wobec nich profilowania;

8) administrator dopuszcza możliwość wykorzystania Twoich danych osobowych (imienia i nazwiska) oraz wizerunku na swojej stronie internetowej w ramach prezentowania wybitnych osiągnięć uzyskanych przez studentów/uczestników studiów doktoramckich PŁ.

Przyjąłem do wiadomości .....

data podpis

Pursuant to article 13(1) and (2) of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1, you are hereby informed of the following:

1) Lodz University of Technology, registered office 90-924 Łódź (postal code 90-924), Żeromskiego 116, is the controller of your personal data;

2) the control has appointed the data protection officer, e-mail address: rbi@adm.p.lodz.pl, phone: 426312039;

3) your personal data will be stored for the period required for the purposes of the processing for which the personal data are intended with reference to the process of education in Lodz University of Technology, including for archiving purposes;

4) you have the right of access to your personal data, the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data or to object to such processing, the right to data portability;

5) you the right to lodge a complaint with the supervisory authority, which in Poland is the President of the Office of Competition and Consumer Protection, Stawki 2, 00-193 Warszawa, if you consider that the processing of personal data relating to you infringes the Regulation referred to above;

6) the provision of your personal data is a statutory requirement;

7) neither you nor your personal data will be subject to a decision based solely on automated processing, including profiling;

8) the controller may use your personal data (full name) and your image for the purpose of presentation of outstanding achievements of the students of Lodz University of Technology.

I have read and understood the above information .....

Date and signature

Załącznik Nr 4 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Pursuant to article 13(1) and (2) of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1, you are hereby informed of the following:

1) Lodz University of Technology, registered office 90-924 Łódź (postal code 90-924), Żeromskiego 116, is the controller of your personal data;

2) the control has appointed the data protection officer, e-mail address: rbi@adm.p.lodz.pl, phone: 426312039;

3) your personal data will be stored for the period required for the purposes of the processing for which the personal data are intended with reference to the process of education in Lodz University of Technology, including for archiving purposes;

4) you have the right of access to your personal data, the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data or to object to such processing, the right to data portability;

5) you the right to lodge a complaint with the supervisory authority, which in Poland is the President of the Office of Competition and Consumer Protection, Stawki 2, 00-193 Warszawa, if you consider that the processing of personal data relating to you infringes the Regulation referred to above;

6) the provision of your personal data is a statutory requirement;

7) neither you nor your personal data will be subject to a decision based solely on automated processing, including profiling;

8) the controller may use your personal data (full name) and your image for the purpose of presentation of outstanding achievements of the students of Lodz University of Technology.

I have read and understood the above information .....

Date and signature

Załącznik Nr 5 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Informujemy, że administratorem Pani / Pana danych osobowych zawartych w umowie o warunkach kształcenia na studiach* ..... jest Politechnika Łódzka z siedzibą w Łodzi, przy ul. Żeromskiego 116; dane przetwarzane są przez** ..... .

W sprawach ochrony danych osobowych można się skontaktować z wyznaczonym przez Rektora inspektorem ochrony danych pod adresem rbi@adm.p.lodz.pl, telefon 42 631 20 39.

Politechnika Łódzka przetwarza Pani / Pana dane osobowe wyłącznie w celu wykonania zadań i zobowiązań wynikających z tej umowy, na podstawie art. 6 ust. 1 lit. b) 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 (RODO).

Pani / Pana dane osobowe będą udostępniane członkom komisji*** ..... oraz osobom lub jednostkom dokumentującym przebieg studiów.

Pani / Pana dane będą przechowywane przez minimum 50 lat poczynając od stycznia roku następnego po zakończeniu toku studiów. W przypadku wniesienia zastrzeżeń lub roszczeń okres ten przedłuża się o czas załatwienia sprawy.

Przysługuje Pani / Panu zgodnie z RODO: prawo dostępu do swoich danych oraz otrzymania ich kopii; prawo do sprostowania i uzupełnienia swoich danych; prawo do usunięcia danych osobowych lub ograniczenia przetwarzania tylko w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa; prawo do uzyskania informacji oraz prawo do wniesienia skargi do Prezes UODO (na adres Urzędu ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa);

Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany i nie będą poddawane profilowaniu.

Oznaczenia:
*stacjonarne, niestacjonarne, międzyuczelniane, międzywydziałowe, doktoranckie
** jednostka prowadząca studia
*** Rekrutacyjnej, Przewodów Doktorskich, Rady Wydziału

Załącznik Nr 6 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

You are hereby informed that Lodz University of Technology, registered office 90-924 Łódź (postal code 90-924), Żeromskiego 116, is the controller of your personal data provided in the agreement on on the terms and conditions of educational services provided during .... degree programmes ; your personal data is processed by**..... .

The controller has appointed a data protection officer, e-mail address: rbi@adm.p.lodz.pl, phone: 426312039, whom you may contact with regard to the protection of your personal data.

Lodz University of Technology processes your personal data only for the purposes required for the completion of tasks and obligations under the said agreement pursuant to article 6(1)(b) of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Your personal data will be shared with members of the ..... Committee*** and with employees or units responsible for maintaining documentation of your studies.

Your personal data will be retained for a minimum period of 50 years starting from January of the year following the year of your graduation. Should objections arise or claims be filed, the period of retention will be extended accordingly to account for the time required to resolve the matter.

In accordance with the GDPR you have the right to access your personal data and to obtain copies thereof; the right of rectification and of having incomplete personal data completed; the right of erasure or restriction of processing only when the processing is for purposes other than required by law; the right of information and the right to lodge a complaint with the President of the Office for the Protection of Personal Data (Office for the Protection of Personal Data, Stawki 2, 00-193 Warszawa);

Your personal data will not be processed by automated means and will not be subject to profiling.

* taught full-time, taught part-time, taught cross-university, taught cross-faculty, PhD, and PhD by research

** organizational unit providing the degree programme

*** Admissions, Doctoral Proceedings, Faculty Council

Załącznik Nr 7 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

.....

imię i nazwisko studenta/doktoranta

.....

nr albumu

Oświadczenie

- Upoważniam* ..... do otrzymywania informacji, w których posiadaniu jest Politechnika Łódzka, o mnie w zakresie: *przebiegu studiów i procesu kształcenia.*
- Nie wyrażam zgody* na udostępnianie moich danych, w których posiadaniu jest Politechnika Łódzka nikomu.
  Upoważnienie traci moc z chwilą rozwiązania stosunku prawnego między uczelnią a osobą podpisującą oświadczenie.

* niepotrzebne skreślić.

.....

data

.....

podpis

Załącznik Nr 8 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Klauzula informacyjna oraz klauzula zgody w związku z przetwarzaniem danych osobowych dotyczących członków rodzin studentów i doktorantów ubiegających się o zakwaterowanie lub stypendium socjalne

Informujemy, że:

1. Administratorem danych osobowych zawartych we wniosku o przyznanie * ..... jest Politechnika Łódzka z siedzibą w Łodzi, (90-924), ul. Żeromskiego 116.

2. Politechnika Łódzka przetwarza Pani / Pana dane osobowe na podstawie art. 6 ust. 1 lit. a) 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).

3. Pani / Pana dane osobowe będą przetwarzane wyłącznie w celu dokumentowania przebiegu przyznawania miejsc zakwaterowania w DS lub stypendium i nie będą udostępniane innym odbiorcom.

3. Podanie danych jest dobrowolne, jednakże niezbędne do rozpatrzenia wniosku oraz przyznania miejsca w akademiku lub świadczenia socjalnego.

4. Przysługuje Pani / Panu zgodnie z RODO: prawo dostępu do swoich danych oraz otrzymania ich kopii; prawo do sprostowania i uzupełnienia swoich danych; prawo do usunięcia danych osobowych lub ograniczenia przetwarzania tylko w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa; prawo do uzyskania informacji oraz prawo do wniesienia skargi do Prezes UODO (na adres Urzędu ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa);

Ja niżej podpisana/-y wyrażam zgodę na przetwarzanie moich danych osobowych przez Administratora zawartych w przedstawionej dokumentacji, w tym danych członków rodziny w celu realizacji procedury przyznania zakwaterowania lub stypendium socjalnego.

Administrator informuje, że niniejsza zgoda może być wycofana w każdym czasie a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie tej zgody przed jej wycofaniem.

*zakwaterowanie, stypendium socjalne

.....

(podpis studenta/doktoranta)

Załącznik Nr 9 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

KWESTIONARIUSZ OSOBOWY DLA OSOBY UBIEGAJĄCEJ SIĘ O ZATRUDNIENIE

1. Imię (imiona) i nazwisko .....
2. Data urodzenia .....
3. Obywatelstwo .....
4. Adres do korespondencji .....
5. Adres poczty elektronicznej lub numer telefonu .....
6. Wykształcenie .....

(nazwa szkoły i rok jej ukończenia)

.....

.....

(zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy)

7. Wykształcenie uzupełniające .....

.....

.....

.....

.....

(kursy, studia podyplomowe, data ukończenia nauki lub data rozpoczęcia nauki w przypadku jej trwania)

8. Przebieg dotychczasowego zatrudnienia .....

.....

.....

.....

.....

.....

(wskazać okresy zatrudnienia u kolejnych pracodawców oraz zajmowane stanowiska pracy)

9. Oświadczam, że dane zawarte w pkt 1 i 2 są zgodne z dowodem osobistym seria ..... nr .....

wydanym przez .....

lub innym dokumentem tożsamości .....

.....

.....
(miejscowość i data)

.....
(podpis osoby ubiegającej się o zatrudnienie)

Załącznik Nr 10 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

KWESTIONARIUSZ OSOBOWY DLA PRACOWNIKA

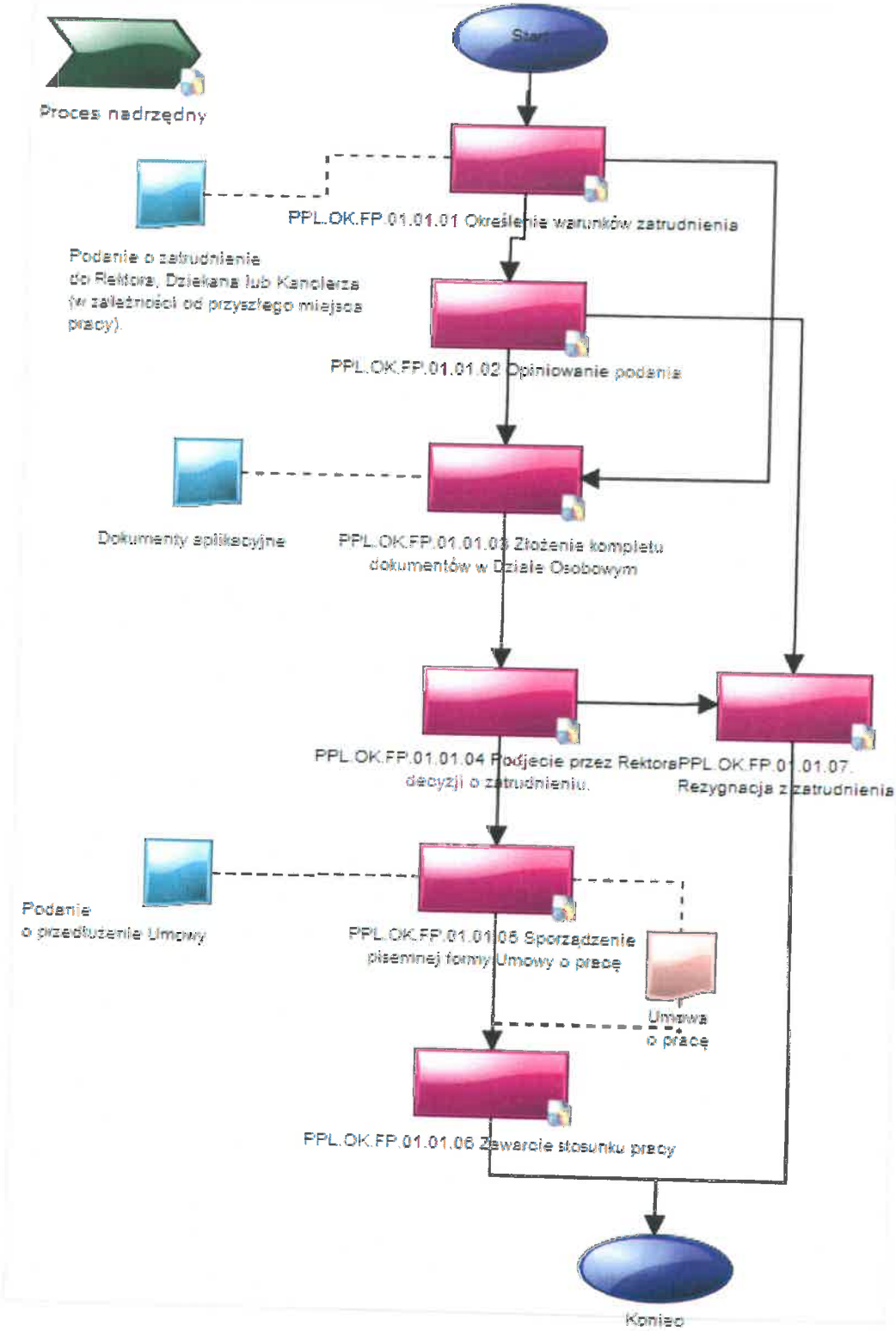
1. Imię (imiona) i nazwisko .....
2. Numer ewidencyjny PESEL (w przypadku jego braku rodzaj i numer dokumentu potwierdzającego tożsamość)
   .....
3. Adres zamieszkania .....
4. Stan rodzinny .....
   .....
   .....
   .....

   (imiona i nazwiska oraz daty urodzenia dzieci pracownika i innych członków rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy)
5. Powszechny obowiązek obrony:
   a) stosunek do powszechnego obowiązku obrony .....
   b) stopień wojskowy .....
      numer specjalności wojskowej .....
   c) przynależność ewidencyjna do WKU .....
   d) numer książeczki wojskowej .....
   e) przydział mobilizacyjny do sił zbrojnych RP .....
6. Osoba, którą należy zawiadomić w razie wypadku .....
   .....

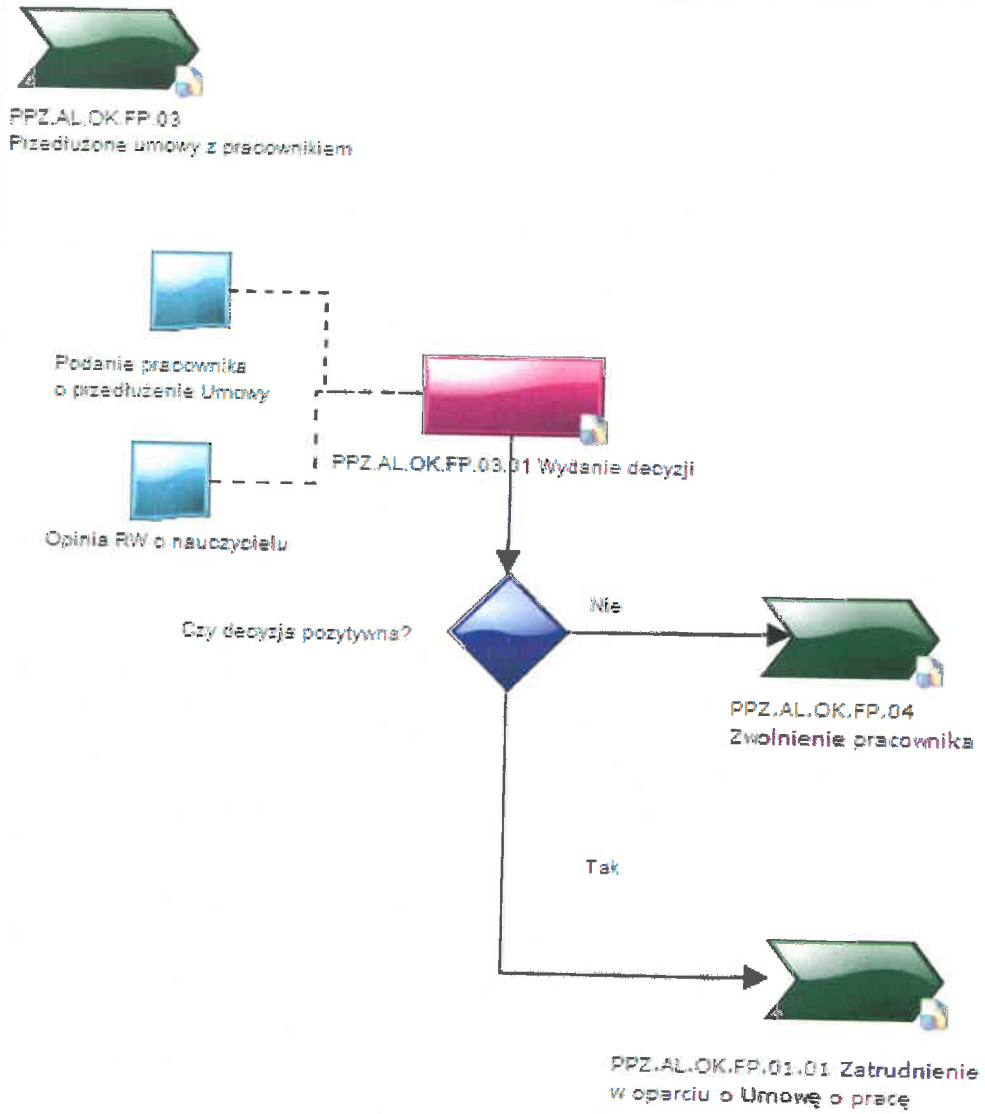
   (imię i nazwisko, adres, telefon)
7. Oświadczam, że dane zawarte w pkt 1 i 2 są zgodne z dowodem osobistym seria ..... nr .....
   wydanym przez .....
   lub innym dokumentem tożsamości .....
   .....

.....
(miejscowość i data)

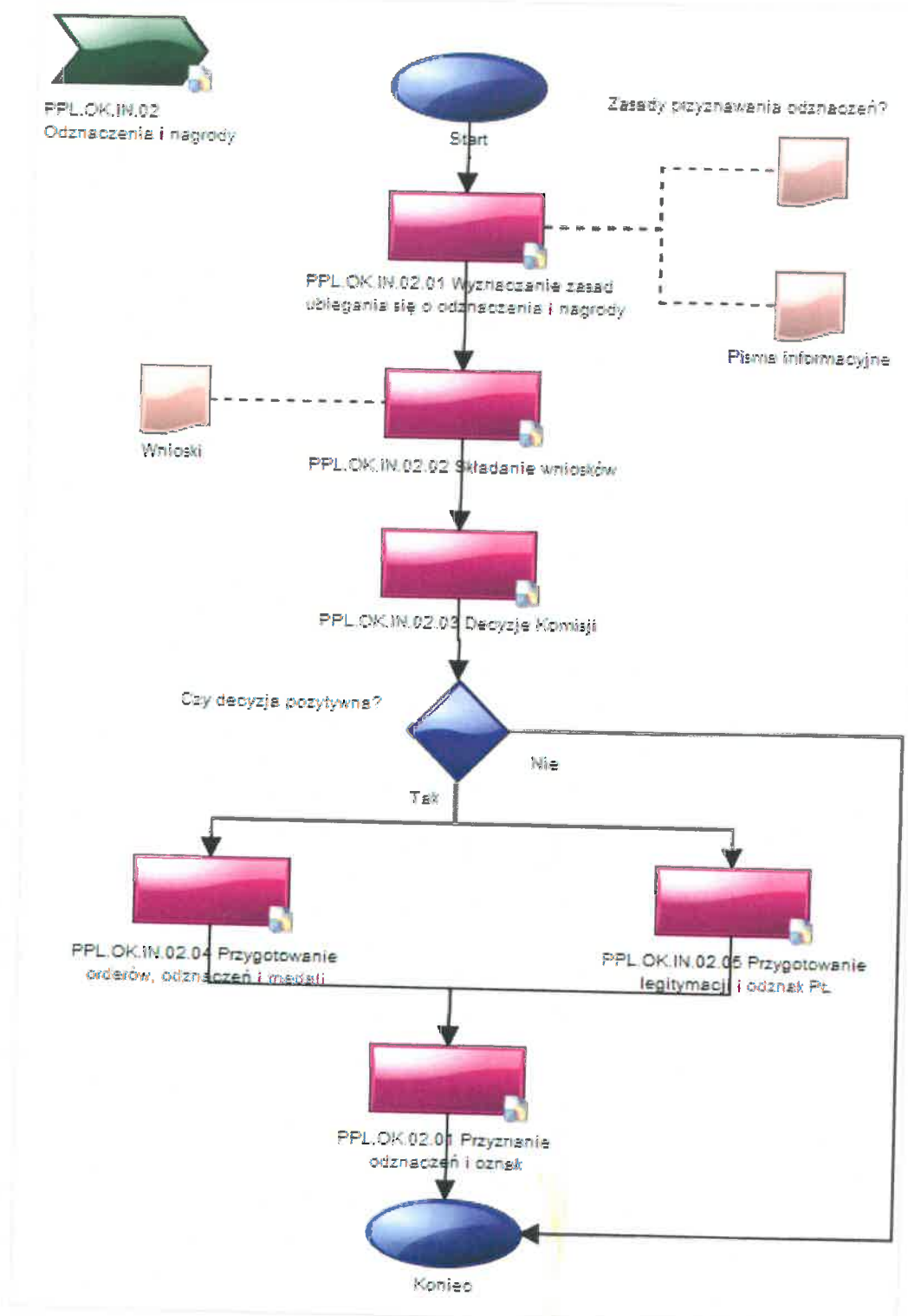
.....
(podpis pracownika)



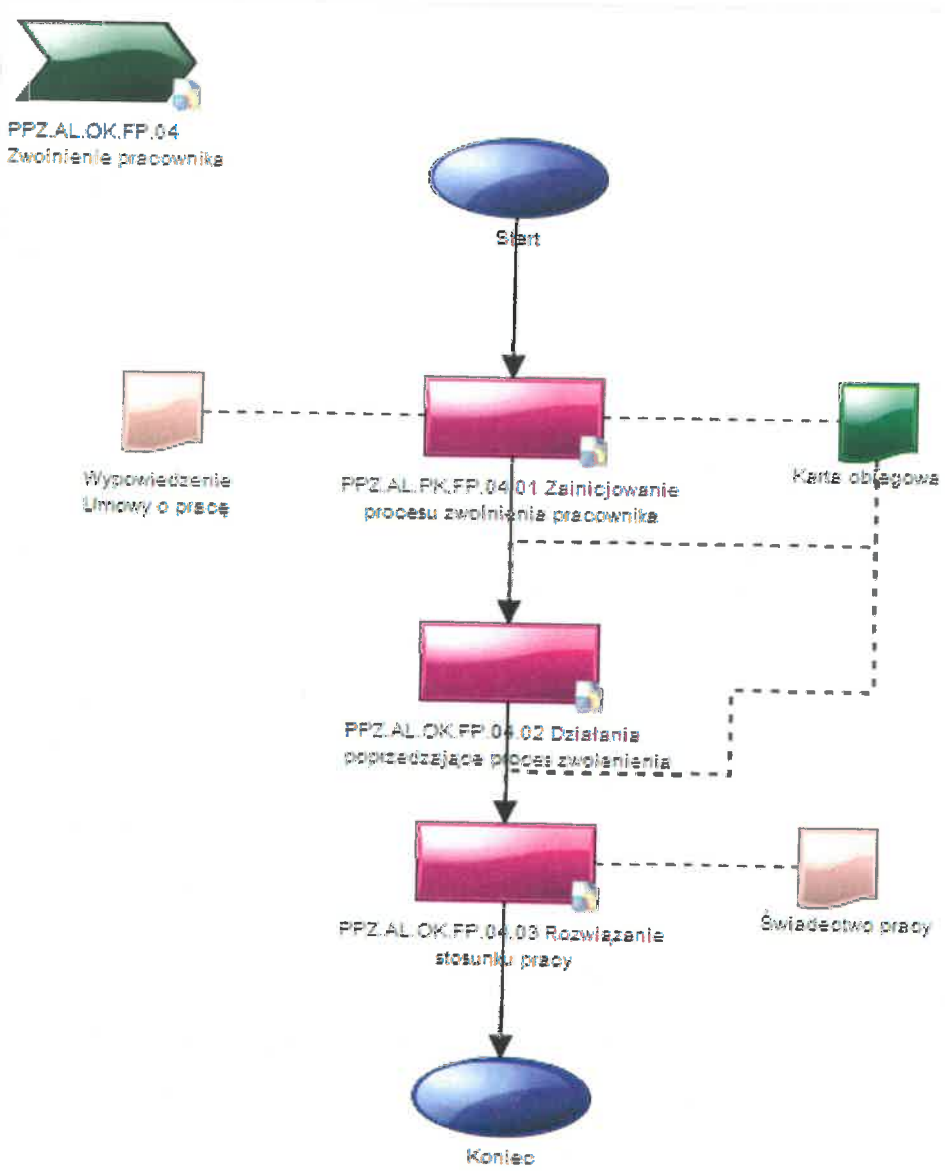
Załącznik Nr 11 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej



Załącznik Nr 12 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej



Załącznik Nr 13 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej



Załącznik Nr 14 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Załącznik Nr 15 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Dane pracownika

Zezwolenie na wykorzystanie i rozpowszechnianie wizerunku

Na podstawie art. 81 ust. 1 ustawy z dnia 4 lutego 1994r. o prawie autorskim i Rawach pokrewnych (j.t. Dz. U. z 2017 r. poz. 800 ze zm.) zezwalam na nieodpłatne utrwalanie i rozpowszechnianie mojego wizerunku w postaci zdjęć wykonywanych w miejscu pracy w dniach ..... przez ..... . Wyrażam również zgodę na nieodpłatne utrwalenie i rozpowszechnianie mojego wizerunku na w/w zdjęciach dla celów ..... na terenie kraju w zakresie marketingu.

Ponadto oświadczam, że nieodpłatna zgoda na utrwalenie i rozpowszechnianie mojego wizerunku obejmuje także wykorzystanie, utrwalanie, zwielokrotnienie, kopiowanie, obróbkę, opracowanie i powielanie wizerunku dowolną techniką bądź za pośrednictwem dowolnego medium dla potrzeb opublikowania we wskazanych celach.

Oświadczam, że wykorzystanie mojego wizerunku zgodnie z treścią niniejszego dokumentu nie narusza dóbr osobistych oraz innych praw osób trzecich.

Oświadczam, że zdjęcia zostały wykonane po uprzednim poinformowaniu i za moją zgodą.

Oświadczam, że niniejsza zgoda do wskazanych celów następuje bez ograniczeń czasowych i terytorialnych, w szczególności zgoda do wskazanych celów obejmuje także okres po ustaniu stosunku pracy.

Oświadczam, że jestem pełnoletni/-a i nieograniczony/-a w zdolności do czynności prawnych oraz, że zapoznałem/-am się z powyższą treścią i w pełni ją rozumiem.

Przeniesienie niniejszego zezwolenia oraz wszelkich praw z nim związanych na osobę lub podmiot trzeci nie wymaga mojej uprzedniej zgody na taką czynność i następuje nieodpłatnie.

.....

Podpis pracownika

Załącznik Nr 16 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Informacja dla zwolnionego pracownika dotycząca odbioru swojej dokumentacji po okresie przechowywania

W związku z rozwiązaniem stosunku pracy informujemy, że Pańska dokumentacja pracownicza będzie przechowywana u pracodawcy przez okres 10 lat, licząc od końca roku kalendarzowego, w którym stosunek racy uległ rozwiązaniu lub wygasł.

Po tym okresie może Pan w ciągu miesiąca odebrać swoja dokumentację, to jest do końca miesiąca kalendarzowego następującego po upływie okresu przechowywania dokumentacji, o którym mowa powyżej.

W przypadku nieodebrania dokumentacji we wskazanym terminie zostanie ona zniszczona w sposób uniemożliwiający odtworzenie jej treści.

Za Pracodawcę

.....

Załącznik Nr 17 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Zgoda i klauzula informacyjna przy formularzu rekrutacyjnym na stronie internetowej pracodawcy

„Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w dokumentach aplikacyjnych przez Politechnikę Łódzką z siedzibą w Łodzi w celu przeprowadzenia obecnego postępowania rekrutacyjnego oraz w kolejnych naborach kandydatów na pracowników Politechniki".

Oświadczenie dotyczące ochrony danych osobowych

Oświadczam, iż zostałem poinformowany o tym że:

1. administratorem danych osobowych przetwarzanych w ramach procesu rekrutacji jest Politechnika Łódzka, ..., ul. ....., 90-924 Łódź, jako pracodawca, za którego czynności z zakresu prawa pracy dokonuje .....
2. kontakt z Inspektorem Ochrony Danych jest możliwy pod adresem e-mail: rbi@adm.p.lodz.pl
3. dane osobowe kandydatów będą przetwarzane w celu przeprowadzenia obecnego postępowania rekrutacyjnego oraz w kolejnych naborach kandydatów na pracowników ..... na podstawie wyrażonej zgody (art. 6 ust. 1 lit. a RODO). Osobie, której dane dotyczą przysługuje prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
4. odbiorcą danych może być podmiot działający na zlecenie administratora danych, tj. podmiot świadczący usługi IT w zakresie serwisowania i usuwania awarii systemu informatycznego;
5. dane zgromadzone w procesach rekrutacyjnych będą przechowywane przez okres nie dłuższy niż do .....
6. osobie, której dane dotyczą przysługuje prawo dostępu do swoich danych osobowych, żądania ich sprostowania lub usunięcia. Wniesienie żądania usunięcia danych jest równoznaczne z rezygnacją z udziału w procesie rekrutacji prowadzonym przez Politechnikę Łódzką. Ponadto przysługuje jej prawo do żądania ograniczenia przetwarzania w przypadkach określonych w art. 18 RODO.
7. osobie, której dane dotyczą przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych na niezgodne z prawem przetwarzanie jej danych osobowych.
8. podanie danych zawartych w dokumentach rekrutacyjnych nie jest obowiązkowe, jednak jest warunkiem umożliwiającym ubieganie się o przyjęcie kandydata do pracy w Politechnice Łódzkiej.

Załącznik Nr 18 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Wniosek byłego pracownika o usunięcie danych ze strony

Niniejszym wnoszę o usunięcie moich danych osobowych (adres e-mail, imię i nazwisko wraz z nazwą stanowiska) ze strony internetowej pracodawcy, gdyż nie jestem już Państwa pracownikiem. W tej sytuacji nie istnieje podstawa do upubliczniania tego rodzaju danych.

Ponadto cofam zgodę na zamieszczenie mojego wizerunku na stronie internetowej jednostki uczelni w postaci zdjęcia zrobionego indywidualnie (np. podczas uroczystości rozdania nagród/ konferencji naukowych, itp.).

Podpis

Załącznik Nr 19 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Dane pracownika

Wniosek o usunięcie informacji zebranych przypadkowo

Proszę o usunięcie z wewnętrznego portalu informacyjnego (tzw. Intranetu) zamieszczonego tam mojego zdjęcia wykonanego na recepcji wraz z moim nazwiskiem, na co nie wyrażałem zgody. Zdjęcie zostało zrobione przypadkowo w trakcie wchodzenia na teren jednostki uczelni. Taka okoliczność powoduje, że może nastąpić naruszenie mojego dobra osobistego, w postaci naruszenia prawa do prywatności.

Usunięcia informacji proszę dokonać niezwłocznie. W przypadku niezrealizowania mojego żądania, wystąpię na drogę sądową ze stosownym powództwem.

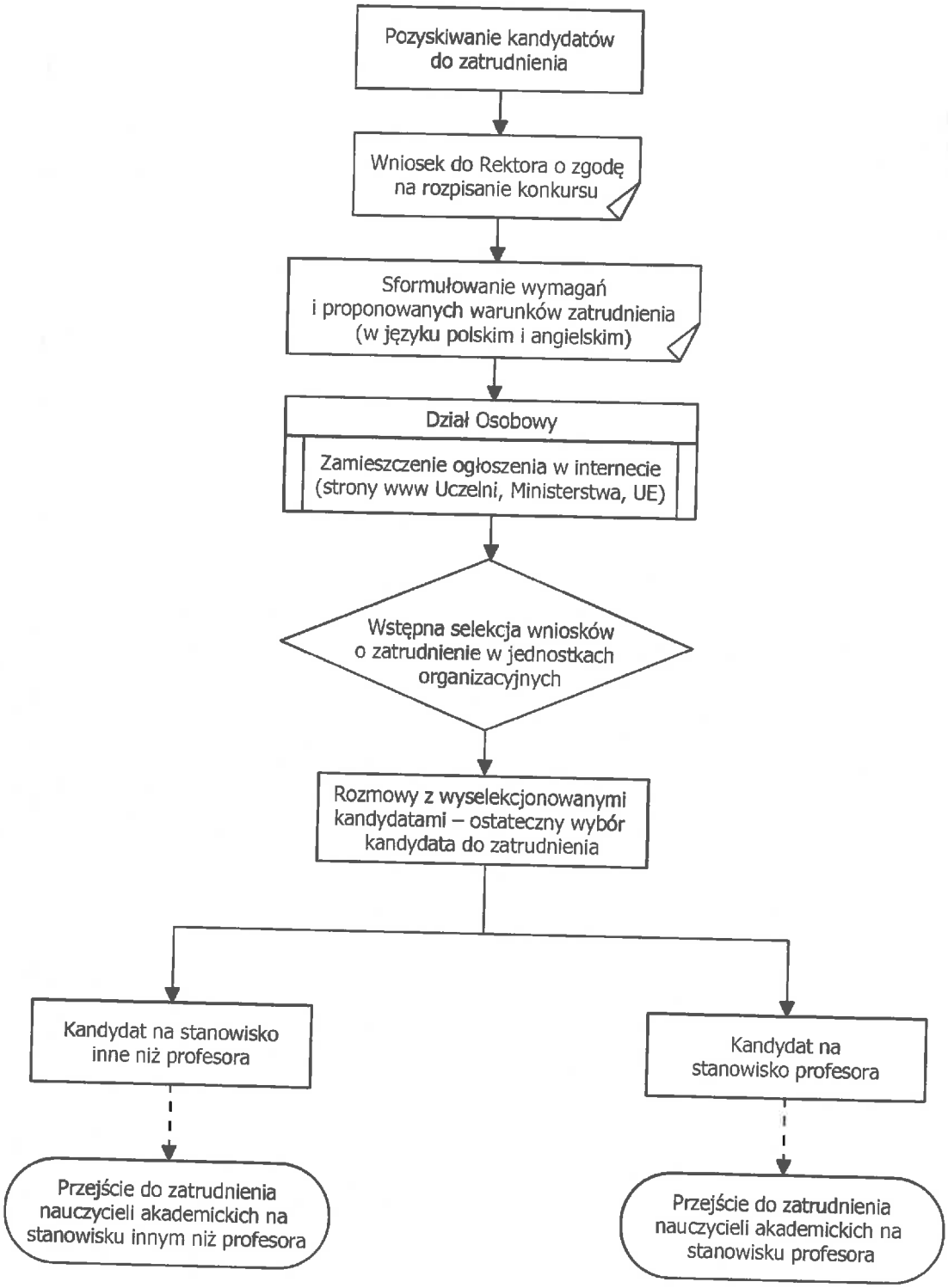
Podpis

.....

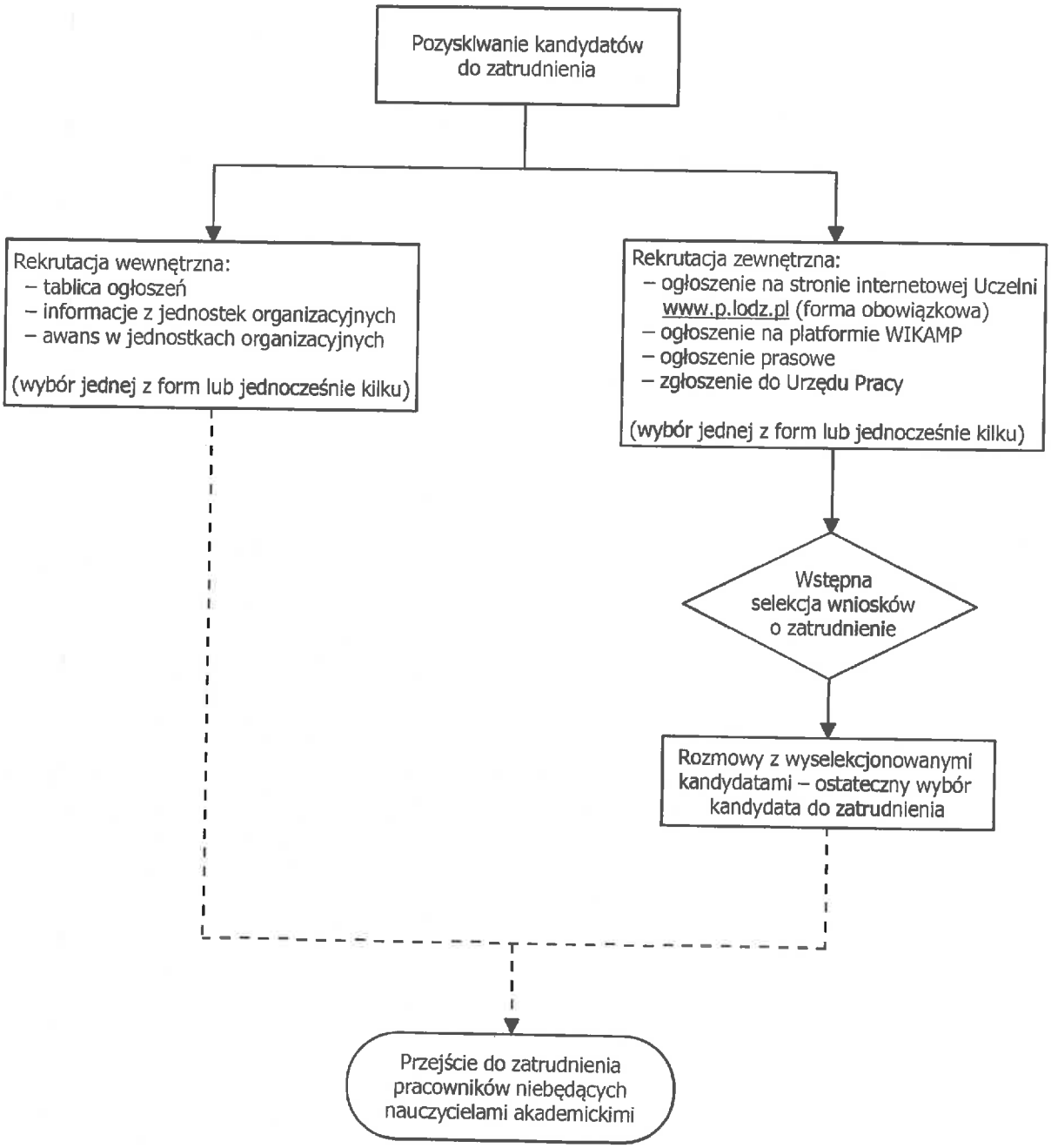
Otrzymują:

1) adresat
2) a/a

REKRUTACJA NAUCZYCIELI AKADEMICKICH



REKRUTACJA PRACOWNIKÓW NIEBĘDĄCYCH NAUCZYCIELAMI AKADEMICKIMI



Umowa o pracę, a dopuszczenie pracownika do pracy

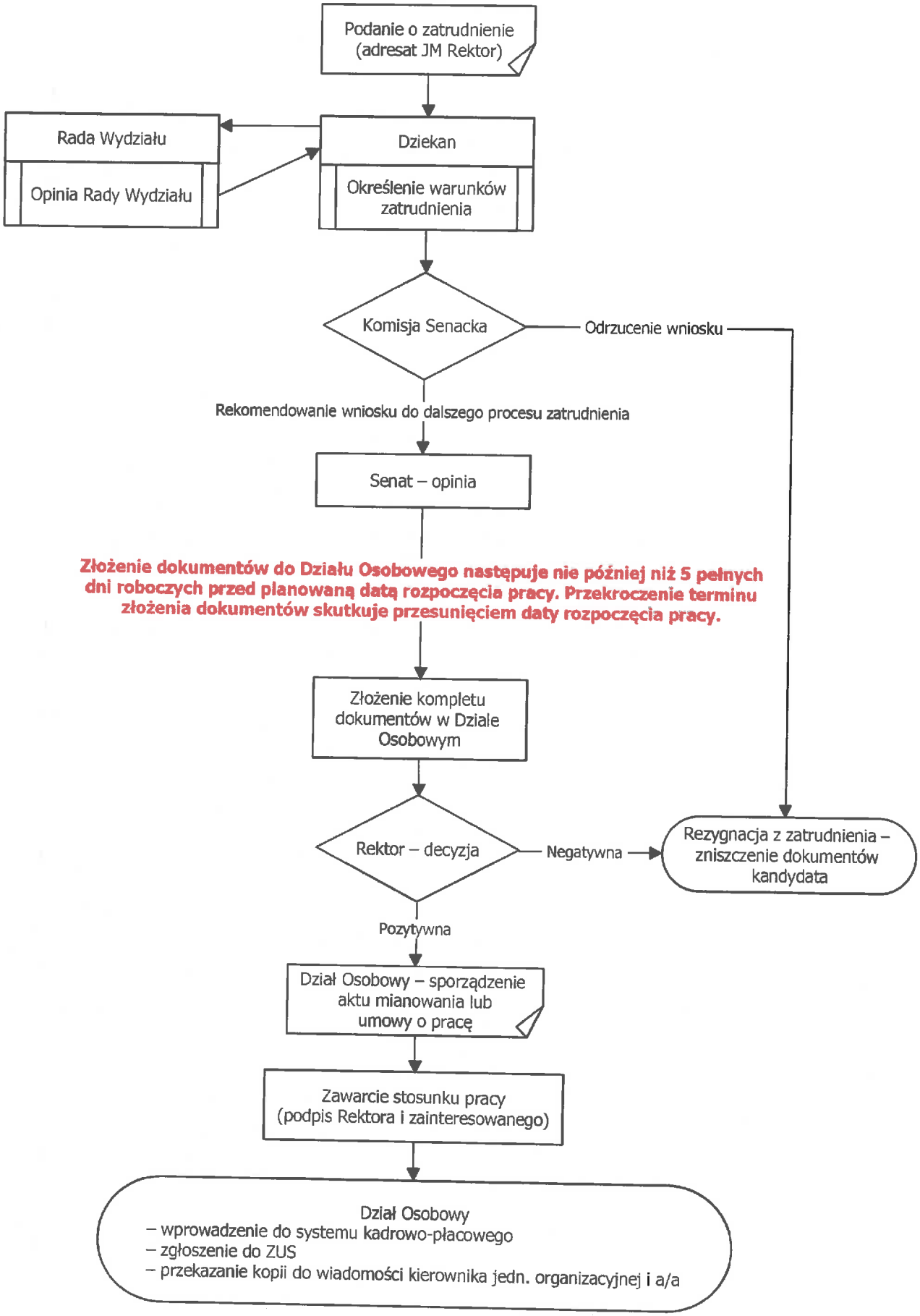
1. Zgodnie z art. 26 Kodeksu Pracy stosunek pracy nawiązuje się w terminie określonym w umowie jako dzień rozpoczęcia pracy, a jeżeli terminu tego nie określono – w dniu zawarcia umowy.
   Z powyższego wynika, że umowa o pracę jest czynnością prawną, która powoduje powstanie stosunku pracy między Stronami umowy.

   Dlatego też dopiero po zawarciu stosownej umowy o pracę kierownik jednostki organizacyjnej może dopuścić pracownika do pracy.

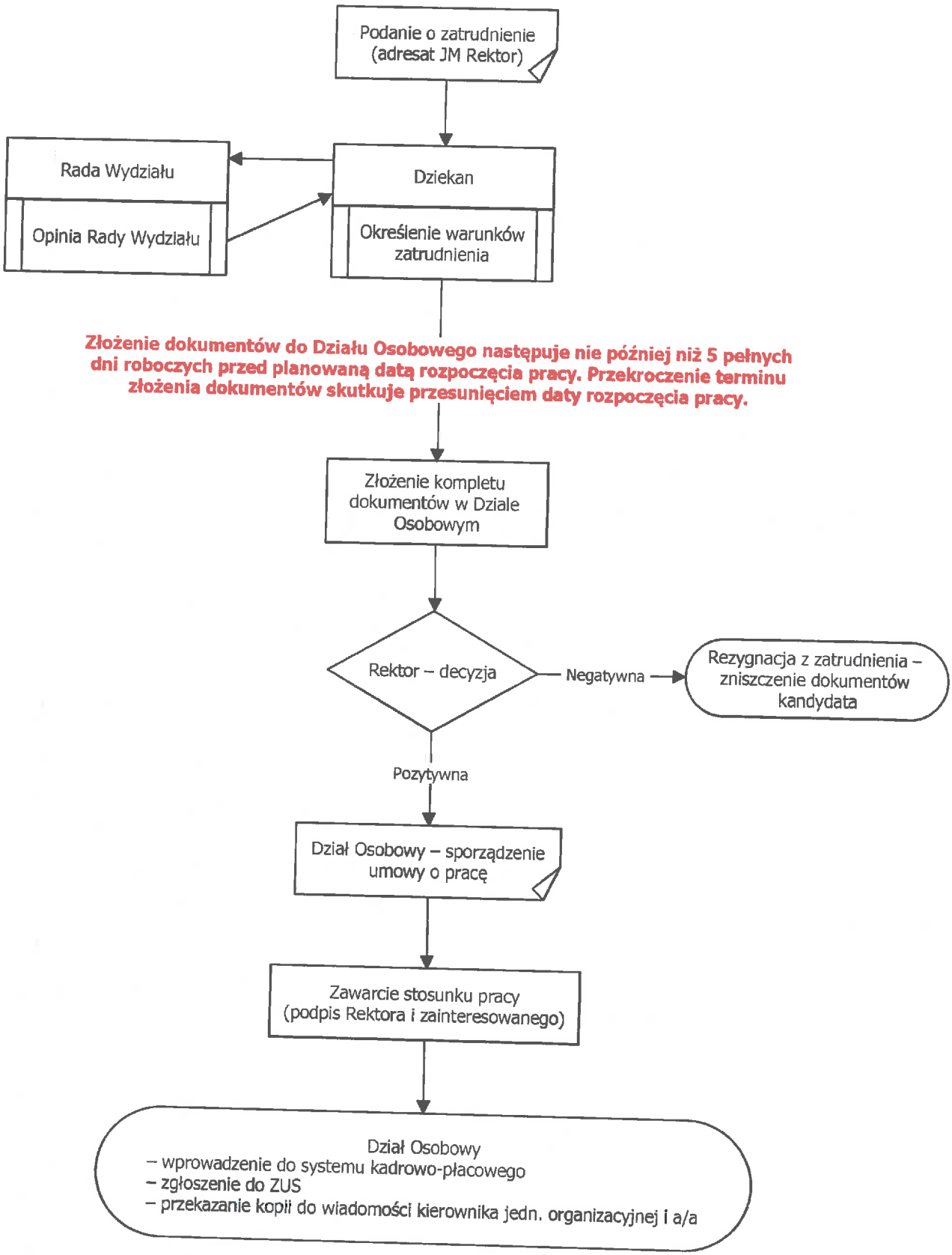
2. Art. 29 Kodeksu Pracy stanowi, że umowę o pracę zawiera się na piśmie. Jeżeli umowa o pracę nie została zawarta z zachowaniem formy pisemnej, to pracodawca powinien – najpóźniej w dniu rozpoczęcia pracy przez pracownika – potwierdzić pracownikowi na piśmie ustalenia co do stron umowy, rodzaju umowy oraz jej warunków.

3. Zgodnie z art. 229 § 4 Kodeksu Pracy pracodawca nie może dopuścić do pracy pracownika bez aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na określonym stanowisku.
   Okresowe i kontrolne badania lekarskie powinny być przeprowadzane w miarę możliwości w godzinach pracy przy zachowaniu przez pracownika prawa do wynagrodzenia.
   Całkowity koszt badania ponosi pracodawca.

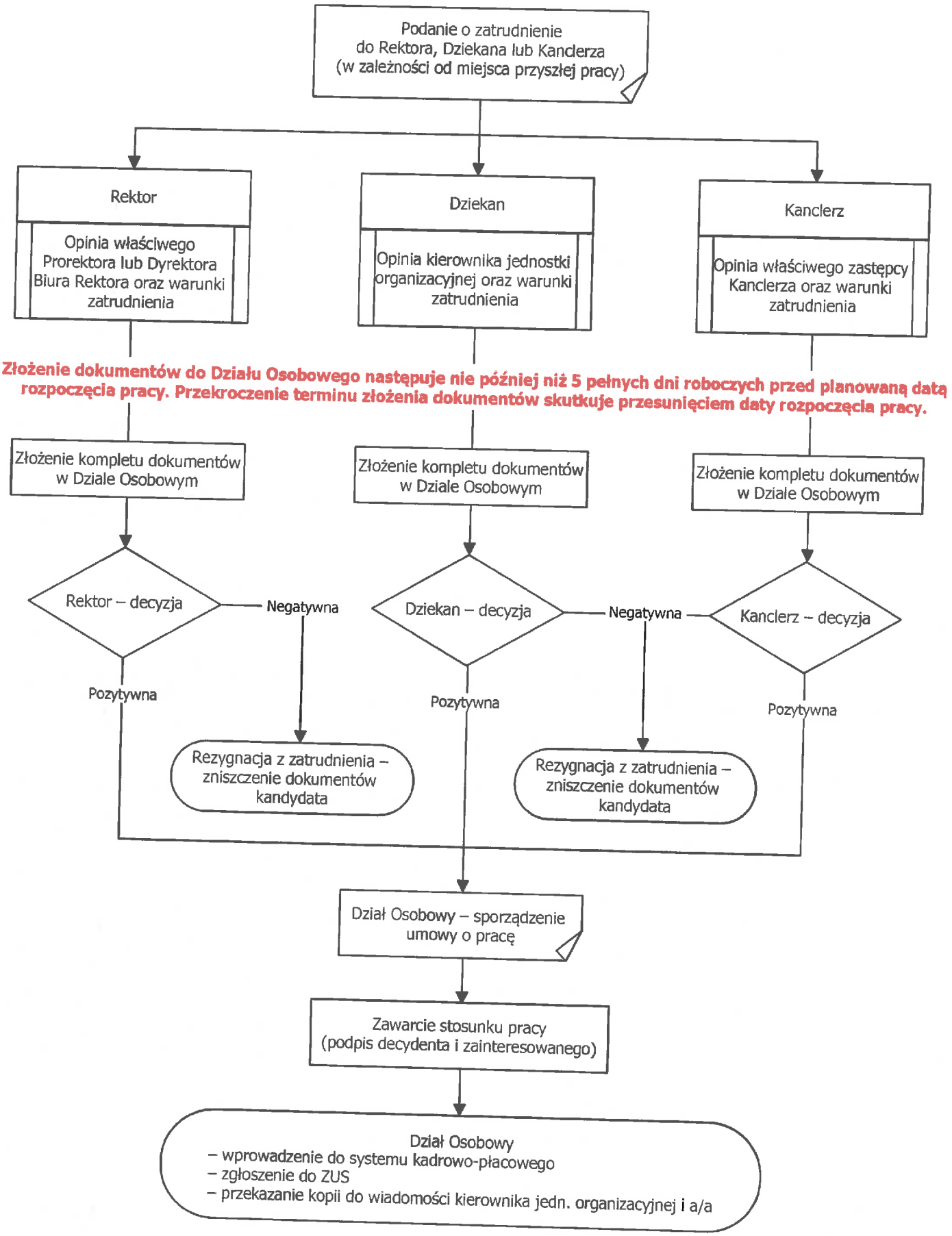
ZATRUDNIENIE NAUCZYCIELA AKADEMICKIEGO NA STANOWISKU PROFESORA



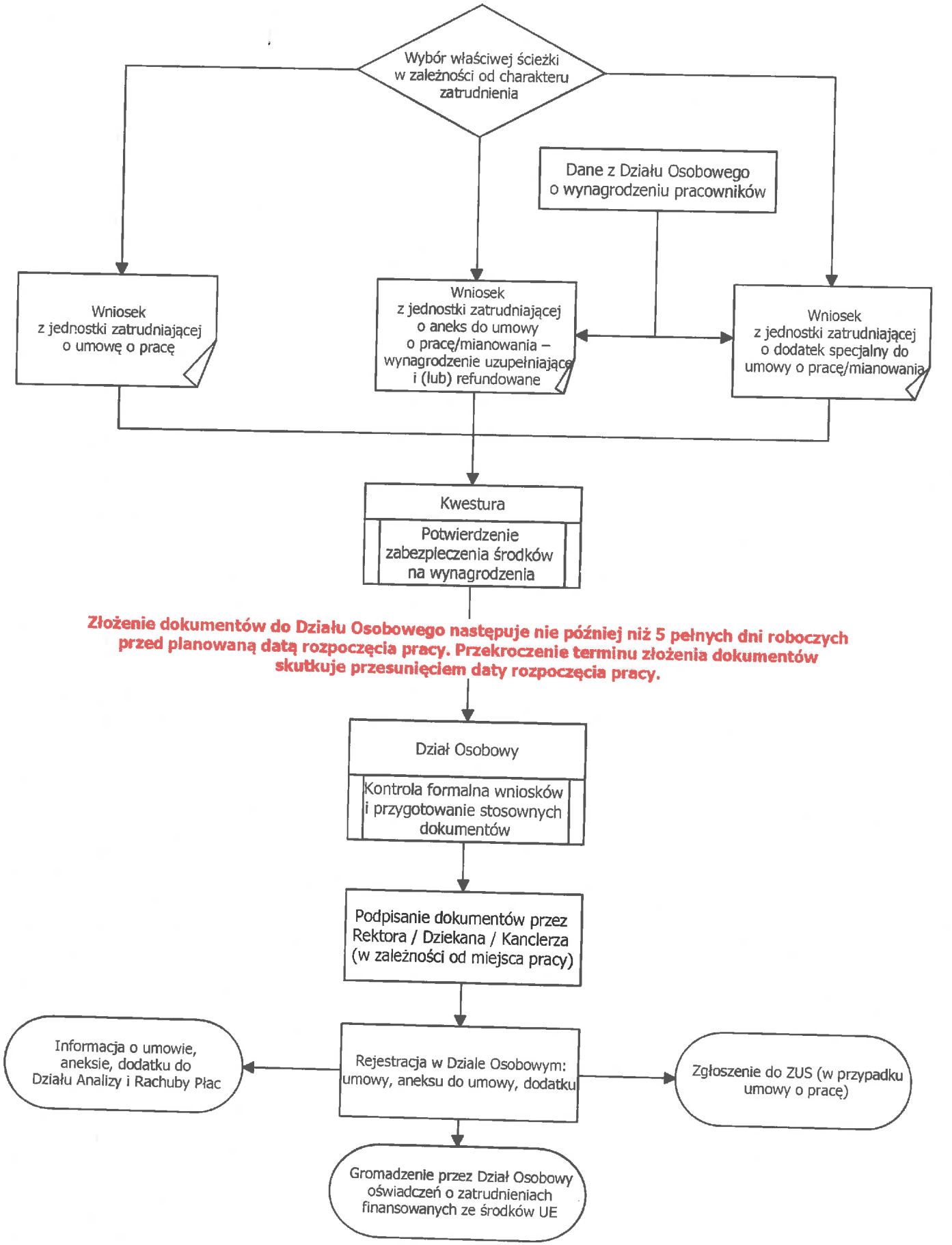
ZATRUDNIENIE NAUCZYCIELA AKADEMICKIEGO NA STANOWISKU INNYM NIŻ PROFESORA



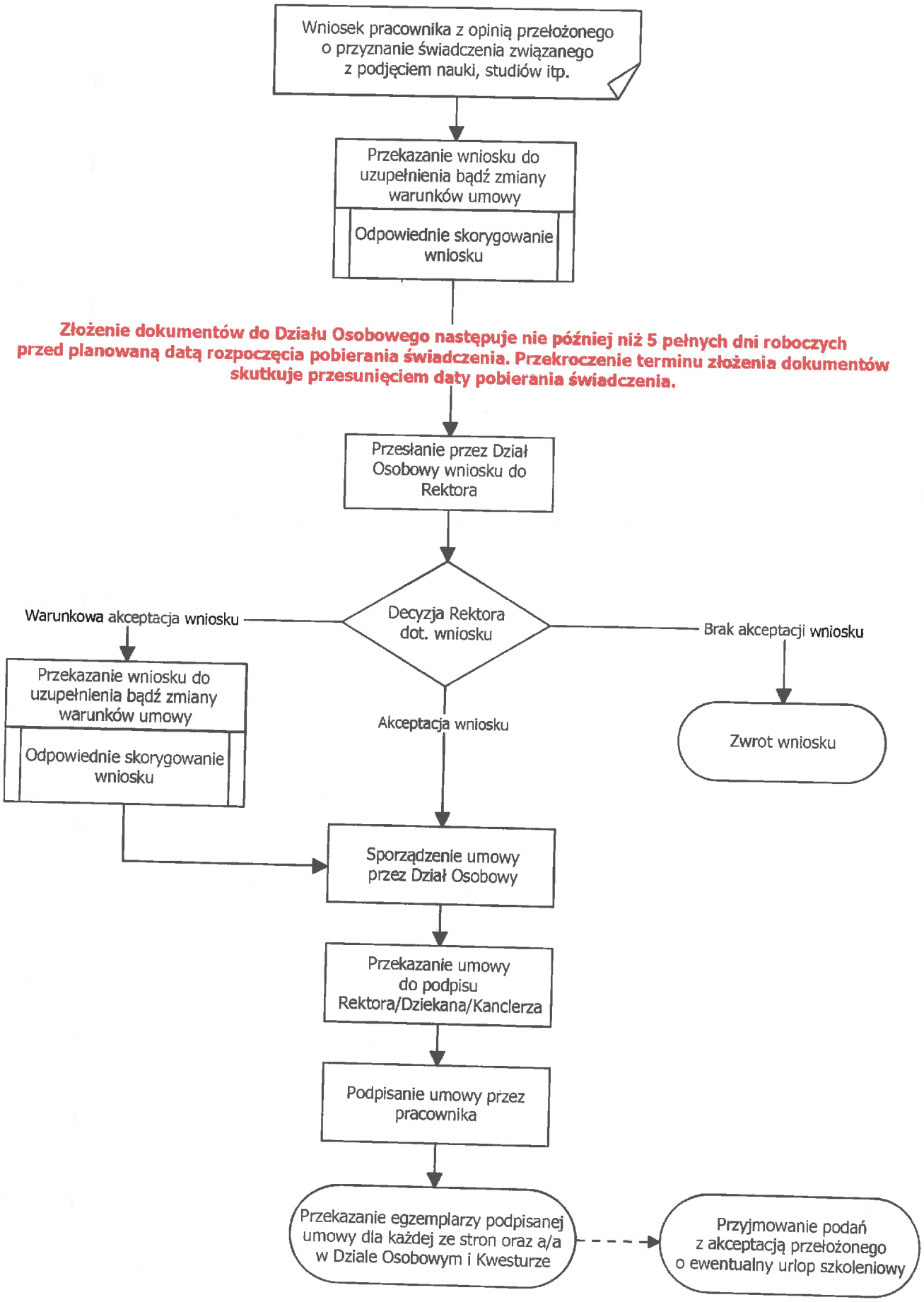
ZATRUDNIENIE PRACOWNIKA NIEBĘDĄCEGO NAUCZYCIELEM AKADEMICKIM



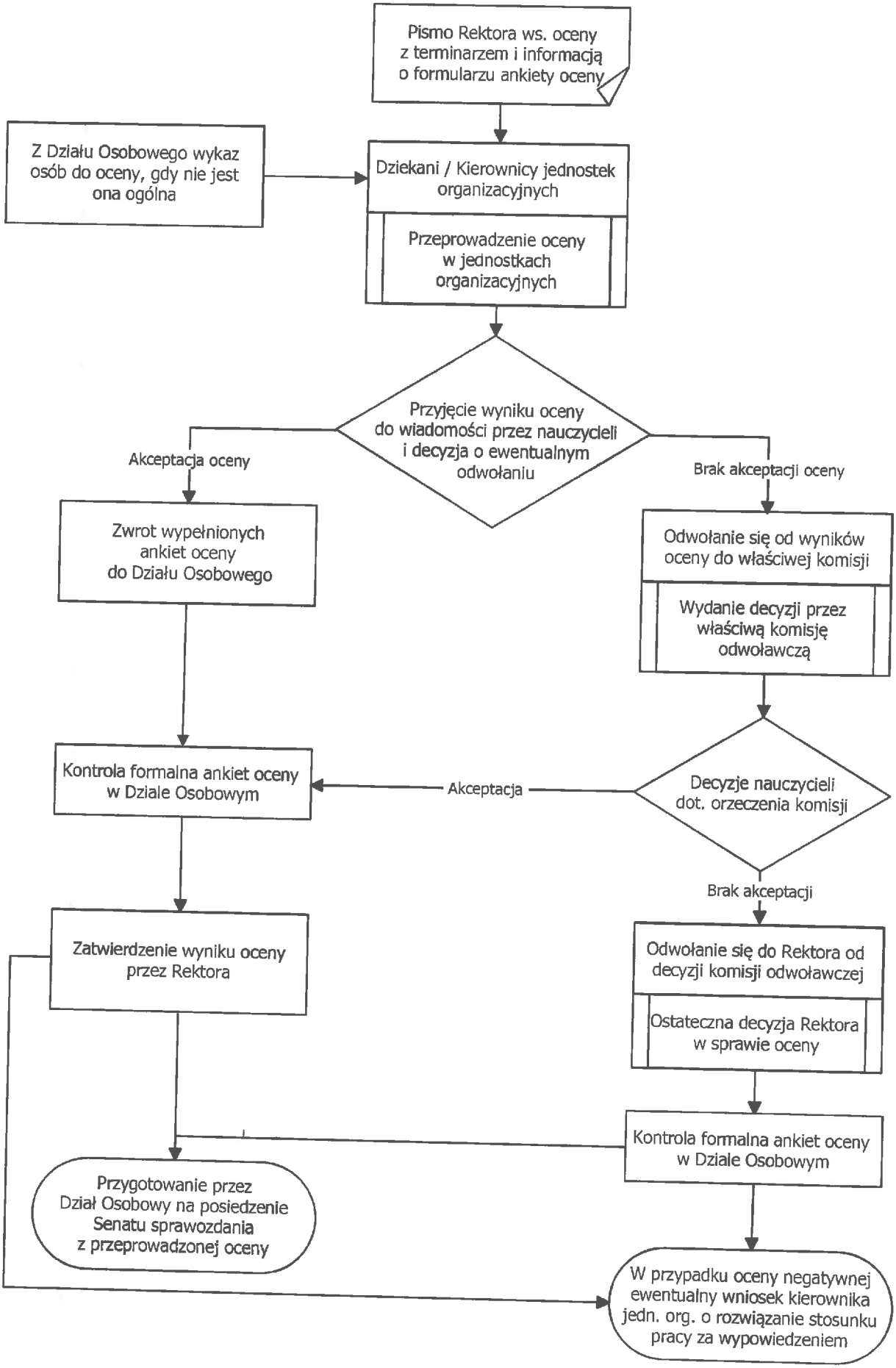
ZATRUDNIENIE – FINANSOWANIE POZABUDŻETOWE



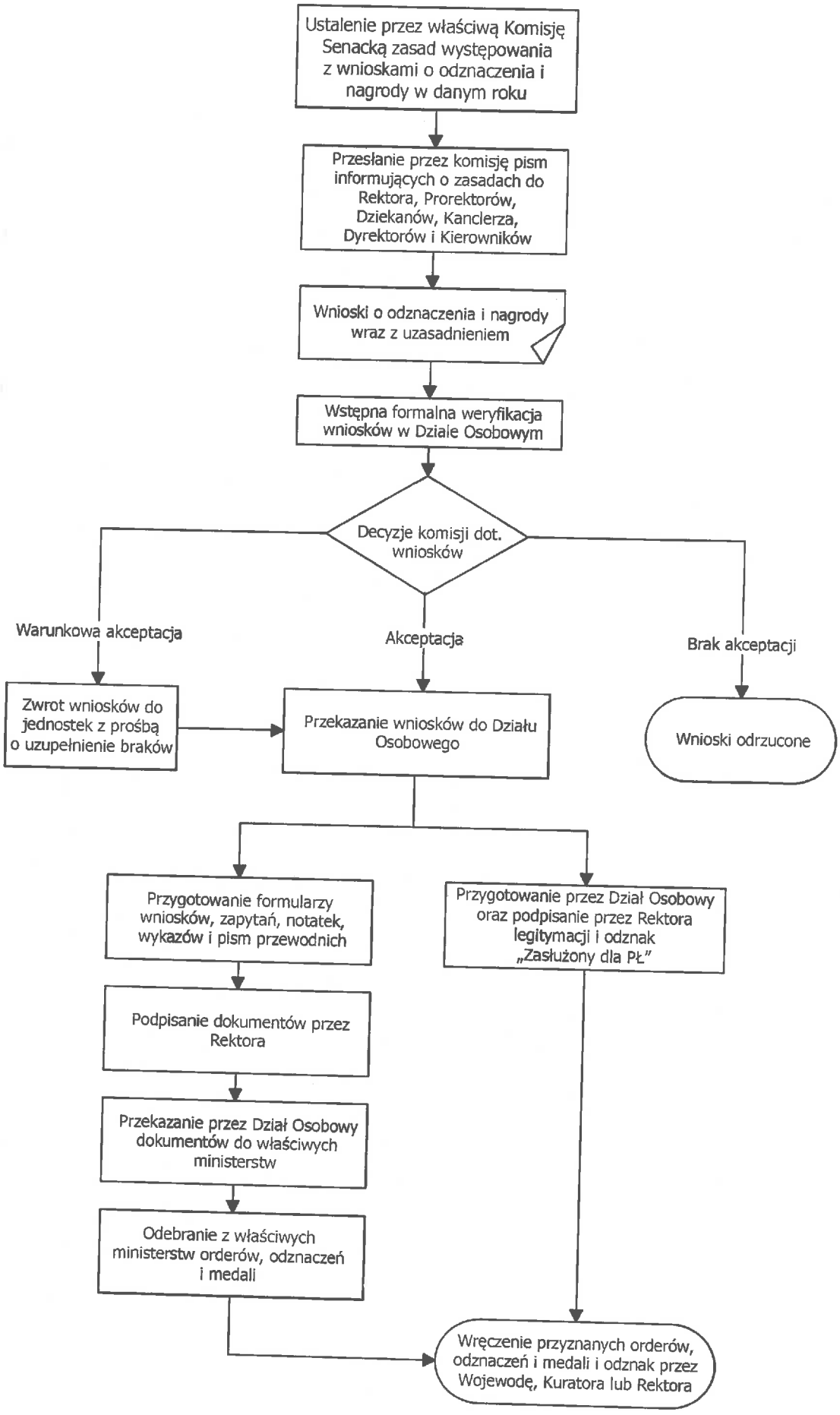
UMOWA O DODATKOWE ŚWIADCZENIA
W ZWIĄZKU Z PODNOSZENIEM KWALIFIKACJI ZAWODOWYCH



OKRESOWA OCENA NAUCZYCIELI AKADEMICKICH



ODZNACZENIA I NAGRODY



Załącznik nr 30 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Proces uwierzytelniania oraz zasady związane z ich zarządzaniem i użytkowaniem, stosowane metody i środki

1. Użytkownicy systemów informatycznych przetwarzających dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła, które są podstawową metodą uwierzytelnienia w sieci.
2. Identyfikator to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym; nie podlega zmianie.
3. Hasło to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym. Nowe hasło jest przekazywane użytkownikowi przez *ASI.*
4. Po zalogowaniu się po raz pierwszy po otrzymaniu hasła od *ASI*, użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet jeżeli system informatyczny nie wymusza takiego działania.
5. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:
   1) składać się z co najmniej 8 znaków,
   2) zawierać małe i wielkie litery oraz cyfry i znaki specjalne.
6. Hasło jest zmieniane przez użytkownika nie rzadziej, niż co 30 dni lub niezwłocznie w przypadku podejrzenia naruszenia poufności hasła.
7. Zarządzanie tworzeniem haseł do systemu informatycznego winno uwzględniać:
   1) nakaz zachowania w poufności haseł, które utraciły ważność,
   2) nakaz zmiany pierwszego hasła przy pierwszym logowaniu do systemu,
   3) bezwzględny zakaz przekazywania hasła innym użytkownikom,
   4) zakaz stosowania jako hasła wyrazu słownikowego lub ciągu tych samych znaków,
   5) zakaz stosowania jako hasła nazwy własnej lub powszechnie używanego słowa czy ciągu znaków, jak choćby nazwy, daty, imienia i nazwiska, numerów rejestracyjnych lub telefonu,
   6) nakaz, aby hasło zawierało maksymalnie trzy kolejne znaki w dowolnym położeniu, które są identyczne jak w poprzednio używanym haśle,
   7) zakaz używania identyfikatora użytkownika jako hasła,
   8) zakaz tworzenia haseł według klucza, tj. stałego układu powtarzających się, ale różnych elementów, np. cyfra roku + nazwa miesiąca,
   9) zakaz stosowania haseł już użytych,
   10) nakaz wprowadzania hasła do sytemu w sposób minimalizujący jego skopiowanie przez innych użytkowników systemu.
8. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ASI o wygenerowanie nowego hasła.
9. W przypadku haseł administracyjnych, na wypadek nieobecności osoby, której przysługują uprawnienia administracyjne hasło zostaje zapisane, ale jest przechowywane w zamkniętej, bezpiecznej kopercie umieszczonej w szafie przełożonego.

7. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał. Niedopuszczalne jest, aby dwóch lub więcej użytkowników wykorzystywało jedno konto.
8. Niedopuszczalne jest włączanie usług zapamiętywania identyfikatora lub hasła w przeglądarce internetowej albo innych programach komputerowych.

Załącznik nr 31 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Proces rozpoczynania, zawieszania i kończenia pracy użytkowników systemu informatycznego, w którym przetwarzane są dane osobowe

1. Rozpoczynając pracę w *systemie informatycznym*, w którym przetwarzane są dane osobowe użytkownik:
   1) włącza komputer, wprowadza niezbędne do pracy nazwę użytkownika, identyfikator i hasło,
   2) hasło powinno być wprowadzane w sposób minimalizujący ryzyko zapoznania się z nim przez osoby trzecie. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną, użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie bezpośredniego przełożonego,
   3) uruchamia program użytkowy,
   4) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, natychmiast kontaktuje się z *ASI* i przełożonym.
2. W przypadku niestandardowego zachowania systemu przetwarzającego dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie bezpośredniego przełożonego, informatyka, *ASI* oraz *IOD*.
3. Zawieszając pracę w systemie informatycznym (czasowe opuszczenie stanowiska pracy, bezczynność użytkownika na stacji roboczej) użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu sesji po wprowadzeniu hasła użytkownika. Hasło wygaszacza ekranu powinno być tożsame z hasłem używanym do uwierzytelniania.
4. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w tym pomieszczeniu nie przebywa inna upoważniona osoba. Zabronione jest pozostawianie bez nadzoru w takich pomieszczeniach osób nieupoważnionych.
5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo, np. w celu konserwacji sprzętu. Planowe zawieszenie prac jest poprzedzone informacją skierowaną do pracowników przez *ASI* (w formie wiadomości email lub osobiście) na co najmniej 1 dzień przed planowanym zawieszeniem.
6. Kończąc pracę w systemie informatycznym, pracownik wylogowuje się ze wszystkich systemów i aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza informatyczne nośniki danych, wydruki lub dokumenty papierowe zawierające dane osobowe, sprawdza czy zostały one zdjęte z otwartych regałów, stołów, biurek i umieszczone na przechowanie w szafie zamykanej na klucz. W przypadku gdy jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, zamyka na klucz drzwi do pomieszczenia oraz zdaje klucz na portiernię.

Załącznik nr 32 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Proces tworzenia i przechowywania kopii zapasowych oprogramowania

i plików zawierających dane osobowe

1. Dla wszystkich danych osobowych przetwarzanych w zasobach danych oraz dla oprogramowania służącego do przetwarzania tych danych należy wykonywać kopie zapasowe.
2. W przypadku *systemów informatycznych* służących do przetwarzania danych osobowych administrowanych przez Centrum Komputerowe, jak i innych systemów używanych do przetwarzania danych osobowych obowiązują zasady tworzenia kopii zapasowych opisane poniżej.
3. Pliki zawierające dane osobowe powinny znajdować się na dyskach serwerów lub na dyskach twardych komputerów, gdzie podlegają ochronie przez mechanizmy bezpieczeństwa systemu operacyjnego oraz w postaci kopii zapasowych.
4. Proces tworzenia kopii zapasowych musi być skonfigurowany w taki sposób, aby w razie awarii możliwe było pełne odtworzenie systemu.
5. Zasady tworzenia kopii zapasowych i archiwizacji systemów informatycznych oraz danych osobowych przetwarzanych w systemie informatycznym :
    a) kopia zapasowa aplikacji przetwarzającej dane osobowe, wykonywana jest na bieżąco przed i po wprowadzeniu istotnych zmian prowadzących do zmiany wersji aplikacji i jest zapisywana na nośnikach przenośnych nie podłączonych do źródła zasilania, przechowywanych w innej lokalizacji ustalonej odpowiednio przez *ASI* lub specjalistę IT z ich bezpośrednimi przełożonymi;
    b) archiwizacja przeprowadzana jest automatycznie (na bieżąco) w godzinach wieczornych i nocnych przy pomocy wbudowanych funkcji w system. Przed uruchomieniem archiwizacji wszystkie procesy niewylogowanego *użytkownika* usuwane są z systemu. *ASI* informuje *ABI* o fakcie braku wylogowania i nie zamknięciu procesów przez zalogowanego użytkownika po zakończeniu korzystania z systemu/komputera;
    c) kopia zapasowa danych lub zmian konfiguracyjnych *systemu informatycznego* służącego do przetwarzania danych osobowych, w tym uprawnień *użytkowników* systemu, wykonywana jest codziennie. Pełna kopia nie rzadziej niż raz w miesiącu. Pozostałe kopie mogą być wykonywane jako kopie różnicowe;
    d) publikowane treści w uczelnianym Biuletynie Informacji Publicznej, zapisane w bazach danych powinny być zabezpieczone poprzez wykonywanie kopii zapasowej nie później niż dobę po ich opublikowaniu lub zmianie danych. Jeżeli zmiany zachodzą częściej niż raz na dobę, kopia zapasowa powinna być wykonywana raz na dobę;
    e) w stosunku do *systemów informatycznych* administrowanych przez Centrum Komputerowe oraz w przypadku innych systemów, za tworzenie i przechowywanie kopii zapasowych danych osobowych odpowiadają wyznaczeni przez bezpośrednich przełożonych *Administratorzy Systemów Informatycznych*;
    f) bezpośredni dostęp do kopii zapasowych mogą mieć tylko imiennie wyznaczone osoby, aplikacje i systemy odpowiedzialne za realizację procedur ochrony danych;
    g) kopie bezpieczeństwa danych osobowych po ustaniu ich użyteczności winny być bezzwłocznie usuwane, a te które uległy uszkodzeniu lub stały się nieprzydatne pozbawia się zapisu danych albo niszczy w stopniu uniemożliwiającym ich odczytanie; proces ten jest dokumentowany przez *ASI* w dzienniku pracy systemu;

h) zaleca się, aby kopie danych przechowywać na nośnikach, dla których nadal są dostępne mechanizmy odczytu informacji;

i) co najmniej jedna z kopii zapasowych zbioru danych powinna być przechowywana w innym budynku niż podstawowa instalacja systemu, to jest w innym budynku niż zbiory danych eksploatowane na bieżąco, w miejscu bezpiecznym, zapewniającym ochronę przed dostępem osób nieuprawnionych, modyfikacją, uszkodzeniem, zniszczeniem oraz wpływem środowiska;

j) przenośne (nie podłączone) nośniki zawierające kopie zapasowe są odpowiednio oznaczone i przechowywane w zamykanej szafie metalowej, mieszczącej się w siedzibie uczelni.
W sytuacji, gdy kopię przechowuje się na innym serwerze procedura powinna ten fakt uwzględnić;

k) za wykonywanie kopii zapasowych danych osobowych znajdujących się na dyskach lokalnych stacji roboczych oraz komputerów przenośnych odpowiada *użytkownik* danego komputera lub lokalny informatyk/specjalista IT.

6. Centrum Komputerowe opracowuje harmonogram wykonywania kopii zapasowych dla bazy danych dostępny dla wszystkich *ASI.*
7. Za zapewnienie prawidłowego odczytu danych z kopii zapasowych odpowiada *ASI.*
8. Zaleca się wykonywanie okresowych testów odtwarzania kopii zapasowych oraz testowanie wszystkich kopii bezpieczeństwa przynajmniej raz na rok. Okresową weryfikację kopii bezpieczeństwa (testowanie) pod kątem ich poprawności odtworzenia przeprowadza *ASI.* Z czynności tych *ASI* sporządza protokół potwierdzający wykonanie testów.

Załącznik nr 33 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Realizacja praw osób, których dane dotyczą

Wprowadzenie

Na podstawie dotychczas obowiązujących przepisów oraz przepisów RODO ukształtował się standard ochrony interesów jednostki polegający na tym, że do osoby, której dane dotyczą należy wybór, czy będzie ona korzystać czy też nie z uprawnień przyznanych jej w przepisach RODO, z wyłączeniem prawa do bycia poinformowanym realizowanego przez administratora danych przy zbieraniu danych.

Przynależny wybór korzystania z przysługujących praw może zostać ograniczony ze względu na potrzebę zapewnienia bezpieczeństwa publicznego.

Prawo do wyrażenia i wycofania zgody na przetwarzanie danych

Zgoda, to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, zrealizowane w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie danych osobowych.

Decyzja o wyrażeniu zgody na przetwarzanie danych osobowych powinna być podjęta w sposób nieprzymuszony, a osoba ją wyrażająca ma mieć pełną wiedzę o tym, jakie jej dane osobowe będą przetwarzane, przez kogo, w jakim celu i w jakim zakresie.

Na kierowniku jednostki pozyskującego zgodę od osoby, spoczywa ciężar dowodu wykazania, że zgoda jest udzielona zgodnie z prawem, dlatego winien archiwizować zgody wyrażone przez wszystkie osoby wraz z zapytaniem, które zostało skierowane do osoby potwierdzające, że adresat pytania, był w stanie wywnioskować, jakie dane i w jakim celu będą przetwarzane.

Wystarczające jest, by osoba udzielająca zgodę była w stanie określić, jakie konkretnie dane są przetwarzane w danym celu. W przypadku gdy przetwarzanie ma służyć kilku różnym celom, niezbędna jest zgoda na wszystkie cele.

Pozyskiwanie zgody w PŁ dla celów pracowniczych jest zawsze obarczone brakiem dobrowolności ze względu na brak równowagi w relacji pracodawca – pracownik. Podobną nierównowagę można zauważyć w przypadku nauczyciel – student.

Pozyskiwanie zgody jako przesłanki legalności w PŁ jako uczelni publicznej może mieć miejsce w wyjątkowych sytuacjach, na przykład wtedy, gdy przetwarzanie danych odbywa się w innym celu niż realizacja obowiązków wynikających z przepisów prawa.

Każda osoba ma prawo w dowolnym momencie cofnąć wyrażoną zgodę, co nie wpływa na legalność przetwarzania danych na podstawie zgody przed jej wycofaniem, a cofnięcie zgody powinno być równie łatwe jak jej pozyskanie.

Kierownik jednostki konsultuje z IOD treść klauzuli zgody.

Informowanie – obowiązek PŁ

Przepisy RODO w ramach zasady przejrzystości zobowiązują administratora danych do przekazywania wszelkich informacji podczas pozyskiwania danych osobowych od podmiotów danych w sposób

umożliwiający im zrozumienie kierowanych do nich komunikatów. Podmiot danych nie może zrzec się uprawnienia do otrzymania informacji.

Przygotowana wcześniej treść klauzuli informacyjnej może być wykorzystywana w wielu sytuacjach, w ramach tożsamych celów przetwarzania danych osobowych, bez konieczności indywidualizacji pod kątem konkretnego podmiotu danych.

PŁ jako administrator ma obowiązek przekazać następujące informacje:

1. Tożsamość PŁ, dane adresowe
2. Cele oraz podstawę prawną przetwarzania
3. Okres, przez który dane osobowe będą przechowywane
4. Prawo żądania od ADO dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawie wniesienia sprzeciwu wobec przetwarzania , prawie do przenoszenia danych
5. Prawie wniesienia skargi do PUODO
6. Czy podanie danych jest wymogiem ustawowym lub umownym oraz czy osoba jest zobowiązana do ich podania i jakie są konsekwencje niepodania danych
7. Dane kontaktowe IOD

Obowiązek informacyjny w PŁ realizuje kierownik działu osobowego zapoznając pracowników zatrudnianych na umowę o pracę. Natomiast pracownicy będący stroną umowy cywilnoprawnej są informowani przez kierowników jednostek zawierających takie umowy.

Treść klauzuli informacyjnej opracowuje IOD.

<u>Prawo do poinformowania w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą</u>

W przypadku pozyskiwania danych nie od osoby, której dane dotyczą taki obowiązek powinien być zrealizowany w rozsądnym terminie po otrzymaniu danych osobowych, na przykład po ich zapisaniu w dokumencie lub na nośniku informatycznym.

Dane osobowe można pobierać w PŁ zgodnie z prawem nie tylko bezpośrednio od osoby, której dane dotyczą (tzw. podmiotu danych), ale także z wielu innych źródeł, w tym na przykład dane mogą być udostępnione przez innego administratora danych, mogą być zbierane automatycznie z ogólnodostępnych stron WWW, skrzynek pocztowych czy portali internetowych, mogą być również pobierane ze źródeł powszechnie dostępnych (np. książek telefonicznych, rejestrów) oraz mogą być pozyskiwane od innych osób fizycznych.

Podmiot danych musi poznać nazwę administratora wraz danymi kontaktowymi, cel przetwarzania, okres przechowywania, także informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu i jego konsekwencjach. Ponadto taka osoba musi być poinformowana o prawie dostępu do swoich danych, ich sprostowaniu, usunięciu lub ograniczeniu przetwarzania, prawo do wniesienia sprzeciwu i przenoszeniu danych.

Pozyskując dane z innych źródeł przekazać należy osobie informacje o podstawie prawnej przetwarzania oraz zakresie danych. Jeśli przetwarzanie danych wrażliwych podlega obowiązkowi informacyjnemu w klauzuli informacyjnej winne one być wyraźnie oznaczone. Tworząc klauzulę informacyjną kierownik jednostki uwzględnić musi fakt, że nie zawsze będzie ona mogła być wielokrotnego użytku; stąd wymóg konsultacji z IOD i weryfikacji treści przekazywanych tylko w przypadkach, gdy ma to zastosowanie.

Niezależnie od sposobu spełnienia obowiązku tego wtórnego informacyjnego (ustnie, telefonicznie, na piśmie czy drogą elektroniczną) PŁ/kierownik jednostki zapewnia możliwość wykazania, że obowiązek został spełniony wobec każdej konkretnej osoby.

Jeśli spełnienie obowiązku informacyjnego wymagałoby niewspółmiernie dużego wysiłku, możliwe jest zwolnienie z tego obowiązku. Jednak niespełnienie obowiązku informacyjnego może prowadzić do poważnej odpowiedzialności finansowej PŁ, chyba że udowodni, że nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

Prawo dostępu przysługujące osobie, której dane dotyczą

Każda osoba fizyczna, która ma podstawy do tego, by przypuszczać, że jednostka PŁ przetwarza jego dane osobowe może wystąpić z żądaniem informacyjnym. Wystąpienie o udzielenie informacji czy dostarczenie kopii może być w dowolnej formie i nie jest warunkowane wykazaniem interesu prawnego czy faktycznego. Nie musi być także popierane argumentacją czy uzasadnieniem.

IOD realizujący wniosek o dostęp do danych weryfikuje tożsamość osoby, która domaga się informacji o przetwarzaniu danych bądź kopii danych. W przypadku uzasadnionych wątpliwości co do tożsamości wnioskodawcy można zażądać dodatkowych informacji niezbędnych do jej potwierdzenia.

Osoba, której dane dotyczą jest uprawniona do uzyskania następujących informacji: cele przetwarzania, kategorie odnośnych danych, informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, planowany okres przechowywania (w miarę możliwości), informacje o prawie sprostowania, usunięcia lub ograniczenia przetwarzania, wniesienia sprzeciwu i skargi, wszelkie dostępne informacje o źródle informacji, informacje o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu.

PŁ/kierownik jednostki dostarcza kopię danych (odtworzenie oryginału danych), które są przetwarzane na wniosek osoby, której dane dotyczą precyzujący informacje lub czynności przetwarzania, których dotyczy żądanie.

Prawo do usunięcia danych - do bycia zapomnianym

Usunięcie danych jest działaniem nieodwracalnym w odróżnieniu od zaprzestania przetwarzania we wskazanym celu, istotnym przede wszystkim w sferze nowych technologii planowanych do wykorzystania w jednostkach PŁ.

Skorzystanie z prawa do żądania usunięcia danych przez jednostki przetwarzające jest możliwe tylko w przypadku zaistnienia następujących przesłanek:

1. pierwsza przesłanka zobowiązuje do usunięcia danych, gdy nie są one już niezbędne do osiągnięcia celów, w których zostały zebrane;
2. druga przesłanka dotyczy cofnięcia zgody, na podstawie której jest dokonywane przetwarzanie danych i jednocześnie brakuje innej podstawy prawnej;
3. trzecią przesłanką jest złożenie sprzeciwu wobec przetwarzania jej danych na podstawie uzasadnionego interesu administratora;
4. czwartą przesłanką jest przetwarzanie danych niezgodnie z prawem;
5. piąta stanowi o konieczności usunięcia danych wynikającej z obowiązku prawnego określonego w prawie, np. prawie o szkolnictwie wyższym i nauce.

Przypadkami uzasadniającymi odmowę usunięcia danych są: konieczność wywiązania się PŁ z prawnego obowiązku wynikającego z ustawy, względy interesu publicznego (w tym powszechnej opieki zdrowotnej), niezbędność przetwarzania dla celów archiwalnych, dochodzenie lub obrona roszczeń, przetwarzanie do celów badań naukowych. Niemożliwe jest uwzględnienie wniosku o usunięcie danych, gdy ich dalsze przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji.

Jednostka PŁ, do której zwróciła się osoba z żądaniem usunięcia danych, powinna po konsultacji z IOD poinformować tę osobę o usunięciu danych w zakresie, w jakim przetwarza jej dane osobowe, a także wskazać, które jednostki i/lub podmioty trzecie również przetwarzają takie dane osobowe.

Ograniczenie przetwarzania danych osobowych

Ograniczenie przetwarzania pozwala osobie fizycznej w określonych okolicznościach na zablokowanie przetwarzania swoich danych przez PŁ, z wyjątkiem ich przechowywania, ale bez definitywnej utraty danych. Wykonanie tego praw pozwala osobie na ograniczenie rozpowszechniania jej danych, zwłaszcza nieprawdziwych lub nieaktualnych.

Ograniczenie przetwarzania polega na zawieszeniu wykonywania aktywnych operacji na danych, co w praktyce oznacza niemożliwość korzystania z danych przez PŁ, która musi rozważyć zaniechanie dokonywania jakichkolwiek dalszych operacji na danych. W konsekwencji należy oznakować i wyodrębnić przechowywane dane osobowe w celu niepodejmowania operacji przetwarzania w przyszłości.

Uprawnienie żądania ograniczenia przetwarzania danych może mieć miejsce w następujących okolicznościach:

1. osoba kwestionuje prawidłowość swoich danych osobowych – PŁ zaprzestaje przetwarzania na okres konieczny do sprawdzenia prawidłowości przetwarzanych danych;
2. przetwarzanie jest niezgodne z prawem, a osoba sprzeciwia się usunięciu danych żądając w zamian ograniczenia ich wykorzystania;
3. PŁ nie potrzebuje już danych osobowych do celów przetwarzania, jednak są one potrzebne osobie do ustalenia, dochodzenia lub obrony roszczeń;
4. osoba wniosła sprzeciw wobec przetwarzania – ograniczenie następuje do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie PŁ są nadrzędne wobec podstaw sprzeciwu.

Wśród metod pozwalających PŁ ograniczyć przetwarzanie mogą być, m.in. czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikowi dostępu do wybranych danych lub czasowe usunięcie opublikowanych danych ze strony internetowej.

Prawo do przenoszenia danych osobowych

Osoba, której dane dotyczą korzysta z uprawnienia otrzymania w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego, tylko tych danych osobowych jej dotyczących, które przekazała PŁ. Osoba ma także prawo otrzymania danych w celu przesłania innemu administratorowi, a także prawo żądania przesłania tych danych osobowych bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Do danych podlegających prawu do przenoszenia można zaliczyć wszelkie dane podawane przez podmiot danych podczas zawierania umowy, składania zamówień, wypełniania formularzy rejestracyjnych lub kontaktowych, takie jak: imię, nazwisko, nazwa użytkownika, adres zamieszkania, adres poczty elektronicznej, numer telefonu, wiek. Rozszerzona lista zawiera listy adresowe z aplikacji poczty e-mail, wiadomości e-mail, informacje dotyczące transakcji bankowych, logi dostępowe, historie wyszukiwania osoby, dane o ruchu, lokalizacyjne, dane poddane pseudonimizacji o ile można je wyraźnie powiązać z osobą, np. poprzez identyfikator..

Nie podlegają przenoszeniu dane anonimowe, ani zanonimizowane w taki sposób, że osób w ogóle już nie można zidentyfikować.

Zrealizowanie wniosku osoby do przeniesienia jej danych innemu administratorowi zależy od spełnienia kumulatywnie trzech warunków: 1) przetwarzanie odbywa się na podstawie zgody lub umowy; 2) przetwarzanie odbywa się w sposób zautomatyzowany; 3) prawo do przenoszenia nie wpływa niekorzystnie na prawa i wolności innych.

PŁ dąży do opracowania interoperacyjnych formatów przechowywania i udostępniania danych osobowych, które umożliwiają przenoszenie danych w ramach Europejskich Ram Interoperacyjności.

Sprzeciw wobec przetwarzania danych osobowych

Podmiot danych ma prawo do sprzeciwu wobec przetwarzania danych ze względu na szczególną sytuację oraz wobec marketingu bezpośredniego, w tym profilowania.

Szczególna sytuacja jest przesłanką sprzeciwu wtedy, gdy wykonywanie zadania jest w interesie publicznym oraz gdy przetwarzanie realizuje prawnie uzasadnione interesy PŁ. Nie można się powołać na szczególną sytuację, gdy przetwarzanie jest realizacją obowiązku prawnego przez PŁ.

Prawo do sprzeciwu wobec marketingu i profilowania jest bezwarunkowe, nie wymaga uzasadnienia i nie istnieją warunki, które mogłyby stanowić podstawę odrzucenia sprzeciwu; sprzeciw klienta wyklucza stosowanie wobec niego marketingu niezwłocznie po złożeniu tego sprzeciwu.

Skutkiem sprzeciwu wobec przetwarzania danych osobowych jest alternatywnie usuniecie danych albo ograniczenie przetwarzania.

Uprawnienie do uzyskania informacji o naruszeniu ochrony danych

Kierownicy jednostek PŁ, w których miało miejsce naruszenie zasad ochrony danych mają obowiązek poinformowania JM Rektora oraz IOD o fakcie naruszenia, który po rozpatrzeniu sprawy informuje PUODO oraz osoby, których dane dotyczą w celu ograniczenia negatywnych konsekwencji, jakie może pociągać za sobą naruszenie.

Naruszenie obowiązków dotyczących zabezpieczenia danych, które powoduje skutki przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych jest podstawą oceny, czy doszło do incydentu zwanego naruszeniem.

PŁ bez zbędnej zwłoki zawiadamia osoby, której dane dotyczą o naruszeniu, jeżeli naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Opis charakteru naruszenia powinien umożliwić osobie dowiedzenie się, co faktycznie się stało i jakie są możliwe zagrożenia.

Zawiadomienie nie jest wymagane w sytuacji, gdy PŁ wdroży odpowiednie środki techniczne i organizacyjne, w szczególności szyfrowanie, zastosuje środki eliminujące prawdopodobieństwo wysokiego ryzyka lub komunikat publiczny o zdarzeniu będzie w skuteczny sposób doprowadzony do wiadomości tych osób.

Załącznik nr 34 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Zamawiający informuje Wykonawcę, że administratorem Pani / Pana danych osobowych zawartych w umowie jest Politechnika Łódzka z siedzibą w Łodzi, przy ul. Żeromskiego 116.

W sprawach ochrony danych osobowych można się skontaktować z wyznaczonym przez Rektora Inspektorem Ochrony Danych pod adresem rbi@adm.p.lodz.pl, telefon 42 631 20 39.

Politechnika Łódzka przetwarza Pani / Pana dane osobowe wyłącznie w celu wykonania zadań wynikających z tej umowy na podstawie art. 6 ust. 1 lit. b) 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).

Odbiorcami Pani / Pana danych osobowych będą osoby lub podmioty uprawnione na podstawie przepisów prawa.

Pani / Pana dane będą przechowywane przez okres uprawniający do zgłaszania reklamacji i roszczeń.

Przysługuje Pani / Panu zgodnie z RODO: prawo dostępu do swoich danych oraz otrzymania ich kopii; prawo do sprostowania i uzupełnienia swoich danych; prawo do usunięcia danych osobowych lub ograniczenia przetwarzania tylko w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa; prawo do uzyskania informacji oraz prawo do wniesienia skargi do Prezes UODO (na adres Urzędu ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa).

Podanie przez Panią / Pana danych osobowych niezbędnych do wykonania umowy jest obowiązkiem wynikającym z art. 6 RODO.

Wersja z dnia 25.05.2018r.

Załącznik nr 35 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Proces monitorowania zgodności przetwarzania z przepisami RODO

Sprawdzenie i opracowanie sprawozdania

Wprowadzenie

Opis procesu określa sposób i tryb realizacji najistotniejszego zadania Inspektora Ochrony Danych dotyczącego monitorowania przestrzegania ogólnego rozporządzenia RODO, przepisów ustawy o ochronie danych osobowych oraz dokumentów wewnętrznych Politechniki lub podmiotów przetwarzających w dziedzinie ochrony danych osobowych.

Weryfikowanie przestrzegania przepisów o ochronie danych osobowych obejmuje także podział obowiązków w tym zakresie, działania zwiększające świadomość, odbywanie szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

Etap 1: Sposób i tryb przeprowadzenia sprawdzeń, w tym audytów

1. Inspektor Ochrony Danych (IOD) skupia główny wysiłek na sprawdzeniu dokumentowania czynności przetwarzania w zakresie niezbędnym do oceny zgodności przetwarzania z przepisami o ochronie danych osobowych (ustalenie stanu faktycznego) oraz na opracowaniu sprawozdania.
2. Sprawdzenie realizowane jest na podstawie planu sprawdzeń oraz sprawdzenia doraźnego w sytuacji powzięcia przez IOD wiadomości o naruszeniu ochrony danych (incydentu) lub uzasadnionego podejrzenia wystąpienia takiego naruszenia. Możliwe jest sprawdzenie na wezwanie organu nadzorczego (PUODO), które może wystąpić w każdym czasie.
3. Czynności przygotowawcze do sprawdzenia polegają na:
   3.1. opracowaniu planu sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok oraz przedstawieniu Rektorowi do zatwierdzenia nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem;
   3.2. zawiadomieniu Rektora o rozpoczęciu sprawdzenia doraźnego przed podjęciem czynności w sprawdzeniu;
   3.3. zawiadomieniu kierownika jednostki objętej sprawdzeniem o zakresie planowanych czynności, w tym jaki proces lub jego część podlega sprawdzeniu, które czynności z rejestru czynności lub rejestru kategorii czynności, który system, program, aplikacja informatyczna, pliki tworzone w pakiecie biurowym, również zasygnalizowanie sprawdzenia przestrzegania obowiązków nałożonych na osoby funkcyjne w dokumentacji;
   3.4. zapewnieniu sprawdzanym możliwości przygotowania się do audytu oraz wzięcia udziału w sprawdzeniu.
4. W przypadku sprawdzenia doraźnego lub na wezwanie PUODO zawiadomienie Rektora ma nastąpić przed podjęciem pierwszej czynności w toku sprawdzenia z zastrzeżeniem sytuacji doraźnego sprawdzenia, gdy jest niezbędne niezwłoczne przywrócenie stanu zgodnego z prawem.
5. Katalog czynności IOD do których jest on uprawniony obejmuje:
   5.1. odbieranie wyjaśnień ustnych lub pisemnych;
   5.2. przeprowadzanie oględzin;
   5.3. dostęp do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych w celu utrwalenia danych cyfrowych;
   5.4. zbieranie dowodów z dokumentów, zrzutów z ekranu, kopii wybranych dokumentów.
6. Sposób dokumentowania czynności wykonywanych przez IOD polega na:

6.1. sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin, z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
6.2. odebraniu pisemnych wyjaśnień od osoby, której czynności objęto sprawdzeniem;
6.3. sporządzeniu kopii otrzymanego dokumentu;
6.4. utrwaleniu danych w postaci cyfrowej:
6.4.1. dokument utrwalający dane z systemu informatycznego lub zabezpieczania danych osobowych na informatycznym nośniku danych;
6.4.2. wydruk danych z systemu informatycznego;
6.4.3. kopia obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego lub zabezpieczenia danych osobowych;
6.4.4. kopia zapisów rejestrów systemu informatycznego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

Etap 2: Sporządzenie i przedstawienie sprawozdania

1. Po zakończonym sprawdzeniu IOD opracowuje sprawozdanie, którego istota sprowadza się do stwierdzenia, czy w ustalonym podczas sprawdzenia stanie faktycznym dotyczącym przetwarzania danych osobowych naruszono przepisy o ochronie danych osobowych. Elementy sprawozdania określa IOD na podstawie dobrych praktyk, kodeksów postępowania i doświadczenia.
2. Sprawozdanie IOD przekazuje Rektorowi w terminie nie później niż 30 dni od dnia zakończenia sprawdzenia w celu podjęcia decyzji co do wykonania zaleceń przez kierowników sprawdzanych jednostek, którzy otrzymują jeden egzemplarz z naniesioną dekretacją. W przypadku sprawdzenia doraźnego sprawozdanie przedkłada się Rektorowi niezwłocznie, a na wezwanie PUODO w terminie wskazanym przez ten organ.

Etap 3: Weryfikacja przestrzegania zapisów w dokumentacji przetwarzania danych

1. Kompetencje w zakresie przestrzegania stosowania procesów i czynności przetwarzania oznaczają przynależne IOD środki oddziaływania, jeżeli w wyniku weryfikacji stwierdzono nieprawidłowości lub uchybienia.
2. Weryfikacji podlega aktualność i kompletność dokumentacji oraz przestrzeganie zasad w niej określonych przez adresatów obowiązków, w tym zwłaszcza przez użytkowników systemu informatycznego. Czynności po weryfikacyjne mają na celu przywrócenie stanu prawidłowego.
3. IOD może przeprowadzić weryfikację w sposób uproszczony na podstawie zgłoszeń innych osób do punktu kontaktowego IOD.
4. Przywrócenie stanu prawidłowego polega na przedstawieniu Rektorowi do wdrożenia projektów dokumentów usuwających stan niezgodności lub aktualizujących stosowne zapisy.
5. W przypadku nieprzestrzegania zasad określonych w dokumentacji przetwarzania danych IOD poucza lub instruuje osobę, u której stwierdzono naruszenie o prawidłowym sposobie realizacji zasad wraz z powiadomieniem przełożonego tej osoby.

Załącznik nr 36 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Proces reagowania na incydenty godzące w bezpieczeństwo przetwarzania danych

Wprowadzenie

Opis procesu dotyczy trybu postępowania pracowników, w szczególności osób przetwarzających dane osobowe w sytuacji, gdy zaistnieje incydent naruszenia zasad przetwarzania danych osobowych lub naruszenia zabezpieczenia systemu informatycznego. W szczególności, gdy stan urządzenia, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych.

W sytuacji ludzkiego błędu, niefrasobliwości bądź stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub reguł ochrony danych osobowych, schemat postępowania opiera się na poniższych zasadach.

1. Inspektor Ochrony Danych (IOD) bierze udział w reagowaniu na incydent bezpieczeństwa, prowadzi czynności sprawdzające i na ich podstawie wnioskuje do Rektora o podjęcie działań niezbędnych do wyeliminowania lub zmniejszenia prawdopodobieństwa wystąpienia zagrożeń i ograniczenia skutków w przyszłości.
2. Sytuacjami, które wskazują na możliwość zaistnienia incydentu są, m.in:
   1) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania
   2) niszczenie dokumentacji bez użycia niszczarki
   3) przebywanie osób bez nadzoru w budynku lub pomieszczeniach obszaru przetwarzania, zachowujących się podejrzanie, zwłaszcza jeśli nie towarzyszy im przedstawiciel załogi jednostki
   4) otwarte drzwi do pomieszczeń, gdzie przechowywane są dokumenty, nieobecność pracownika na stanowisku pracy, gdy dokumenty są dostępne dla każdego, po zakończeniu pracy nie zamknięte szafy i nie wylogowany komputer
   5) ustawienie monitorów komputerów pozwalające na wgląd w ich zawartość przez osoby postronne, w tym brak wygaszacza ekranu
   6) wynoszenie dokumentów zawierających dane osobowe w wersji papierowej lub elektronicznej na zewnątrz uczelni bez zgody przełożonego
   7) umieszczanie na stronach jednostek list imiennych, do których dostęp możliwy jest bez zalogowania oraz próba skopiowania bazy danych (np. pracowników, studentów, doktorantów, klientów) i przekazania ich podmiotowi nieuprawnionemu
   8) ustne przekazywanie informacji zawierających dane osobowe osobom nieuprawnionym
   9) telefoniczne próby wyłudzenia danych osobowych
   10) kradzież komputerów lub innych urządzeń stanowiących zasób informatyczny jednostki
   11) otwieranie maili zachęcające do ujawnienia identyfikatora i/lub hasła, klikanie na fałszywe linki zachęcające do dokonania określonej czynności, przesyłane przez osoby trzecie
   12) pojawienie się wirusa komputerowego (zainfekowanie wirusem) lub niestandardowe zachowanie komputerów, np. spowolnienie pracy
   13) hasła do systemów przyklejone na kartkach typu post-it bądź jakichkolwiek innych dostępnych w pobliżu komputera

14) logowanie się kilku pracowników do jednej stacji roboczej przy użyciu ogólnie dostępnego hasła.

3. Każdy pracownik, zwłaszcza przetwarzający dane osobowe, który stwierdzi, podejrzewa lub uzyska informacje o naruszeniu zabezpieczeń danych osobowych lub zasad ochrony danych osobowych ma obowiązek niezwłocznego zgłaszania bezpośredniemu przełożonemu zdarzeń mających związek z naruszeniem bezpieczeństwa przetwarzania danych
4. Informacje o zdarzeniu należy przekazać wpierw bezpośrednio przełożonemu oraz administratorowi systemu informatycznego jeśli dotyczy systemu, w dalszej kolejności IOD za pośrednictwem wiadomości e-mail lub telefonicznie.
5. Nawet jeśli problem mający znamiona incydentu został rozwiązany we własnym zakresie informacje o tym należy przekazać do IOD.
6. IOD odbiera zgłoszenia przekazywane na punkt kontaktowy, dokonuje rejestracji, kategoryzuje zdarzenie oraz przesyła zwrotną informację do osoby zgłaszającej o sposobie zamknięcia sprawy.
7. W sytuacji, gdy okaże się, że dla oceny zdarzenia, wyjaśnienia przyczyn, podjęcia działań zmniejszających negatywne następstwa koniecznym jest skorzystać z pracowników mających wiedzę fachową w danej dziedzinie, IOD powołuje do rozpatrzenia incydentu takich specjalistów, głównie informatyków.
8. Po otrzymaniu zgłoszenia IOD na miejscu zdarzenia zbiera informacje i je analizuje, rozpoznaje charakter i rodzaj incydentu/naruszenia, sprawdza okoliczności, udział osób, rozmawia ze świadkami dążąc do potwierdzenia, że incydent miał miejsce.
9. Kierownik jednostki podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

   1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, podejmuje działanie zapobiegające zainfekowanie wirusem w podobny sposób oraz wdraża skuteczniejsze środki zabezpieczenia a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych;

   2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe instruktaże i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań inicjuje postępowanie dyscyplinarne.

10. IOD sporządza raport zawierający opis działań wyjaśniających, przyczyny oraz winnych incydentu, zalecenia powstrzymujące pogarszaniu sytuacji oraz wymienia niezbędne działania, by przywrócić stan zgodny z prawem. Raport wraz z załącznikami jako dowodami dokumentującymi naruszenie przekazuje kierownikowi jednostki, w której miało miejsce dane zdarzenie. Rektor otrzymuje informację zbiorczą za dany rok w raporcie o stanie bezpieczeństwa i ochrony danych osobowych.

11. W przypadku naruszeń najbardziej powszechnych procedur przetwarzania danych pracownik ponosi odpowiedzialność porządkową. Wobec osoby, która nie podjęła działania określonego w niniejszym procesie, a w szczególności nie powiadomiła przełożonego i IOD, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, mogą mieć zastosowanie przepisy odpowiedzialności porządkowej, materialnej lub wdrożone zostanie postepowanie dyscyplinarne.

Załącznik nr 37 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Wzór umowy powierzenia danych osobowych Podmiotowi Przetwarzającemu

1. *(Politechnika Łódzka w Łodzi/Zleceniodawca/Zamawiający - należy zmodyfikować zgodnie z nazewnictwem zawartym w treści umowy)* jako administrator danych, na warunkach określonych w art. 28 ust. 3 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 (ogólne rozporządzenie o ochronie danych) Dz.U.UE.L.2016.119.1 (dalej: ogólne rozporządzenie o ochronie danych), powierza *(X Y Sp. z o.o. - należy zmodyfikować zgodnie z nazewnictwem zawartym w treści umowy)* jako podmiotowi przetwarzającemu dane osobowe *(przykładowo: pracowników Uczelni, studentów, absolwentów).*
2. *(Politechnika Łódzka w Łodzi)* powierza *(X Y Sp. z o.o.)* przetwarzanie następujących danych osobowych: *(należy wskazać wszystkie rodzaje danych, do których będzie miał dostęp Podmiot Przetwarzający tzn. imię, nazwisko, adres zamieszkania itp.; w przypadku, gdy podmiotowi przetwarzającemu będą przekazywane dane dot. różnych kategorii osób np. pracowników i studentów, to należy dokładnie wskazać, które dane dotyczą wskazanych kategorii osób tzn. pracownicy: imię i nazwisko, studenci – adres zamieszkania itp.).*
3. *(X Y Sp. z o.o.)* będzie przetwarzać powierzone przez *(Politechnikę Łódzką)* dane osobowe w związku z realizacją przedmiotu umowy (*zasadniczej, rodzaju usługi)* przez czasokres jej realizacji.
4. Na podstawie niniejszej umowy *(X Y Sp. z o.o.)* na zlecenie *(Politechniki Łódzkiej)* będzie *(należy określić częstotliwość wykonywania czynności: stale i systematycznie/doraźnie/sukcesywnie na podstawie jednostkowych zamówień)* wykonywać następujące operacje na danych osobowych: *(przykładowo: zbierać, przechowywać, usuwać, aktualizować)* w celu realizacji przedmiotu umowy.
5. *(X Y Sp. z o.o.)* zobowiązuje się nie przetwarzać danych osobowych w sposób inny niż określony w niniejszej umowie lub wynikający z wyraźnego i udokumentowanego polecenia *(Politechniki Łódzkiej).*
6. *(X Y Sp. z o.o.)* nie może powierzyć przetwarzania danych osobowych innemu podmiotowi.
7. *(X Y Sp. z o.o.)* zobowiązuje się wobec *(Politechniki Łódzkiej)*, że w odniesieniu do powierzonych mu danych osobowych zastosuje środki techniczne i organizacyjne, o których mowa w art. 32 ogólnego rozporządzenia o ochronie danych, a w szczególności *(X Y Sp. z o.o.)* zapewni stopień bezpieczeństwa powierzonych mu danych odpowiedni do prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych.
8. Dostęp do danych powinni mieć wyłącznie pracownicy posiadający upoważnienie do przetwarzania danych osobowych nadane przez *(X Y Sp. z o.o.)*, przy czym osoby upoważnione do przetwarzania danych osobowych będą zobowiązane do zachowania ich

w tajemnicy (poprzez złożenie pisemnego oświadczenia) lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy zgodnie z art. 28 ust. 3 lit. b ogólnego rozporządzenia o ochronie danych.

9. W przypadku spełnienia przesłanek, o których mowa w art. 37 ust. 1 lit b) lub c) ogólnego rozporządzenia o ochronie danych, *(X Y Sp. z o.o.)* powoła Inspektora Danych Osobowych, a także powiadomi o fakcie jego powołania *(Politechnikę Łódzką)* i przekaże dane kontaktowe IOD.
10. W przypadku ustania terminu lub rozwiązania niniejszej umowy, *(X Y Sp. z o.o.)* jest zobowiązany w terminie 14 dni do:

a) nieodwracalnego usunięcia danych ze wszystkich nośników danych, urządzeń, systemów informatycznych oraz dysków w sposób uniemożliwiających ich odzyskanie,
b) zniszczenia dokumentacji pozyskanej w trakcie realizacji umowy zawierającej dane osobowe,
c) przekazania protokołów z dokonanych zniszczeń danych, o których mowa w pkt. a i b.

11. Przekazanie przez *(X Y Sp. z o.o.)* powierzonych mu danych do państwa trzeciego może nastąpić wyłącznie na podstawie uprzedniej pisemnej zgody *(Politechniki Łódzkiej)* chyba, że obowiązek taki wynika z przepisów prawa o czym podmiot przetwarzający informuje *(Politechnikę)* na min. 14 dni przed planowanym przekazaniem danych, o ile przepisy prawa nie zabraniają *(X Y Sp. z o.o.)* udzielania takiej informacji z uwagi na ważny interes publiczny.
12. *(Politechnika Łódzka)* zastrzega sobie możliwość przeprowadzenia zaplanowanej lub doraźnej kontroli w zakresie zastosowanych przez *(X Y Sp. z o.o.)* środków ochrony oraz procesu przetwarzania danych osobowych. O rozpoczęciu doraźnej kontroli *(Politechnika)* poinformuje *(X Y Sp. z o.o.)* nie później niż na 3 dni przed jej rozpoczęciem. W celu umożliwienia przeprowadzania kontroli *(X Y Sp. z o.o.)* zobowiązuje się do udostępnienia pomieszczeń, w których przechowywana jest dokumentacja zawierająca dane osobowe związana z realizacją zawartej umowy, w tym dostępu do informatycznych nośników danych.
13. W przypadku stwierdzenia nieprawidłowości w procesie przetwarzania danych osobowych w wyniku przeprowadzonej kontroli, *(Politechnika Łódzka)* prześle *(X Y Sp. z o.o.)* powiadomienie wzywające do ich usunięcia, zaś *(X Y Sp. z o.o.)* zobowiązuje się dostosować do zaleceń pokontrolnych. O sposobie i terminie usunięcia uchybień *(X Y Sp. z o.o.)* poinformuje *(Politechnikę Łódzka)* w formie pisemnej.
14. *(X Y Sp. z o.o.)* zobowiązuje się do niezwłocznego, jednak nie później niż w ciągu 12 godzin po stwierdzeniu naruszenia lub podejrzeniu jego wystąpienia, poinformowania *(Politechniki Łódzkiej)* oraz przekazania wszelkich niezbędnych informacji o jakimkolwiek zdarzeniu, które stanowi lub może stanowić naruszenie ochrony danych osobowych.
15. *(X Y Sp. z o.o.)* będzie pomagać *(Politechnice Łódzkiej)*, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III ogólnego rozporządzenia o ochronie danych. *(X Y Sp. z o.o.)* będzie również pomagać *(Politechnice)* wywiązywać się z obowiązków określonych w art. 32-36 przepisów ogólnego rozporządzenia o ochronie danych.

16. *(X Y Sp. z o.o.)* ponosi wobec *(Politechniki Łódzkiej)* pełną odpowiedzialność za szkodę wyrządzoną *(Politechnice)* lub osobom i podmiotom trzecim w związku z przetwarzaniem otrzymanych danych w sposób niezgodny z postanowieniami niniejszej umowy.
17. *(Politechnice Łódzkiej)* przysługuje prawo rozwiązania umowy ze skutkiem natychmiastowych w przypadku:
    a) gdy w ciągu 14 dni roboczych od dnia otrzymania powiadomienia, o którym mowa w ust. 14, *(X Y Sp. z o.o.),* nie zgłosi faktu usunięcia uchybień,
    b) stwierdzenia przez *(Politechnikę Łódzką)* naruszenia przez *(X Y Sp. z o.o.)* przepisów ogólnego rozporządzenia o ochronie danych.
18. W sprawach nieuregulowanych w niniejszym paragrafie mają zastosowania przepisy ogólnego rozporządzenia o ochronie danych.

Załącznik nr 38 do Załącznika Nr 1 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Proces postępowania z kluczami do pomieszczeń, w których są przetwarzane dane osobowe

Zgodnie z art. 36 ust 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, PŁ jest obowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Jednym z tego rodzaju środków jest procedura określająca sposób postępowania z kluczami do pomieszczeń tworzących obszar przetwarzania, w którym są przetwarzane dane osobowe pracowników, studentów i słuchaczy czy też klientów/kontrahentów uczelni.

1. Zasady ogólne stosowania procedury

a) obszar przetwarzania, to wyszczególnione w sposób spójny i jednoznaczny miejsca, w których przetwarza się dane osobowe w sposób zautomatyzowany (elektronicznie) lub niezautomatyzowany (na papierze);
b) obszar przetwarzania danych osobowych obejmuje zarówno miejsca, w których użytkownicy wykonują operacje na danych osobowych jak i miejsca, gdzie przechowywane są papierowe zbiory ewidencyjne czy też informatyczne nośniki informacji zawierające dane osobowe. Dotyczy to szaf z dokumentacją papierową, pomieszczeń, gdzie zlokalizowane zostały elementy infrastruktury IT, takie jak stacje robocze, pomieszczenia serwerowni, pomieszczenia przechowywania kopii zapasowych, węzły sieci, miejsce gromadzenia archiwum dokumentów papierowych z danymi osobowymi, itp.;
c) przy identyfikowaniu obszaru przetwarzania należy uwzględniać pomieszczenia, w których dane osobowe są odczytywane, wpisywane, modyfikowane, niszczone lub przechowywane;
d) obszaru przetwarzania nie stanowią audytoria, sale wykładowe i konferencyjne, pomieszczenia użytkowe, gospodarcze, sanitarne i socjalne;
e) nie stanowią obszaru przetwarzania miejsca, z których studenci mają dostęp do informacji o uzyskanych ocenach. Podobnie, nie stanowią obszaru przetwarzania tymczasowe miejsca i pomieszczenia, w których doraźnie są przetwarzane dane osobowe;
f) wszelkie prace remontowe i konserwacyjne w takich pomieszczeniach, wykonywane przez osoby nieupoważnione,
w szczególności spoza uczelni muszą być wykonywane w obecności przedstawiciela załogi jednostki. pomieszczenia wchodzące w skład obszaru przetwarzania danych osobowych ustala kierownik jednostki i przekazuje do wiadomości IOD, tj. przekazuje adres budynku, piętro oraz numery pomieszczeń. Oznaczenie takich pomieszczeń w sposób wyróżniający od pozostałych jest uzasadnione i zależy od decyzji kierownika jednostki;
g) dostęp do pomieszczeń obszaru przetwarzania możliwy jest wyłącznie poprzez wyznaczone do tego drzwi. Wszystkie pozostałe drzwi umożliwiające dostęp do takich pomieszczeń powinny być trwale zamknięte. Zabrania się otwierania tych drzwi przez pracowników bez zgody administratora budynku lub kierownika jednostki;
h) kierownik jednostki może zezwolić na posiadanie klucza użytkowego przez każdego z kilku pracowników zajmujących to samo pomieszczenie;
i) administrator budynku w porozumieniu z kierownikiem jednostki zapewnia nadzór nad osobami sprzątającymi pomieszczenia, w których przetwarzane są dane osobowe, także poza ustalonymi godzinami pracy w jednostce;
j) kierownik jednostki nadzoruje stosowanie procedury oraz wyraża zgodę na dorobienie klucza w przypadku jego zagubienia lub kradzieży.

2. Wydawanie i zdawanie kluczy w trakcie dnia pracy
a) wszędzie tam, gdzie budynek jest pod całodobową ochroną, klucze do pomieszczeń wydawane są przez portiera (aktualnie pełniącego służbę ochroniarza) za pobraniem przez osobę upoważnioną-w sytuacji braku portierni w budynku, zwłaszcza gdy jest w nim dostępny inny system zabezpieczeń kierownik jednostki może na stałe wydać klucze określonym pracownikom;

b) klucze do pomieszczeń szczególnie chronionych, np. serwerowni, miejsce przechowywania kopii zapasowych, archiwum, itp. wydawane są według odrębnej procedury ustalonej przez kierownika jednostki, któremu dane pomieszczenie podlega;
c) zaleca się, by dostęp do pomieszczeń szczególnie chronionych miały osoby wskazane imiennie, posługujące się kluczem z kodem lub kartą, a pomieszczenie pozostawało pod stałym nadzorem służby ochrony lub kamer monitoringu;
d) pracownicy upoważnieni do pobierania kluczy zobowiązani są do odnotowania pobrania i zdania kluczy w księdze, której wzór jest powszechnie stosowany. Księga pozostaje w dyspozycji pracownika (portiera) odpowiedzialnego za przechowywanie kluczy. zabrania się pozostawiania kluczy w drzwiach w czasie pracy, jak i po zakończeniu dnia pracy;
e) w godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą odpowiedzialność za ich zabezpieczenie;
f) po zakończeniu pracy, klucze zamykające biurka i szafy muszą być przechowywane w ustalonym miejscu, znanym współpracownikom, np. szufladzie, skrytce, plombowanym worku, itp. miejscu. Klucz zbiorczy jest zdawany do przechowania razem z kluczem do danego pomieszczenia lub jest przechowywany w innym miejscu.

3. Wydawanie i zdawanie kluczy zapasowych
a) wydawanie kluczy zapasowych i kart magnetycznych upoważnionym pracownikom, także z firmy ochraniającej budynek, może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych, za zgodą kierownika jednostki;
b) klucze zapasowe do pomieszczeń przechowywane są w depozycie - miejscu wskazanym przez kierownika jednostki np. na portierniach w zaplombowanych workach;
c) klucze zapasowe (służbowe karty magnetyczne) po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu za poświadczeniem zwrotu.
4. Naruszający procedurę może być pociągnięty do odpowiedzialności porządkowej, a w przypadku powstania szkód w mieniu do odpowiedzialności materialnej.

Załącznik Nr 2 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

Wytyczne - standardy ochrony danych osobowych przyjęte jako adekwatne do oceny ryzyka w Politechnice Łódzkiej

i. Obszar przetwarzania danych osobowych

1) obszar przetwarzania, to wyszczególnione miejsca, w których przetwarza się dane osobowe w sposób zautomatyzowany (elektronicznie) lub niezautomatyzowany (na papierze). Obejmuje zarówno miejsca, w których użytkownicy wykonują operacje na danych osobowych jak i miejsca, gdzie przechowywane są papierowe zbiory ewidencyjne czy też informatyczne nośniki informacji zawierające dane osobowe;
2) obszaru przetwarzania nie stanowią audytoria, sale wykładowe i konferencyjne, pomieszczenia użytkowe, gospodarcze, sanitarne i socjalne;
3) przebywanie wewnątrz strefy z pomieszczeniami z urządzeniami i nośnikami danych, na których zlokalizowane są procesy z danymi osobowymi powinno być dopuszczalne pod warunkiem uzyskania zgody kierownika jednostki oraz w obecności osób upoważnionych;
4) przebywanie wewnątrz strefy z pomieszczeniami z urządzeniami, na których nie są zlokalizowane dane osobowe, ale które umożliwiają dostęp do tych danych poprzez sieć komputerową za pośrednictwem terminali lub stacji roboczych po wykonaniu autoryzacji powinno być możliwe za zgodą kierownika jednostki;
5) dostęp do pomieszczeń obszaru przetwarzania możliwy jest wyłącznie poprzez wyznaczone do tego drzwi. Wszystkie pozostałe drzwi umożliwiające dostęp do takich pomieszczeń powinny być trwale zamknięte. Zabrania się otwierania tych drzwi przez pracowników bez zgody administratora budynku lub kierownika jednostki;
6) wszelkie prace remontowe i konserwacyjne wykonywane w pomieszczeniach obszaru przetwarzania przez osoby nieupoważnione i spoza uczelni, muszą być wykonywane w obecności przedstawiciela załogi jednostki.

ii. Zachowanie czystego biurka i czystego ekranu

1) personel uczestniczący w operacjach przetwarzania jest zobowiązany do stosowania zasady czystego biurka. Polega ona na bieżącym użytkowaniu dokumentów tylko niezbędnych do wykonania zadania, przechowywaniu dokumentów w szafach i biurkach oraz stosowaniu zabezpieczeń przed kradzieżą lub wglądem osób nieupoważnionych w trakcie godzin pracy jak i po jej zakończeniu;
2) każdy komputer musi mieć ustawiony wygaszasz ekranu po podaniu hasła lub wyłączający się automatycznie po określonym czasie bezczynności użytkownika. Dodatkowo przed pozostawieniem włączonego komputera bez opieki użytkownicy powinni zablokować go (włączając wygaszasz ekranu) lub w przypadku dłuższej nieobecności wylogować się z systemu;
3) dokumenty papierowe i wydruki zawierające dane osobowe przechowuje się w zamykanych na klucz szafach kartotekowych postawionych w pomieszczeniach stanowiących obszar przetwarzania w danej jednostce;
4) pracownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania. Krótkotrwałe składowanie większej partii dokumentów nie podlegających archiwizacji przeznaczonej do niszczenia w archiwum politechnicznym jest dopuszczalne.

iii. Korzystanie z urządzeń biurowych

1) pracownicy korzystający z urządzeń biurowych typu kopiarka, faks, drukarka nie powinni zostawiać żadnych dokumentów w otoczeniu oraz wewnątrz urządzeń, na czas dłuższy niż jest to konieczne;
2) organizacja procesu drukowania na urządzeniach innych niż indywidulane drukarki (dołączone tylko do jednego stanowiska roboczego) powinna zapewnić wstrzymywanie fizycznego wydruku do momentu pojawienia się przy urządzeniu drukującym i uwierzytelnienia się (np. przez podanie hasła, kodu) osoby, która wydruk zleciła;

3) organizacja procesu drukowania powinna zapewniać rozliczalność tego procesu metodą ukrytego znakowania dokumentów, w sposób umożliwiający co najmniej ujawnienie daty i czasu powstania wydruku oraz identyfikatora osoby, która druk zleciła;
4) urządzenia drukujące, kopiujące, faksy powinny znajdować się w miejscu niedostępnym dla osób nieuprawnionych;
5) zalecana jest ostrożność przy przesyłaniu dokumentów zawierających dane osobowe przy użyciu faxu, gdyż wiąże się to z możliwością ich upublicznienia;
6) zabrania się przekazywania bezpośrednio lub w rozmowie przez telefon danych osobowych osobom nieuprawnionym do ich poznania.

iv. Przekazywanie danych osobowych

Przekazywanie danych (informacji) pomiędzy jednostkami na rzecz administracji rektorskiej, wydziałowej i kanclerskiej ma charakter wewnętrznego ich przekazania w celu wykonania statutowych zadań dziekanatów i sekretariatów. Takie przekazanie nie ma cech udostępniania.

v. Prywatne urządzenia mobilne

1) wykorzystywanie w sieci Politechniki Łódzkiej sprzętu teleinformatycznego i urządzeń stanowiących własność prywatną pracowników i studentów, jako alternatywy wobec sprzętu służbowego czy przydzielonego im do użytku, wymaga uzyskania pisemnej zgody kierownika jednostki organizacyjnej;
2) Kierownik jednostki organizacyjnej rozważając możliwość używania dla celów służbowych prywatnych urządzeń i innego sprzętu elektronicznego z dostępem do Internetu rozstrzyga, kto z użytkowników jest uprawniony do telepracy (zabierania pracy do domu) i przegląda ich potrzeby w zakresie przydzielenia im konkretnych uprawnień;
3) pracownik wnioskujący o wykonywanie czynności na odległość (telepracę) korzysta z prawa wyboru modelu urządzenia lub nośnika pod warunkiem, że jest on wyposażony w funkcje zabezpieczające i blokujące dostęp poprzez PIN i/lub funkcję auto-lock. Zaakceptowany nośnik oznacza się w sposób zapewniający jego identyfikację jako nośnika służbowego i pisemnie lub mailowo informuje IOD o jego użytkowaniu;
4) składając wniosek pracownik świadomie akceptuje prawo przełożonego (Pracodawcy) do kontroli prywatnego sprzętu;
5) pozwalając na korzystanie z urządzenia prywatnego kierownik wyznacza cel, zakres i granice posługiwania się tym urządzeniem, wskazuje na wymagania bezpieczeństwa obowiązujące w PŁ oraz przenosi odpowiedzialność za ochronę przechowywanych tam służbowych informacji, w tym danych osobowych na użytkownika urządzenia;
6) po ustaniu stosunku pracy, pracownik wykonujący telepracę zwraca lub pod nadzorem informatyka/specjalisty IT wykasowuje z prywatnego sprzętu wszelkie służbowe informacje, dane osobowe i materiały. Z wykonanych czynności sporządzany jest protokół przekazywany do wiadomości IOD.

vi. Ograniczenia dotyczące instalacji i stosowania oprogramowania

1) użytkownicy zobowiązani są do używania oprogramowania udostępnionego im lub nabytego dla uczelni wyłącznie na podstawie licencji lub innych umów;
2) instalowanie lub używanie oprogramowania innego niż przekazanego bądź udostępnionego użytkownikom przez kierownika jednostki organizacyjnej, zwłaszcza prywatnie zakupionych płyt CD, programów ściąganych ze stron internetowych jak również odpowiadanie na samoczynnie pojawiające się reklamy internetowe jest zabronione;
3) użytkownik nie ma prawa do powielania danych lub programów zainstalowanych w komputerze przez administratora oprogramowania na swoje własne potrzeby ani na potrzeby osób trzecich.;
4) użytkownicy mają prawo do używania oprogramowania jedynie za zgodą kierownika jednostki, który przypisuje użytkownikowi oprogramowanie, które może być eksploatowane w danym komputerze. Każdy komputer powinien być skonfigurowany w taki sposób, aby do pracy niezbędne było zalogowanie się hasłem znanym jedynie użytkownikowi;
5) użytkownicy nie mają prawa do zmiany parametrów systemu, udostępniania osobom trzecim nośników i kodów instalacyjnych licencjonowanego oprogramowania. Podobne ograniczenie

obowiązuje studentów w przypadku, gdy zamierzają dokonywać zmian w konfiguracji oprogramowania, jeśli do tych zmian nie zostali upoważnieni przez prowadzących zajęcia;

6) podejmowanie prób przełamywania lub omijania zabezpieczeń oprogramowania i sieci w uczelni lub naruszanie któregokolwiek z powyższych postanowień może zagrozić bezpieczeństwu danych. Kierownik jednostki organizacyjnej ma prawo zażądać usunięcia nielegalnie lub niewłaściwie zainstalowanego oprogramowania. W takim przypadku użytkownik ponosi odpowiedzialność dyscyplinarną lub porządkową.

vii. Bezpieczne użytkowanie sprzętu IT

1) sprzęt IT służący do przetwarzania zbiorów danych osobowych jest zasobem informatycznym rzeczywistym (sprzętowym) bądź wirtualnym. Zasób obejmuje serwery, komputery stacjonarne lub mobilne, wydzielone ich części (przestrzeń dyskowa, udział sieciowy), urządzenia peryferyjne i komunikacji elektronicznej (telefony komórkowe), informatyczne nośniki danych (dyski CD, DVD, Blueray, pamięci USB), drukarki;
2) elementy zasobu informatycznego stanowią mienie powierzone użytkownikowi przez uczelnię (pracodawcę), który może sprawdzić w jaki sposób podwładni użytkują taki sprzęt IT;
3) użytkownik ponosi odpowiedzialność za nieuzasadnioną ingerencję w oprogramowanie instalowane i składowane na przydzielonym sprzęcie;
4) samowolne otwieranie (demontaż) sprzętu IT, instalowanie bez zezwolenia przełożonego dodatkowych urządzeń lub podłączanie do zasobu informatycznego jakichkolwiek urządzeń o niepotwierdzonej legalności jest zabronione;
5) użytkowanie mobilnych informatycznych nośników danych do przetwarzania danych osobowych możliwe jest za zgodą przełożonego. Taki nośnik jak laptop, smartfon, tablet czy pendrive jest przypisany imiennie do użytkownika i podlega ewidencjonowaniu jeśli zawiera dane osobowe. Zaleca się, by dostęp do składowanych tam danych osobowych wymuszał podanie indywidualnego hasła, PIN-u lub innego kodu dostępu;
6) używanie laptopów zawierających dane osobowe przez pracowników poza miejscem pracy, także na terenie campusów PŁ wymaga zezwolenia kierownika jednostki organizacyjnej. Takie laptopy muszą posiadać zainstalowaną ochronę antywirusową zapewniającą ochronę kryptograficzną wobec przetwarzanych danych osobowych. Pracownik użytkujący komputer przenośny do wykonywania pracy na odległość (telepraca), zachowuje szczególną ostrożność podczas transportu, przechowywania i użytkowania poza obszarem przetwarzania, do zabezpieczenia linką zapobiegającą kradzieży sprzętu włącznie;
7) za wskazanie specjalistycznego oprogramowania, które pozwala na zaszyfrowanie poszczególnych plików, partycji czy całego dysku komputera przenośnego, odpowiada Dyrektor Centrum Komputerowego PŁ.

viii. Monitoring wdrożonych zabezpieczeń systemów informatycznych

1) obowiązek monitorowania wdrożonych zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych wykonywany jest w imieniu Rektora, w praktyce w imieniu kierownika jednostki właściciela systemu przez administratora danego systemu lub technika/analityka;
2) celem monitorowania jest zapewnienie utrzymania zabezpieczeń systemu informatycznego na poziomie odpowiadającym stopniowi ochrony wynikającym z szacowania ryzyka. W praktyce chodzi o to, czy zabezpieczenia działają, należycie chronią dane osobowe, czy nie zostały one naruszone przez osoby trzecie, czy środki techniczne przyjęte w PŁ zapewniają oczekiwaną skuteczność;
3) adekwatnym do tego celu działaniem administratora/ów systemu/ów będzie przeglądanie logów lub fizyczny wgląd w zabezpieczenia serwerowni w przypadku podejrzenia naruszenia bezpieczeństwa systemu;
4) administratorzy systemów czy też technicy raportują do kierownika jednostki raz w miesiącu o podjętych czynnościach monitorujących, który po zaakceptowaniu przesyła informacje do IOD w celu zagregowania danych w sprawozdaniu dla Rektora.

ix. Monitoring systemów informatycznych

1) jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, PŁ może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej). Monitorowaniu podlegać będzie korzystanie przez pracowników i osób uczących się z komputerów, Internetu, aplikacji, kart dostępowych, itp.;
2) użytkownik skrzynki pocztowej ponosząc odpowiedzialność za treść i zawartość listów wysyłanych za pośrednictwem poczty elektronicznej SPE, powinien liczyć się z możliwością zachowania w archiwum poczty elektronicznej całości korespondencji.

x. **Monitoring aktywności w Internecie**

1) Odwiedziny na portalach społecznościowych w godzinach pracy, zakupy, uruchamianie innych stron internetowych, uruchamianie gier internetowych czy też oglądanie nagrań wideo może być objęte programem monitorującym aktywność służbowego komputera, monitorowanie nie dotyczy przeglądania for branżowych stanowiących bazę wiedzy przydatnej w pracy.
2) Kontrola korzystania z Internetu w miejscu pracy podyktowana jest względami bezpieczeństwa danych osobowych i jest możliwa poprzez stosowanie narzędzi prewencyjnych, takich jak filtry lub blokady zapobiegające gromadzeniu prywatnych informacji.
3) Kierownik jednostki organizacyjnej może bez uprzedzenia użytkownika blokować dostęp do niektórych portali, stron lub treści dostępnych za pośrednictwem Internetu.

xi. **Monitoring wizyjny**

1) Kierownik jednostki za zgodą Rektora może wprowadzić szczególny nadzór nad terenem swojego zakładu pracy lub terenem wokół w postaci środków technicznych umożliwiających rejestrację obrazu, to jest monitoringu;
2) celem monitoringu wizyjnego może być tylko potrzeba zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Zapobieganie kradzieżom sprzętu służbowego, ustanowienie szczególnej ochrony pomieszczeń technicznych (serwerownie, miejsca przechowywania kopii bezpieczeństwa, urządzenia sieciowe), itp. wchodzi w zakres ochrony mienia;
3) cele, zakres oraz sposób zastosowania monitoringu określa wewnątrzzakładowy regulamin pracy;
4) przed zastosowaniem monitoringu kierownik jednostki zapewnia opracowanie dokumentacji projektu systemu monitoringu i po uzyskaniu zgody Rektora informuje pracowników o wprowadzeniu monitoringu w sposób przyjęty w jednostce, nie później niż 2 tygodnie przed jego uruchomieniem;
5) obowiązek informacyjny wobec osób, których dane pozyskane zostały za pomocą systemu monitoringu wizyjnego realizuje kierownik jednostki wprowadzający monitoring oznaczając pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą znaków lub ogłoszeń, komunikatów i piktogramów;
6) tam, gdzie system monitoringu już funkcjonuje, administrator systemu dokonuje oceny konieczności dalszego stosowania monitoringu biorąc pod uwagę aktualny stan bezpieczeństwa w obszarze monitorowanym, poprawność rozmieszczenie kamer, sprawowanie nadzoru nad nagraniami. Jeśli z oceny skutków dla praw i wolności osób obserwowanych wynika zasadność stosowania takiego środka technicznego system monitoringu może nadal funkcjonować. W przeciwnym razie urządzenia należy zdemontować a oznaczenia terenu monitorowanego należy zdjąć;
7) Informacje o tym, jakie przepisy regulują monitoring, jak można korzystać z monitoringu, a także co na to przepisy RODO znajdują się **w webinarium pod linkiem** ...

xii. **Dostęp do skrzynki pocztowej nieobecnego pracownika**

1) Obowiązuje następująca procedura dostępu do służbowej skrzynki pocztowej nieobecnego pracownika:
   1. Kierownik jednostki organizacyjnej korzysta z prawa dostępu do korespondencji służbowej prowadzonej przez podległego pracownika, zwanego dalej użytkownikiem skrzynki pocztowej z wykorzystaniem systemu poczty elektronicznej SPE w przypadku jego dłuższej nieobecności zagrażającej ciągłości działania swojej jednostki;
   2. w tym celu, w razie zaistnienia takiej okoliczności kierownik jednostki organizacyjnej:

a) podejmuje próbę nawiązania kontaktu z nieobecnym pracownikiem proponując mu przeniesienie zawartości służbowych maili do innej wskazanej skrzynki służbowej;

b) jeśli to niemożliwe, występuje z pisemnym wnioskiem rejestrowanym w systemie obsługi zgłoszeń CK, realizowanym przez administratora poczty SPE o przeniesienie e-maili ze skrzynki służbowej danego pracownika do innej, wskazując przy tym na korespondencję, która jest istotna dla dalszego prowadzenia konkretnych zadań, projektów czy przedsięwzięć realizowanych dotychczas przez nieobecnego pracownika.

3. wyszczególnienie warunków, które administrator systemu poczty SPE może brać pod uwagę obejmuje wskazanie adresu nadawcy korespondencji, domeny nadawcy korespondencji oraz folderu źródłowego bez interpretacji jego nazwy;

4. tak wyszczególnione warunki pozwolą na umieszczenie przedmiotowej zawartości w odrębnym, nowo założonym folderze skrzynki docelowej dostępnej dla wnioskującego kierownika jednostki;

5. użytkownik skrzynki jest pisemnie poinformowany przez kierownika jednostki o przeprowadzeniu opisanej w punkcie 2 b) procedury;

6. podczas przenoszenia danych oraz e-maili nie jest wykorzystywane hasło do żadnej ze skrzynek pocztowych widniejących w systemie SPE, a administrator poczty SPE nie będzie miał wglądu w przenoszoną korespondencję.

xiii. **Zarządzanie projektami**

1) PŁ jako Beneficjent przetwarza dane osobowe uczestników projektów w celu udzielenia wsparcia przy realizacji określonego projektu, ewaluacji, monitoringu, kontroli i sprawozdawczości z wykorzystaniem systemu informatycznego dostarczonego przez Instytucję Pośredniczącą lub w innym bezpiecznym systemie informatycznym;
2) jeśli przy realizacji projektu podmioty zewnętrzne świadczą usługę związaną z dostępem do danych osobowych osób realizujących projekt, kierownik projektu wspólnie z IOD opracuje projekt umowy powierzenia przetwarzania danych osobowych w kształcie zgodnym z przepisami RODO;
3) odpowiedzialność za ochronę danych osobowych przetwarzanych w projekcie zgodnie ze wskazaniami umowy o dofinansowanie projektu ponosi kierownik projektu, w szczególności za wykonanie obowiązków informacyjnych wobec uczestników projektu oraz zapewnienie zgodności przetwarzania z przepisami RODO;
4) Kierownik Działu Projektów nadaje osobom realizującym projekty elektroniczne upoważnienia do przetwarzania danych osobowych na ustalonym przez Instytucję Pośredniczącą wzorze lub na wzorze uczelnianym;
5) na dzień zakończenia projektu kierownik projektu dopełnia obowiązku trwałego zniszczenia i wykasowania wszelkich danych osobowych przetwarzanych w sporządzonych w związku i przy okazji wykonywania prac projektowych dokumentów, z wyłączeniem danych podlegających archiwizacji;
6) niezbędne do finansowo - księgowego rozliczenia projektu dane o składnikach wynagrodzeń pracowników projektów udostępniane są przez Dział Osobowy na wniosek; wzór wniosku znajduje się w załączniku;
7) do środków zabezpieczenia danych osobowych zaliczane są środki organizacyjne, techniczne i ochrony fizycznej:

a) Do zabezpieczeń organizacyjnych zaliczono m.in.:

— opracowano i wdrożono Politykę ochrony danych osobowych;
— powołano pracownika do wykonywania funkcji Inspektora Ochrony Danych (IOD), o czym poinformowano organ nadzorczy;
— opracowano i wdrożono dokumentację opisującą sposób przetwarzania danych osobowych, to jest Politykę ochrony danych osobowych wraz z opisem procesów przetwarzania danych realizowanych przy pomocy systemu NND;
— przetwarzanie danych osobowych podlega przeglądowi i aktualizowaniu w ramach procesu monitorowania zgodności przetwarzania z przepisami RODO, sprawdzenia i opracowania sprawozdania przez właściciela proces, którym jest IOD;

- Rektor nadał władzom uczelni zajmującym stanowiska odpowiednio do struktury organizacyjnej uczelni uprawnienia do nadawania upoważnień do przetwarzania danych osobowych w systemie NND, w których kompetencji pozostaje wskazanie czynności przetwarzania, systemu i zakresu uprawnień dostępu; proces monitoruje IOD jego właściciel;
- osobom posiadającym upoważnienie do przetwarzania danych osobowych administratorzy systemów służących do przetwarzania danych osobowych realizują wnioski o nadanie uprawnienia pracy w systemach;
- kierownicy jednostek zobowiązani zostali występować do uprawnionego przełożonego w celu bezzwłocznej zmiany uprawnień pracowników w przypadku zmiany zadań tych osób na zajmowanym stanowisku;
- prowadzona jest ewidencja udostępnień danych osobowych, umów powierzenia, informatycznych nośników danych używanych w jednostkach do przetwarzania danych osobowych;
- osoby przetwarzające dane osobowe zostały zobowiązane do zachowania ich w tajemnicy poprzez zaznaczenie zaakceptowania treści oświadczenia;
- zarządzającym - właścicielom procesów opisanych w Polityce przypisane zostały obowiązki i odpowiedzialność za realizację celów procesu oraz monitorowanie jego aktualności i zgodności z prawem;
- odpowiednio do decyzji kierowników jednostek, w miarę możliwości wydzielono strefy ograniczonego dostępu, w tym strefę, gdzie gromadzone są dokumenty zawierające dane osobowe;
- opracowano proces reagowania na incydenty godzące w bezpieczeństwo przetwarzania danych, którego właścicielem jest IOD;
- opracowano i prezentuje się webinaria tematyczne przeznaczone dla przetwarzających dane osobowe. Prowadzone jest szkolenie na wniosek kierowników jednostek z wybranych aspektów przepisów RODO;
- opracowano i bieżąco prowadzi się rejestr czynności przetwarzania .

b) Zabezpieczenia techniczne:

- wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą co najmniej zapory ogniowej;
- zapewniono kontrolę dostępu poprzez zakładanie indywidulanych kont dla każdego użytkownika systemu informatycznego i stosowanie mechanizmu identyfikacji użytkowników w systemach informatycznych poprzez nadane identyfikatory i hasła;
- jeśli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie rejestrowany był dla każdego użytkownika odrębny identyfikator a dostęp był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia;
- stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową;
- działa system centralnej aktualizacji oprogramowania systemowego, system wykrywania włamań w sieci wewnętrznej;
- zabezpieczenie zasilania awaryjnego poprzez zasilacze awaryjne (UPS) dla wszystkich komputerów przetwarzających dane osobowe;
- na komputerach przenośnych kierownictwa i wybranych osób zastosowano środki ochrony kryptograficznej w stosunku do danych osobowych w nich przetwarzanych;
- ustanowiono zarządzanie usługami dostarczanymi przez strony (podmioty, osoby) trzecie;
- scentralizowano nabywanie urządzeń i sprzętu, w tym prowadzone są zbiorcze zakupy licencyjnego oprogramowania;
- czasowa przerwa w posługiwaniu się komputerem powoduje uruchomienie wygaszacza ekranu;
- zastosowano mechanizmy wymuszające okresową zmianę haseł (nie rzadziej, niż co 30 dni) oraz wymuszające złożoność haseł;
- kopiowanie danych osobowych na nośniki mobilne zatwierdzone przez kierownika jednostki i dopuszczone do użytku tylko jeśli posiadają one funkcje zabezpieczające i blokujące dostęp poprzez PIN;
- wprowadzono monitorowanie dla nieautoryzowanych działań związanych z przetwarzaniem informacji, w tym dzienniki audytu rejestrujące działania użytkowników, a także rejestrację

błędów i incydentów związanych z naruszeniem atrybutów bezpieczeństwa informacji: poufności, dostępności lub integralności;
- zapewniono, by praca na odległość (telepraca) odbywała się za zgodą kierownika jednostki bezpiecznym kanałem komunikacji, szyfrowanym tunelem VPN;
- dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

c) Środki ochrony fizycznej rozumiane jako:
- obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem;
- stosowana jest procedura postępowania z kluczami do pomieszczeń obszaru przetwarzania ograniczająca dostęp do kluczy tylko dla osób do tego uprawnionych,
- w przypadku sprzątania pomieszczeń przed przyjściem pracowników lub po ich wyjściu, osobom sprzątającym udziela się instruktażu o obowiązku przekazania (nie niszczenia) wszelkich materiałów pozostawionych bez zabezpieczenia;
- przebywanie osób nieuprawnionych na obszarze przetwarzania danych możliwe jest za zgodą kierownika jednostki lub w obecności osoby upoważnionej;
- dokumenty papierowe zawierające dane osobowe przechowywane są w szafach zamykanych na klucz lub zamykanych regałach. Dostęp do dokumentacji zawierającej dane osobowe mają wyłącznie osoby do tego upoważnione;
- w pomieszczeniach, w których przetwarzane są dane osobowe zamontowane są czujniki dymu systemu automatycznego gaszenia na wypadek pożaru lub przy pomocy wolno stojącej gaśnicy;
- do wybranych pomieszczeń budynków wymagających zwiększonego nadzoru zastosowano system automatycznej rejestracji wejść i wyjść. W niektórych przypadkach takie pomieszczenia zabezpieczono kartami dostępu, w innych ograniczono dostęp do osób imiennie wyznaczonych;
- archiwum z zasobem materiałów archiwalnych i dokumentacji niearchiwalnej, m.in. dokumentacją studencką, przewodami doktorskimi, przewodami habilitacyjnymi, itp. umieszczono w specjalnie przygotowanych i wyposażonych magazynach na tzw. niskim parterze, w budynkach chronionych przez licencjonowaną firmę ochroniarską oraz system ochrony przeciwpożarowej. Archiwum dokumentów papierowych i elektronicznych zawierających dokumentację pracowniczą, w tym osób wykonujących pracę na podstawie umów cywilnoprawnych umieszcza się w odrębnym budynku chronionym systemem alarmowym;
- wybrane pomieszczenia w budynkach uczelni monitorowane są w celu zapewnienia bezpieczeństwa i zapobieżenia kradzieży sprzętu trwałego, o czym informują komunikaty na tablicach informacyjnych oraz piktogramy umieszczone w miejscach ogólnodostępnych;
- do pomieszczeń, gdzie zlokalizowane zostały elementy infrastruktury IT, takie jak stacje robocze, pomieszczenia serwerowni, pomieszczenia przechowywania kopii zapasowych, węzły sieci, miejsce gromadzenia archiwum dokumentów papierowych z danymi osobowymi, itp. mają dostęp osoby imiennie wyznaczone przez kierownika jednostki.

Rektor
Politechniki Łódzkiej
Prof. dr hab. inż. Sławomir Wiak

Załącznik Nr 1 do Załącznika Nr 2 do Zarządzenia Nr 7/2018
Rektora Politechniki Łódzkiej z dnia 24 maja 2018 roku
w sprawie wdrożenia dokumentacji ochrony
danych osobowych w Politechnice Łódzkiej

WNIOSEK O UDOSTĘPNIENIE/PRZEKAZANIE DANYCH Z BAZY DANYCH OSOBOWYCH PŁ

1. Wniosek do .....
.....
(oznaczenie administratora danych, zarządzającego procesem)

2. Wnioskodawca .....
.....
.....
(nazwisko, imię np. kierownika jednostki, projektu, wnioskodawcy, imię nazwisko osoby przetwarzającej dane)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych:
.....
.....

4. Wskazanie przeznaczenia dla udostępnionych danych:.....
.....

5. Oznaczenie lub nazwa procesu/bazy, z którego mają być udostępnione dane:.....
.....

6. Zakres żądanych informacji z bazy: .....
.....
.....
.

7. Forma udostępnienia/przekazania:

.....
.(jednorazowy/okresowy wydruk, udostępnienie możliwości wydruku, udostępnienie w określonym formacie za pomocą szyfrowanego kanału systemu teleinformatycznego, dostęp do widoku/odczytu, inne)

8. Informacje umożliwiające wyszukanie w bazie żądanych danych:.....

.....
(data, podpis, ew. pieczęć wnioskodawcy)

ZGODA

.....

(podpis zarządzającego procesem)