Zarządzenie Nr 109/2021
Rektora Politechniki Białostockiej
z dnia 23 września 2021 roku
w sprawie wprowadzenia w Politechnice Białostockiej zasad oceny ryzyka i oceny skutków dla ochrony danych osobowych (DPIA)

Na podstawie art. 23 ust. 2 ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021r. poz. 478, z późn. zm.), § 26 ust. 1 Statutu Politechniki Białostockiej oraz art. 24, art. 25, art. 32 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 (zwanego dalej RODO), zarządza się, co następuje:

§1
Wprowadza się w Politechnice Białostockiej zasady oceny ryzyka i oceny skutków dla ochrony danych osobowych (DPIA), jak w treści niniejszego zarządzenia.

§2
Definicje
Ilekroć w niniejszym zarządzeniu jest mowa o:
1) administratorze systemów informatycznych (ASI) – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu oraz wdrożenie i stosowanie zasad bezpieczeństwa danych w zakresie technicznych zabezpieczeń systemu informatycznego;
2) aktywach – należy przez to rozumieć zasoby wykorzystywane przez Politechnikę Białostocką w procesie przetwarzania danych osobowych np.: oprogramowanie, sprzęt i nośniki danych, sieć, personel i informacje, siedziba i wykorzystywana infrastruktura;
3) 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;
4) danych szczególnej kategorii – należy przez to rozumieć dane, o których mowa w art. 9 ust. 1 RODO tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.
5) dostępności danych – należy przez to rozumieć nieograniczoną możliwość korzystania z danych przez uprawnione osoby;
6) DPIA – należy przez to rozumieć ocenę skutków dla ochrony danych osobowych (ang. Data Protection Impact Assessment);
7) działaniach zaradczych – należy przez to rozumieć zaprojektowane działania, wdrażane w przypadku ryzyk na nieakceptowalnym poziomie, mające na celu zredukowanie istotności ryzyka do poziomu akceptowalnego;

8) integralności danych – należy przez to rozumieć zapewnienie, że dane nie zostały zmienione lub zniszczone w nieautoryzowany sposób;
9) zabezpieczeniach – należy przez to rozumieć wszystko, co zmniejsza ryzyko wystąpienia naruszenia (tj. zabezpieczenia organizacyjne, środki techniczne);
10) mapie ryzyka – należy przez to rozumieć graficzną metodę przedstawienia oceny istotności ryzyka za pomocą macierzy, która przedstawia zależność między wartością punktową prawdopodobieństwa wystąpienia zagrożenia a skutkami (oddziaływaniem) tego zagrożenia;
11) monitorowaniu ryzyka – należy przez to rozumieć ciągłą obserwację i nadzorowanie zidentyfikowanych ryzyk, identyfikację nowo powstałych zagrożeń oraz systematyczną ocenę skuteczności podejmowanych działań prewencyjnych;
12) naruszeniu ochrony danych osobowych – należy przez to rozumieć naruszenie, o którym mowa w art. 4 pkt 12 RODO, tj. naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
13) osobach nadzorujących zarządzanie ryzykiem – należy przez to rozumieć rektora, prorektorów, kanclerza, kwestora, dziekanów, dyrektora Szkoły Doktorskiej, dyrektora Akademickiego Liceum Ogólnokształcącego;
14) organie nadzorczym – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych;
15) podatności – należy przez to rozumieć słabość naszych aktywów lub zabezpieczeń, która może być wykorzystana i której skutkiem może być wystąpienie ryzyka;
16) poufności danych – należy przez to rozumieć zapewnienie niedostępności danych osobom/podmiotom nieuprawnionym;
17) poziomie ryzyka – należy przez to rozumieć wielkość ryzyka, będącą iloczynem wartości oceny prawdopodobieństwa wystąpienia zdarzenia i wartości oceny skutków;
18) prawdopodobieństwie (P) – należy przez to rozumieć możliwość wystąpienia zagrożenia;
19) procesie/czynności przetwarzania – należy przez to rozumieć zbiorcze oznaczenie wielu różnych operacji przetwarzania, które łączy realizacja tego samego celu;
20) 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;
21) pseudonimizacji – należy przez to rozumieć przetworzenie danych osobowych w taki sposób, żeby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
22) rejestrze ryzyka – należy przez to rozumieć zestawienie zidentyfikowanych istotnych ryzyk mających faktyczny wpływ na prawa i wolności osób fizycznych;
23) skutkach (S) – należy przez to rozumieć niepożądany wpływ na przetwarzane dane osobowe oraz prawa i wolności osób fizycznych, których dane dotyczą;

24) właścicielu procesu przetwarzania danych osobowych – należy przez to rozumieć osoby zarządzające ryzykiem tj. ASI, kierowników jednostek organizacyjnych lub pracowników zatrudnionych na samodzielnych stanowiskach, którzy realizują procesy związane z przetwarzaniem danych osobowych i którzy posiadają wiedzę o procesach m.in. czynnościach wykonywanych podczas procesów, uczestnikach procesów, danych przetwarzanych w ramach procesu oraz zasobach wykorzystywanych w procesie;
25) zagrożeniu – należy przez to rozumieć ryzyko wystąpienia naruszenia praw lub wolności osób związane z przetwarzaniem danych osobowych i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

§ 3

1. Wprowadza się zasady przeprowadzania oceny ryzyka w ochronie danych osobowych, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dla przetwarzanych danych osobowych, adekwatnego do zidentyfikowanych zagrożeń wynikających 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. Oceny ryzyka w ochronie danych osobowych dokonują właściciele procesów przetwarzania danych osobowych, w których realizowane są procesy przetwarzania danych osobowych oraz ASI, w zakresie szacowania ryzyka dla systemów informatycznych, w których są przetwarzane dane osobowe.
3. Ocenę ryzyka w ochronie danych osobowych przeprowadza się nie rzadziej niż raz na dwa lata w terminach określonych w § 6.
4. Niezależnie od analizy przeprowadzonej zgodnie z ust. 3, ocenę ryzyka należy dodatkowo przeprowadzić w następujących sytuacjach:
   1) wdrożenia nowego procesu lub jakichkolwiek zmian w sposobach przetwarzania w ramach procesu;
   2) zaistnienia zdarzenia będącego naruszeniem ochrony danych osobowych;
   3) na żądanie Inspektora Ochrony Danych (IOD);
5. Raport końcowy z analizy ryzyka, wskazujący poziom bezpieczeństwa przetwarzanych danych osobowych, sporządzony na podstawie złożonych rejestrów ryzyka, po zaopiniowaniu przez Zespół do spraw kontroli zarządczej, sporządza i przedkłada Rektorowi Zespół ds. oceny ryzyka w ochronie danych osobowych.
6. Za proces analizy ryzyka w ochronie danych osobowych odpowiadają osoby zarządzające ryzykiem.

§ 4

Cel oceny ryzyka w Uczelni

Ocena ryzyka jest procesem ciągłym, monitorującym adekwatność oraz skuteczność stosowanych oraz planowanych zabezpieczeń organizacyjnych i technicznych i ma na celu:

1) zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności danych osobowych;
2) definiowanie i wdrażanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku;
3) ocenę, czy stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem danych osobowych;
4) utrzymanie ryzyka na poziomie akceptowalnym.

§ 5

Metoda analizy ryzyka

1. Do przeprowadzenia analizy ryzyka w ochronie danych osobowych służy rejestr ryzyka będący załącznikiem nr 1 do zarządzenia.
2. Analizując ryzyko należy w szczególności uwzględnić:
   1) rodzaj przetwarzanych danych (dane zwykłe, dane szczególnych kategorii);
   2) skalę przetwarzanych danych (duże/małe zasoby danych);
   3) przekazywanie danych do państw trzecich;
   4) współpraca z podmiotami przetwarzającymi dane.
3. Oceniając ryzyko w ochronie danych osobowych należy wziąć pod uwagę ryzyko związane z przetwarzaniem tych danych mogące prowadzić w szczególności do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, których dane są przetwarzane, takich jak: utrata kontroli nad własnymi danymi lub ograniczenie praw, dyskryminacja, kradzież tożsamości, strata finansowa, naruszenie dobrego mienia, naruszenie poufności danych osobowych, nieuprawnione odwrócenie pseudonimizacji, znaczna szkoda gospodarcza lub społeczna.
4. Analizy ryzyka dokonuje właściciel procesu (współuczestniczący w procesie przetwarzania) oraz ASI w następujących etapach:
   1) identyfikacja czynności przetwarzania – proces w rejestrze czynności przetwarzania danych osobowych, (dla podobnych procesów przetwarzania można przeprowadzić jedną wspólną analizę ryzyka);
   2) wskazanie aktywów wykorzystywanych przy procesie przetwarzania danych osobowych;
   3) identyfikacja podatności tj. wskazanie słabej strony wykorzystywanych aktywów;
   4) identyfikacja zagrożeń;
   5) wskazanie istniejących zabezpieczeń;
   6) szacowanie prawdopodobieństwa wystąpienia określonego zagrożenia według skali określonej
      w załączniku nr 2 do zarządzenia, w tabeli nr 1;
   7) ocena poziomu skutków tego zagrożenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą według skali określonej w załączniku nr 2 do zarządzenia, w tabeli nr 2;
   8) oszacowanie poziomu ryzyka zgodnie z mapą ryzyka znajdującą się w załączniku nr 2 do zarządzenia, w tabeli nr 3.
5. Rejestr, o którym mowa w ust. 4 pkt 1 dostępny jest pod adresem www.pb.edu.pl/odo w zakładce „ODOorganizer”, po uprzednim zalogowaniu się (logowanie odbywa się na tych samych zasadach co logowanie na pocztę w domenie pb.edu.pl). W przypadku braku zidentyfikowanej jednostki/procesu w rejestrze czynności przetwarzania w rejestrze ryzyka, należy wpisać proces (czynność przetwarzania), podczas którego dochodzi do przetwarzania danych osobowych w jednostce organizacyjnej oraz dodatkowo przesłać uzupełniony rejestr czynności przetwarzania wykorzystując w tym celu formularz dostępny na stronie www.pb.edu.pl/odo w zakładce Dokumenty do pobrania→ Wzory dokumentów do pobrania.
6. W celu zidentyfikowania/dodania procesu w rejestrze czynności kierownik jednostki organizacyjnej, w której realizowany jest proces składa wniosek do Centrum Danych i Analiz Strategicznych (CDSiAS) o wpisanie procesu do rejestru. CDiAS na podstawie przesłanego wniosku aktualizuje rejestr czynności.

§ 6
Postępowanie z dokumentacją

1. Rejestr ryzyka, o którym mowa w § 5 ust.1 właściciel procesu oraz ASI, po zatwierdzeniu przez osobę nadzorującą, przekazuje w wersji papierowej i elektronicznej do Sekcji ds. Ryzyka w terminie do 31 października roku, w którym prowadzona jest analiza ryzyka w ochronie danych osobowych.
2. Sekcja ds. Ryzyka przekazuje Zespołowi ds. oceny ryzyka w ochronie danych osobowych zbiorczą dokumentację, o której mowa w ust. 1, do dnia 31 grudnia roku, w którym prowadzona jest analiza ryzyka w ochronie danych osobowych.
3. Dokumentację elektroniczną należy przesłać na adres e-mail: zrodo@pb.edu.pl.
4. W przypadku zidentyfikowania w rejestrze, o którym mowa w § 5 ust.1, ryzyka wysokiego lub bardzo wysokiego, osoby przeprowadzające ocenę ryzyka zobowiązane są postępować zgodnie
   z § 7 ust. 2 – 3.

§ 7
Postępowanie z ryzykiem

1. Wyróżnia się następujące rodzaje ryzyka:
   1) ryzyko niskie – ryzyko to nie ma znaczącego wpływu. Jest akceptowalne, nie wymaga podejmowania działań zaradczych i należy je monitorować;
   2) ryzyko średnie – ryzyko to ma umiarkowany wpływ na realizację celów i zadań. Jest akceptowalne, nie wymaga podejmowania działań zaradczych, należy je monitorować (w przypadku poziomu ryzyka 5-6) lub rozważyć potrzebę wprowadzenia działań zaradczych (w przypadku poziomu ryzyka 8-9). Poziom ryzyka określa tabela nr 3 w załączniku nr 2 do zarządzenia;
   3) ryzyko wysokie i bardzo wysokie - jest nieakceptowalne, wymaga natychmiastowych działań zaradczych, przez podjęcie natychmiastowych działań zaradczych i wdrożeniu odpowiedniej reakcji na ryzyko.
2. Postępowanie z ryzykiem wysokim lub bardzo wysokim polega na:
   1) przeciwdziałaniu (obniżaniu ryzyka) – podjęciu działań zaradczych mających na celu zmniejszenie istotności ryzyka;
   2) unikaniu ryzyka – eliminacji działań powodujących ryzyko m.in. poprzez modyfikację procedur, które mają na celu wyeliminowanie potencjalnych podatności będących przyczyną wystąpienia ryzyka;
   3) transferze ryzyka – przeniesieniu ryzyka w całości lub w części na inną organizację np. poprzez powierzenie procesów przetwarzania.
3. W przypadku postępowania z ryzykiem na poziomie wysokim lub bardzo wysokim, osoby dokonujące oceny ryzyka w ochronie danych osobowych, a w przypadku systemów informatycznych również ASI, są zobowiązane do wskazania w rejestrze ryzyka, o którym mowa w § 5 ust. 1:
   1) działań zaradczych potwierdzających wprowadzenie środków zabezpieczających;
   2) kolejności podejmowanych działań zmierzających do zminimalizowania ryzyka;
   3) terminu realizacji proponowanych działań.

§ 8
Procedura przeprowadzania oceny skutków dla ochrony danych osobowych (DPIA)

1. Obowiązkowo DPIA przeprowadza właściciel procesu w odniesieniu do operacji przetwarzania ujętych w wykazie ustanowionym i podanym do publicznej wiadomości,

na podstawie art. 35 ust. 4 RODO przez organ nadzorczy. Aktualny wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony znajduje się w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych (https://uodo.gov.pl/pl/p/najwazniejsze-tematy/administrator).

2. Podczas szacowania ryzyka w ochronie danych osobowych właściciele procesów są zobowiązani do okresowego przeglądu procesów przetwarzania pod kątem konieczności przeprowadzenia DPIA. Właściciel procesu przeprowadza również DPIA każdorazowo na żądanie Zespołu ds. oceny ryzyka w ochronie danych osobowych lub Inspektora Ochrony Danych.
3. DPIA w Politechnice Białostockiej obowiązkowo powinna być przeprowadzona, 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. W szczególności DPIA przeprowadza się w przypadkach:
   1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osoby fizyczne;
   2) przetwarzania na dużą skalę danych szczególnej kategorii lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO;
   3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
4. W przypadkach innych niż określone w ust. 1 i ust. 3, gdy poziom ryzyka określono jako wysoki lub bardzo wysoki, Zespół ds. oceny w ochronie danych osobowych rekomenduje, do których procesów obowiązkowe jest przeprowadzenie DPIA.
5. W przypadku planowania nowych operacji przetwarzania danych osobowych DPIA powinna być dokonywana przed rozpoczęciem przetwarzania danych.
6. Właściciele procesów, dokonując DPIA, konsultują się w tej sprawie z Inspektorem Ochrony Danych.
7. Dokumentacja przeprowadzonej DPIA przechowywana jest wraz z oceną ryzyka, dla którego została sporządzona.
8. DPIA powinna zawierać przede wszystkim:
   1) opis operacji przetwarzania danych osobowych i cel ich przetwarzania;
   2) ocenę niezbędności przetwarzania danego rodzaju danych oraz wskazanie, czy danego ryzykownego działania można uniknąć, a jeśli nie, to wskazanie, jakie środki zapobiegawcze przyjęto;
   3) ocenę ryzyka naruszenia praw i wolności podmiotów danych osobowych;
   4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie przepisów RODO.
9. Jeżeli DPIA wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.
10. Dokonanie DPIA dokumentowane jest w formie arkusza oceny DPIA, którego wzór stanowi załącznik nr 3 do zarządzenia.

§ 9
Monitorowanie ryzyka

1. Proces monitorowania ryzyka i DPIA jest procesem ciągłym.
2. Osoby zarządzające ryzykiem zobowiązane są do bieżącego monitorowania poziomu ryzyk ujętych w rejestrze ryzyka poprzez:
   1) dokonywanie na bieżąco oceny prawdopodobieństwa wystąpienia ryzyka i jego skutków;
   2) identyfikację oraz analizę nowych ryzyk;
   3) przegląd stanu realizacji planu postępowania z ryzykiem nieakceptowalnym;
   4) ocenę funkcjonowania działań zaradczych pod kątem ich adekwatności i skuteczności.

§ 10
Zespół ds. oceny ryzyka w ochronie danych osobowych (ZRODO)

1. Powołuję w Politechnice Białostockiej Zespół ds. oceny ryzyka (ZRODO) w ochronie danych osobowych w następującym składzie:
   1) mgr Tomasz Klim – przewodniczący;
   2) mgr Katarzyna Karp – protokolant;
   3) mgr Marta Płońska – Wasieńko;
   4) mgr Wojciech Puchalski;
   5) mgr inż. Marcin Rodzianko;
   6) mgr inż. Piotr Zalewski.
2. Za obsługę ZRODO oraz zebranie rejestrów odpowiada Sekcja ds. Ryzyka.
3. W posiedzeniach ZRODO mogą uczestniczyć, z głosem doradczym, osoby zaproszone przez przewodniczącego.
4. Zespół zostaje powołany do dnia 31 sierpnia 2024 roku.
5. Do zadań ZRODO, w zakresie oceny ryzyka i DPIA, należy:
   1) koordynowanie procesu identyfikacji i analizy ryzyka;
   2) rekomendacja konieczności sporządzania DPIA na podstawie przekazanej analizy ryzyka;
   3) sporządzenie i przekazanie Zespołowi do spraw kontroli zarządczej, w terminie do dnia 28 lutego roku kalendarzowego, w którym prowadzona jest analiza ryzyka w ochronie danych osobowych:
      a) sprawozdań z procesu zarządzania ryzykiem,
      b) rekomendacji do podjęcia działań;
   4) sprawowanie nadzoru nad terminowością i skutecznością działań zaradczych wdrażanych dla ryzyka na nieakceptowalnym poziomie, poprzez:
      a) sprawdzenie, czy nastąpiło obniżenie poziomu istotności ryzyka do akceptowalnego,
      b) przedłożenie rektorowi informacji o działaniach podjętych przez osoby zarządzające ryzykiem;
   5) przekazywanie Zespołowi do spraw kontroli zarządczej informacji o istotnych zdarzeniach.
6. ZRODO przekazuje Rektorowi, po zaopiniowaniu przez Zespół do spraw kontroli zarządczej, ostateczne sprawozdanie wraz z rekomendacją działań.
7. W celu wykonania zadań Zespołu, Przewodniczący ZRODO może występować na piśmie o przedkładanie dodatkowych wyjaśnień.

8. Przewodniczący ZRODO może zaprosić do udziału w pracach Zespołu, z głosem doradczym, osoby zarządzające, których wiedza będzie niezbędna do zapewnienia prawidłowego wykonania zadań wyznaczonych ZRODO.

§ 12
Odpowiedzialnymi za prawidłową realizację zarządzenia czynię osoby zarządzające ryzykiem tj. ASI, kierowników jednostek organizacyjnych lub pracowników zatrudnionych na samodzielnych stanowiskach, którzy realizują procesy związane z przetwarzaniem danych osobowych.

§ 13
Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

dr hab. inż. Marta Kosior-Kazberuk, prof. PB