Załącznik do zarządzenia nr 203/2025

Procedura ochrony danych osobowych podczas pracy zdalnej w Uniwersytecie Jana Kochanowskiego w Kielcach

I. Zakres i cel procedury

§ 1

1. Procedura ochrony danych osobowych podczas pracy zdalnej, zwana dalej „Procedurą" określa zasady postępowania z danymi osobowymi, w szczególności ich zabezpieczenie oraz ochronę.
2. Każdy pracownik wykonujący pracę zdalną, bez względu na tryb, w jakim jest ona wykonywana, jest obowiązany do stosowania niniejszej Procedury.

II. Słownik pojęć

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:

1) RODO – należy przez to rozumieć 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);
2) Uniwersytecie/UJK – należy przez to rozumieć Uniwersytet Jana Kochanowskiego w Kielcach;
3) administratorze danych osobowych (zwanym dalej ADO) – należy przez to rozumieć, reprezentowany przez rektora, Uniwersytet Jana Kochanowskiego w Kielcach, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
4) inspektorze ochrony danych (zwanym dalej IOD) – należy przez to rozumieć pracownika wyznaczonego przez ADO i jemu bezpośrednio podległego, spełniającego wymogi kompetencyjne RODO, działającego zgodnie z zasadami określonymi w art. 37-39 RODO;
5) administratorze systemów informatycznych (zwanym dalej ASI) – należy przez to rozumieć osobę wyznaczoną przez ADO, odpowiadającą za poszczególne systemy informatyczne służące do przetwarzania danych, w tym odpowiedzialną za bezpieczeństwo informacji przetwarzanych w systemie, w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu oraz podejmowanie odpowiednich działań w porozumieniu ze specjalistą ds. bezpieczeństwa teleinformatycznego w zakresie ochrony danych przetwarzanych w systemie, również w przypadku wykrycia w nim naruszeń;

6) administratorze zasobów (zwanym dalej AZ) – należy przez to rozumieć pracownika, który jest odpowiedzialny za prawidłowe zabezpieczenie sprzętu służącego do przetwarzania danych osobowych w poszczególnych jednostkach Uniwersytetu;
7) użytkowniku – należy przez to rozumieć osobę posiadającą upoważnienie do przetwarzania danych osobowych w zbiorach tradycyjnych lub/i w systemach informatycznych, w zakresie wskazanym w upoważnieniu;
8) danych osobowych – należy przez to rozumieć 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;
9) przetwarzaniu danych osobowych – należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
10) zbiorze danych – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
11) systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
12) ustawie – należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U z 2019 r. poz. 1781);
13) zarządzeniu – należy przez to rozumieć zarządzenie rektora w sprawie wprowadzenia Procedury ochrony danych osobowych podczas pracy zdalnej;
14) Polityce Bezpieczeństwa – należy przez to rozumieć Politykę Bezpieczeństwa w zakresie ochrony danych osobowych w Uniwersytecie Jana Kochanowskiego w Kielcach, stanowiącą załącznik nr 1 do zarządzenia Rektora UJK nr 53/2018 z dnia 24 sierpnia 2018 roku;
15) Instrukcji – należy przez to rozumieć Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Uniwersytecie Jana Kochanowskiego w Kielcach, stanowiącą załącznik nr 2 do zarządzenia Rektora UJK nr 53/2018 z dnia 24 sierpnia 2018 roku;
16) Polityce Bezpieczeństwa Informacji – należy przez to rozumieć Politykę Bezpieczeństwa Informacji Uniwersytetu Jana Kochanowskiego w Kielcach,

wprowadzoną zarządzeniem Rektora nr 1/2019 z dnia 4 stycznia 2019 roku;

17) Regulaminie – Regulamin Sieci Komputerowej Uniwersytetu Jana Kochanowskiego w Kielcach,
wprowadzony zarządzeniem Rektora Nr 60/2022 z dnia 24 maja 2022 roku;

18) zasoby – dane gromadzone/przetwarzane/udostępniane za pomocą urządzeń i systemów Uniwersytetu, w tym usługi dostępu do platform pracy i kształcenia zdalnego oraz poczty elektronicznej.

III. Przepisy ogólne

§ 3

1. W Uniwersytecie prowadzi się dokumentację opisującą sposób przetwarzania danych osobowych oraz środki ochrony tych danych. W skład tej dokumentacji wchodzą w szczególności:
   1) zarządzenie rektora w sprawie ochrony danych osobowych w Uniwersytecie Jana Kochanowskiego w Kielcach zawierające jako integralne części m.in:
      a) Politykę Bezpieczeństwa,
      b) Instrukcję.
   2) inne pisma, komunikaty i instrukcje szczegółowe mające znaczenie dla ochrony danych
      osobowych, wydawane przez ADO lub IOD.
2. Dokumentację, o której jest mowa w ust. 1, stosuje się do wszystkich użytkowników, zarówno zatrudnionych w Uniwersytecie, jak i innych, np.: stażystów, praktykantów.
3. W Uniwersytecie przetwarza się dane osobowe z poszanowaniem obowiązujących w tym zakresie przepisów prawa zawartych m.in. w:
   1) RODO,
   2) ustawie,
   3) Kodeksie pracy,
   4) innych aktach normatywnych, które odnoszą się do problematyki ochrony danych osobowych.

§ 4

1. Użytkownik wykonujący pracę zdalną jest zobowiązany do złożenia oświadczenia pracownika skierowanego do wykonywania pracy zdalnej. Wzór oświadczenia stanowi załącznik do niniejszej Procedury.
2. Użytkownik wykonujący pracę zdalną, uzyskuje dostęp do danych osobowych, których przetwarzanie jest niezbędne do wykonywania obowiązków służbowych.
3. Nie jest dopuszczalne wykorzystywanie danych osobowych przetwarzanych w ramach pracy zdalnej w innym celu niż wykonywanie obowiązków pracowniczych.

IV. Zasady dotyczące bezpieczeństwa danych osobowych podczas pracy zdalnej

§ 5

1. Dostęp do danych osobowych podczas pracy zdalnej może odbywać się poprzez:
   1) pracę z dokumentami tradycyjnymi (kopie dokumentów z Uniwersytetu),
   2) pracę w systemach informatycznym zgodnie z uprawnieniami i zrealizowanym dostępem do zasobów; dostęp do zasobów Uniwersytetu realizowany jest przez Centrum Informatyki poprzez bezpieczny tunel szyfrowany; podstawą do uzyskania zdalnego dostępu jest wypełniony wniosek załącznik nr 2h do Regulaminu,
   3) korzystanie z platform do pracy i nauki na odległość, zasady korzystania z platform określa załącznik nr 8 do Regulaminu.
2. Komunikacja służbowa odbywa się w sposób zapewniający bezpieczeństwo informacji oraz danych osobowych, wyłącznie poprzez wskazane przez pracodawcę narzędzia i połączenia.

§ 6

1. Użytkownik zobowiązany jest do dbałości o bezpieczeństwo danych osobowych przetwarzanych w ramach wykonywania obowiązków służbowych.
2. Zobowiązany jest w szczególności do:
   1) zapoznania się procedurami wewnętrznymi dotyczącymi ochrony danych osobowych,
   2) zabezpieczenia danych osobowych przed osobami nieupoważnionymi,
   3) uporządkowania swojego stanowiska pracy po zakończeniu pracy i przechowywania dokumentów tradycyjnych oraz nośników elektronicznych, zgodnie z zasadą ,,czystego biurka",
   4) niezapisywania na pulpicie systemowym plików zawierających dane osobowe,
   5) niepozostawiania niezabezpieczonych komputerów w stanie aktywnej sesji dostępu do ich zawartości,
   6) niepodłączania zewnętrznych nośników elektronicznych niewiadomego pochodzenia,
   7) utrzymania w tajemnicy otrzymanych od pracodawcy danych dostępowych, w tym loginów i haseł oraz zabezpieczenia ich przed dostępem osób nieuprawnionych, w tym domowników; szczegółowe zasady dotyczące zmiany hasła, jego budowy i przechowywania zostały określone w Instrukcji,
   8) pracy w ramach przydzielonego mu konta w systemie informatycznym,
   9) szyfrowania za pomocą odpowiednich programów plików zawierających dane osobowe; nie należy przesyłać plików z danymi osobowymi (np. w celu pracy z danymi osobowymi), jeżeli możliwy jest dostęp do danych w systemie informatycznym,
   10) ograniczenia do niezbędnego minimum drukowania plików zawierających dane osobowe i do sytuacji, gdy jest to konieczne,
   11) ograniczenia do niezbędnego minimum wynoszenia dokumentacji papierowej z siedziby Uniwersytetu; w przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą Uniwersytetu w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której użytkownik będzie pracował; kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały,

12) niszczenia roboczych wydruków zawierających dane osobowe po ustaniu ich przydatności dla bieżącej pracy przy użyciu niszczarki; w przypadku nieposiadania niszczarki w miejscu wykonywania pracy zdalnej użytkownik powinien zniszczyć zbędną dokumentację papierową niezwłocznie na Uniwersytecie,
13) cyklicznego usuwania niepotrzebnych plików zawierających dane osobowe pobranych w celu pracy z nimi,
14) niekorzystania i nieuruchamiania programów i aplikacji pochodzących od nieznanych nadawców,
15) nieudostępniania domownikom komputera przenośnego lub innego sprzętu wykorzystywanego do pracy zdalnej, jeżeli komputer stanowi własność pracownika, praca odbywa się wyłącznie na wydzielonych kontach systemowych,
16) prawidłowego transportowania powierzonego sprzętu oraz dokumentacji zawierającej dane osobowe; w szczególności nie jest dozwolone pozostawianie ich bez nadzoru (np.: w samochodzie, przechowalni bagażu).

4. Użytkownikowi zabrania się:
   1) korzystania ze sprzętu wykorzystywanego do pracy zdalnej oraz dokumentacji zawierającej dane osobowe w miejscu publicznym, np.: środku transportu zbiorowego, kawiarni,
   2) ustawienia zapamiętywania hasła do poczty elektronicznej przez przeglądarkę internetową i klientów poczty,
   3) przekazywania informacji chronionych, w szczególności danych osobowych bez zabezpieczenia hasłem, w szczególności w treści wiadomości e-mail; przekazywania hasła do zabezpieczonych informacji tą samą drogą komunikacji, którą przekazywany jest zabezpieczony hasłem plik lub pliki; szczegółowe zasady korzystania z poczty e-mail określa Regulamin.

§ 7

1. Minimalne wymagania w zakresie bezpieczeństwa danych osobowych przetwarzanych na prywatnym sprzęcie:
   1) na urządzeniu jest legalne i aktualne oprogramowanie,
   2) zostały włączone automatyczne aktualizacje,
   3) została włączona zapora systemowa,
   4) został zainstalowany i działa w tle program antywirusowy,
   5) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny
      login i hasło użytkownika, kod PIN, token,
   6) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
   7) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np.: 7 zip),
   8) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności,
   9) jeżeli urządzenie daje taką możliwość, praca jest wykonywana na koncie z ograniczonymi uprawnieniami,

2. Zaleca się także zaszyfrowanie dysku twardego sprzętu wykorzystywanego do pracy zdalnej.

§ 8

IOD przeprowadza szkolenia wśród pracowników Uniwersytetu w celu poszerzania wiedzy z zakresu ochrony danych osobowych podczas pracy zdalnej.

§ 9

1. Problemy w działaniu udostępnionego sprzętu lub oprogramowania należy niezwłocznie zgłaszać do Centrum Informatyki.
2. W przypadku zgubienia, zniszczenia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, należy niezwłocznie, w dniu zdarzenia zgłosić zdarzenie do IOD, ASI lub AZ.
3. Pracownik jest obowiązany zgłosić incydenty naruszenia ochrony danych oraz ich podejrzenia IOD, ASI lub AZ.
4. Szczegółowy sposób postępowania w przypadku zauważenia incydentu ochrony danych określa Polityka bezpieczeństwa.

§ 10

Przetwarzanie danych osobowych podczas pracy zdalnej następuje z poszanowaniem – odpowiednio stosowanych – zasad bezpieczeństwa informacji określonych w Polityce Bezpieczeństwa Informacji.

V. Przepisy końcowe

§ 11

1. Wszelkie przypadki naruszenia przepisów Procedury oraz propozycje zmian w regulacjach funkcjonujących w Uniwersytecie, mające na celu zwiększenie bezpieczeństwa przetwarzania danych osobowych, należy niezwłocznie zgłaszać IOD.
2. W sprawach nieuregulowanych w niniejszej Procedurze zastosowanie mają w szczególności:
   1) Polityka Bezpieczeństwa,
   2) Instrukcja,
   3) Polityka Bezpieczeństwa Informacji,
   4) Regulamin.

Załącznik do Procedury ochrony danych osobowych podczas pracy zdalnej w Uniwersytecie Jana Kochanowskiego w Kielcach

OŚWIADCZENIE PRACOWNIKA SKIEROWANEGO DO WYKONYWANIA PRACY ZDALNEJ

Ja……..oświadczam, że podczas wykonywania pracy zdalnej będę przestrzegać obowiązujących przepisów o ochronie danych osobowych (w szczególności przepisów ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych oraz 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), w tym także wewnętrznych aktów prawnych i procedur dotyczących ochrony danych osobowych obowiązujących w Uniwersytecie Jana Kochanowskiego w Kielcach, a także dbać o bezpieczne przetwarzanie przeze mnie powierzonych mi danych z zapewnieniem, że osoby nieupoważnione nie uzyskają dostępu do tych danych.

Jednocześnie oświadczam, że znane są mi zasady ochrony danych osobowych oraz że zapoznałem się z materiałami szkoleniowymi dotyczącymi zasad bezpiecznej pracy zdalnej, znajdującymi się na stronie internetowej UJK (https://bip.ujk.edu.pl/odo_do_pobrania.html).

……

(data i podpis pracownika)