

Zarządzenie wewnętrzne Nr R021.1.23.2022
Rektora Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie
z dnia 21 marca 2022 r.
w sprawie zasad przeprowadzania w Uniwersytecie Humanistyczno-Przyrodniczym
im. Jana Długosza w Częstochowie
oceny ryzyka przetwarzania danych osobowych
oraz oceny skutków dla ochrony danych osobowych

Na podstawie art. 23 ust. 1 i 2 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (tj. Dz.U. z 2022 poz. 574 z późn. zm.) w związku z § 24 ust.1 – 3 Statutu Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie, zgodnie z art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2 oraz art. 35 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), zarządza się, co następuje:

§1

W celu zapewnienia odpowiedniego stopnia bezpieczeństwa dla przetwarzanych danych osobowych adekwatnego do stopnia zidentyfikowanych zagrożeń wprowadza się zasady przeprowadzania oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą wiążącego się z przetwarzaniem danych osobowych w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§2

1. Oceny ryzyka przetwarzania danych osobowych dokonują właściciele ryzyka, czyli osoby zarządzające ryzykiem, które realizują procesy związane z przetwarzaniem danych osobowych i posiadają uprawnienia do podjęcia działań zaradczych w ramach obszaru, którym zarządzają.
2. Właścicielami ryzyka w odniesieniu do przetwarzania danych osobowych realizowanego w podległych jednostkach są:
 - a. rektor, prorektorzy, dziekani, kanclerz
 - b. dyrektorzy jednostek ogólnouczelnianych
 - c. kierownicy jednostek organizacyjnych
 - d. pracownicy na samodzielnych stanowiskach
 - e. administratorzy systemów informatycznych (ASI) w zakresie oceny ryzyka dla systemów informatycznych służących do przetwarzania danych osobowych.

3. Nadzór nad przeprowadzaniem oceny ryzyka związanego z przetwarzaniem danych osobowych sprawuje rektor oraz lokalni administratorzy danych osobowych (LADO): prorektorzy w obszarze przetwarzania w podległych jednostkach, dziekani w obszarze przetwarzania w podległych wydziałach, kanclerz w obszarze przetwarzania dokonywanego przez administrację centralną i w innych obszarach niepodlegających dziekanom i prorektorom.

§3

1. Ocena ryzyka przeprowadzana jest cyklicznie w celu zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń.
2. Pracownicy w ramach wykonywanych obowiązków służbowych są zobowiązani do informowania przełożonych o zidentyfikowanych ryzykach i wszelkich podejrzeniach możliwości wystąpienia ryzyka w przetwarzaniu danych osobowych, które to ryzyka/podejrzenia ryzyka są następnie analizowane przez przełożonych – właścicieli ryzyka.
3. Oceny ryzyka przetwarzania danych osobowych właściciele ryzyka dokonują:
 - a. w przypadku wszystkich prowadzonych procesów przetwarzania przynajmniej raz w roku – w terminie wskazanym przez administratora,
 - b. w przypadku planowanych do wprowadzenia nowych procesów przetwarzania czy też nowych mechanizmów przetwarzania, np. z wykorzystaniem nowych systemów informatycznych – przed rozpoczęciem przetwarzania.
4. Analizy wyników oceny ryzyka przeprowadzonej przez właścicieli ryzyka, o której mowa w §3 pkt. 3, a w przypadku, o którym mowa w §3 pkt. 3 lit. a. także ich zbiorczego opracowania, dokonuje Zespół ds. wdrożenia ogólnego rozporządzenia o ochronie danych RODO powołany zarządzeniem wewnętrznym Nr R0161/18/2018 Rektora Akademii im. Jana Długosza w Częstochowie z dnia 21 lutego 2018r. w sprawie powołania Zespołu ds. wdrożenia Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (ogólnego rozporządzenia o ochronie danych RODO) w Akademii im. Jana Długosza w Częstochowie. Wyniki analizy zatwierdza administrator.
5. Do przeprowadzenia oceny ryzyka przetwarzania danych osobowych służy *Tabela oceny ryzyka w przetwarzaniu danych osobowych* stanowiąca załącznik nr 1 do niniejszego zarządzenia.
6. Oceny ryzyka właściciele ryzyka dokonują w następujących etapach:
 - a. zweryfikowanie aktualności wykonywanych w jednostce czynności przetwarzania wyszczególnionych w *Rejestrze czynności przetwarzania*, o którym mowa w zarządzeniu wewnętrznym Nr R021.1.58.2021 Rektora z dnia 1 czerwca 2021 r. w sprawie prowadzenia przez Administratora danych – Uniwersytet Humanistyczno-Przyrodniczy im. Jana Długosza w Częstochowie *Rejestru czynności przetwarzania danych osobowych*.
W przypadku braku danej czynności przetwarzania w *Rejestrze czynności przetwarzania* należy dla tej czynności przeprowadzić ocenę ryzyka w *Tabeli oceny ryzyka w przetwarzaniu danych osobowych* oraz jednocześnie przesłać na adres email: iod@ujd.edu.pl uzupełniony o tę czynność szablon *Rejestru czynności*

przetwarzania dostępny na Portalu pracowniczym w zakładce Druki do pobrania – Inspektor ochrony danych.

Dla podobnych czynności przetwarzania można przeprowadzić jedną wspólną ocenę ryzyka

- b. wskazanie aktywów wykorzystywanych w procesie przetwarzania danych osobowych
- c. identyfikacja zagrożeń dla bezpieczeństwa danych osobowych przetwarzanych w ramach wskazanych czynności z wykorzystaniem wskazanych aktywów
- d. ocena prawdopodobieństwa wystąpienia zagrożenia
- e. identyfikacja podatności, czyli czynników sprzyjających wystąpieniu zagrożenia
- f. ocena wpływu wystąpienia zagrożenia na poufność, integralność i dostępność danych
- g. wskazanie proponowanych działań zaradczych – zabezpieczeń chroniących przed wystąpieniem ryzyka, osób odpowiedzialnych za wdrożenie tych działań oraz terminu zrealizowania tych działań obowiązkowo w przypadku: wysokiego prawdopodobieństwa ryzyka, krytycznego wpływu wystąpienia ryzyka, niskiego poziomu istniejących zabezpieczeń.

§4

1. Jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, właściciel ryzyka, przed rozpoczęciem przetwarzania, dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (tzw. DPIA). Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. Właściciel ryzyka każdorazowo przy dokonywaniu oceny ryzyka i weryfikacji wykonywanych czynności przetwarzania w sytuacji podejrzenia wystąpienia wysokiego ryzyka jest zobowiązany do rozważenia konieczności przeprowadzenia DPIA. Służy do tego punkt 1 *Arkusza oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych* (DPIA).
3. Właściciel ryzyka obowiązkowo przeprowadza DPIA dla rodzajów operacji przetwarzania ujętych w ustanowionym przez organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych) i podanym do wiadomości publicznej wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Aktualny wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych dostępny jest na <https://uodo.gov.pl/p/najwazniejsze-tematy/administrator>
4. Dokonując DPIA właściciel ryzyka konsultuje się z Inspektorem ochrony danych Uniwersytetu.
5. DPIA przeprowadzoną przez właścicieli ryzyka opiniuje Zespół ds. wdrożenia ogólnego rozporządzenia o ochronie danych RODO powołany zarządzeniem wewnętrznym Nr R0161/18/2018 Rektora Akademii im. Jana Długosza w Częstochowie z dnia 21 lutego 2018r. w sprawie powołania Zespołu ds. wdrożenia Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (ogólnego rozporządzenia o ochronie danych RODO) w Akademii im. Jana Długosza w Częstochowie.
6. Wyniki DPIA zatwierdza administrator.

7. Właściciel ryzyka dokonuje DPIA na wzorze stanowiącym załącznik nr 2 do niniejszego zarządzenia.
8. W sytuacji, gdy DPIA wykaże, że przetwarzanie powodowałoby wysokie ryzyko, którego nie da się zminimalizować przy użyciu posiadanej technologii i możliwych do poniesienia kosztów wdrożenia to przed rozpoczęciem przetwarzania należy skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.

§5

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor
Uniwersytetu Humanistyczno-Przyrodniczego
im. Jana Długosza w Częstochowie
Prof. dr hab. Anna Wypych-Gawrońska