Zarządzenie Nr 108/2025
Rektora Politechniki Białostockiej
z dnia 5 listopada 2025 roku

w sprawie wprowadzenia w Politechnice Białostockiej zasad oceny ryzyka i oceny skutków dla ochrony danych osobowych (DPIA) oraz oceny ryzyka bezpieczeństwa informacji

Na podstawie art. 23 ust. 2 ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce
(Dz. U. z 2024 r. poz. 1571 z późn. zm.) § 26 ust. 1 Statutu Politechniki Białostockiej oraz art. 24, art. 25, art. 32 i 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) oraz oceny ryzyka bezpieczeństwa informacji jak w treści niniejszego zarządzenia.

§2
Definicje
Ilekroć w niniejszym zarządzeniu jest mowa o:
1) aktywach – należy przez to rozumieć zasoby wykorzystywane przez Politechnikę Białostocką
   w procesie przetwarzania informacji, w tym danych osobowych np.: personel, obiekty, urządzenia, sprzęt komputerowy, oprogramowanie, elektroniczne nośniki informacji, umiejętności, technologie, informacje, dane itp. które są niezbędne do prowadzenia działalności Uczelni;
2) danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej
   do zidentyfikowania osobie fizycznej (zwanej dalej „osobą, 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;

3) 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;
4) dostępności danych – należy przez to rozumieć nieograniczoną możliwość korzystania z danych przez uprawnione osoby;
5) DPIA – należy przez to rozumieć ocenę skutków dla ochrony danych osobowych (ang. Data Protection Impact Assessment);
6) działaniach zaradczych – należy przez to rozumieć zaprojektowane działania wprowadzające zabezpieczenia, wdrażane w przypadku ryzyk na nieakceptowalnym poziomie, mające na celu zredukowanie istotności ryzyka do poziomu akceptowalnego;
7) incydent – niespodziewane lub niepożądane zdarzenie lub seria takich zdarzeń świadczących
o naruszeniu lub wysokim ryzyku naruszenia bezpieczeństwa informacji i danych osobowych;
8) integralności danych – należy przez to rozumieć zapewnienie, że dane nie zostały zmienione
lub zniszczone w nieautoryzowany sposób;
9) 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;
10) monitorowaniu ryzyka – należy przez to rozumieć ciągłą obserwację i nadzorowanie zidentyfikowanych ryzyk, identyfikację nowo powstałych zagrożeń oraz systematyczną ocenę skuteczności podejmowanych działań prewencyjnych;
11) 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;

12) organie nadzorczym – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych;
13) osobach nadzorujących zarządzanie ryzykiem – należy przez to rozumieć rektora, prorektorów, kanclerza, kwestora, dziekanów, dyrektora Szkoły Doktorskiej, dyrektora Akademickiego Liceum Ogólnokształcącego;
14) osobach zarządzających ryzykiem bezpieczeństwa informacji i przetwarzania danych osobowych/ osoby zarządzające ryzykiem – należy przez to rozumieć: kierowników jednostek organizacyjnych i pracowników zatrudnionych na samodzielnych stanowiskach, którzy realizują procesy związane z przetwarzaniem informacji i danych osobowych, posiadają wiedzę o procesach m.in. o czynnościach wykonywanych podczas procesów, uczestnikach procesów, danych przetwarzanych w ramach procesu oraz aktywach wykorzystywanych w procesie;
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 zagrożenia 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 bezpieczeństwa informacji – należy przez to rozumieć zestawienie zidentyfikowanych istotnych ryzyk mających faktyczny wpływ na bezpieczeństwo informacji;
23) rejestrze ryzyka ochrony danych osobowych – należy przez to rozumieć zestawienie zidentyfikowanych istotnych ryzyk mających faktyczny wpływ na ochronę danych osobowych;
24) skutkach (S) – należy przez to rozumieć następstwo naruszenia bezpieczeństwa informacji i ochrony danych osobowych;
25) zabezpieczeniach – należy przez to rozumieć wszystko, co zmniejsza ryzyko wystąpienia naruszenia
(tj. zabezpieczenia organizacyjne, środki techniczne);
26) zagrożeniu – należy przez to rozumieć ryzyko wystąpienia incydentu bezpieczeństwa informacji oraz ochrony danych osobowych.

§ 3

1. Wprowadza się zasady przeprowadzania oceny ryzyka bezpieczeństwa informacji i danych osobowych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dla przetwarzanych danych, 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. Za proces oceny ryzyka bezpieczeństwa informacji i danych osobowych odpowiadają osoby zarządzające ryzykiem.
3. Administratorzy Systemów Informatycznych i pracownicy zatrudnieni na stanowiskach ds. informatyki przeprowadzają ocenę ryzyka bezpieczeństwa informacji i ochrony danych osobowych dla systemów teleinformatycznych zgodnie z wytycznymi Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji.
4. Ocenę ryzyka bezpieczeństwa informacji i danych osobowych przeprowadza się co roku w terminach określonych w § 8.
5. Niezależnie od analizy przeprowadzonej zgodnie z ust. 2 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 bezpieczeństwa informacji i ochrony danych osobowych;

3) każdorazowo na żądanie Inspektora Ochrony Danych/Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji.

§ 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;
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 bezpieczeństwem informacji i danych osobowych;
4) utrzymanie ryzyka na poziomie akceptowalnym.

§ 5
Metoda analizy ryzyka w ochronie danych osobowych

1. Analizy ryzyka w ochronie danych osobowych dokonują osoby zarządzające ryzykiem tj. kierownicy jednostek i pracownicy zatrudnieni na samodzielnych stanowiskach - zgodnie ze wzorem rejestru ryzyka stanowiącym załącznik nr 1.
2. Każda osoba zarządzająca ryzykiem w procesie analizy ryzyka zobowiązana jest do uwzględnienia wszystkich aktywów wykorzystywanych w procesach, w ramach których przetwarzane są dane osobowe w jednostce.
3. Analizując ryzyko należy w szczególności uwzględnić:
   1) procesy przetwarzania danych osobowych zgłoszone do Rejestru czynności przetwarzania dostępne 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);
   2) rodzaj przetwarzanych danych (dane zwykłe, dane szczególnych kategorii);
   3) skalę przetwarzanych danych (duże/małe zasoby danych);
   4) przekazywanie danych do państw trzecich;
   5) współpraca z podmiotami przetwarzającymi dane.

4. 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.
5. Analiza ryzyka dokonywana jest w następujących etapach:
   1) wskazanie aktywów wykorzystywanych do przetwarzania danych osobowych;
   2) identyfikacja ryzyka tj. zagrożeń i podatności, wskazanie słabej strony wykorzystywanych aktywów;
   3) wskazanie istniejących zabezpieczeń;
   4) szacowanie prawdopodobieństwa wystąpienia określonego zagrożenia według skali określonej
      w załączniku nr 3 do zarządzenia, w tabeli nr 1;
   5) 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 3, do zarządzenia, w tabeli nr 2;
   6) oszacowanie poziomu ryzyka zgodnie z mapą ryzyka znajdującą się w załączniku nr 3 do zarządzenia, w tabeli nr 4.

§ 6

Metoda analizy ryzyka bezpieczeństwa informacji

1. Do przeprowadzenia analizy ryzyka bezpieczeństwa informacji służy rejestr ryzyka będący załącznikiem nr 2 do zarządzenia.
2. Analizy ryzyka bezpieczeństwa informacji dokonują osoby zarządzające ryzykiem tj. kierownicy jednostek oraz pracownicy zatrudnieni na samodzielnych stanowiskach w następujących etapach:
   1) wskazanie aktywów wykorzystywanych do przetwarzania informacji;
   2) identyfikacja ryzyka tj. zagrożeń i podatności, wskazanie słabej strony wykorzystywanych aktywów;
   3) wskazanie istniejących zabezpieczeń;
   4) szacowanie prawdopodobieństwa wystąpienia określonego zagrożenia według skali określonej
      w załączniku nr 3 do zarządzenia, w tabeli nr 1;
   5) ocena poziomu skutków tego zagrożenia według skali określonej w załączniku nr 3 do zarządzenia, w tabeli nr 3;

6) oszacowanie poziomu ryzyka zgodnie z mapą ryzyka znajdującą się w załączniku nr 3 do zarządzenia, w tabeli nr 4.

§ 7
Monitorowanie ryzyka

1. Proces monitorowania ryzyka 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.

§ 8
Postępowanie z dokumentacją

1. Rejestry ryzyka, o którym mowa w § 5 ust.1 i § 6 ust.1 osoby zarządzające ryzykiem, przekazują do zatwierdzenia osobom nadzorującym.
2. Zbiorcze rejestry z pionu/wydziału, po zatwierdzeniu przez osoby nadzorujące należy przekazać
   w wersji papierowej i elektronicznej do Sekcji ds. Ryzyka, w terminie do 31 marca każdego roku.
3. Sekcja ds. Ryzyka przekazuje Zespołowi ds. oceny ryzyka bezpieczeństwa informacji i danych osobowych zbiorczą dokumentację, o której mowa w ust. 2, do 15 maja każdego roku.
4. Dokumentację elektroniczną należy przesłać na adres e-mail: zrodo@pb.edu.pl.
5. W przypadku zidentyfikowania w rejestrze, o którym mowa w § 5 ust.1 i § 6 ust.1 ryzyka średniego i wysokiego osoby zarządzające ryzykiem zobowiązane są postępować zgodnie z § 9 ust. 2 – 3.

§ 9
Postępowanie z ryzykiem

1. Wyróżnia się następujące poziomy ryzyka:
   1) ryzyko niskie – ryzyko to nie ma znaczącego wpływu. Jest akceptowalne, nie wymaga podejmowania działań zaradczych. Należy je okresowo monitorować;
   2) ryzyko średnie – ryzyko to ma umiarkowany wpływ na bezpieczeństwo informacji i danych osobowych. Jest nieakceptowalne,

wymaga zaplanowania i wdrożenia działań zaradczych. Należy je stale monitorować;

3) ryzyko wysokie – jest nieakceptowalne, wymaga natychmiastowych działań zaradczych
i wdrożenia odpowiedniej reakcji na ryzyko. Należy je stale monitorować.

2. Postępowanie z ryzykiem średnim i 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 nieakceptowalnym na poziomie średnim lub wysokim, osoby zarządzające ryzykiem bezpieczeństwa informacji i danych osobowych są zobowiązane do wskazania w rejestrze ryzyka, o którym mowa w § 5 ust. 1 i § 6 ust. 1:
   3. opisu planowanych działań zaradczych;
   4. kolejności podejmowanych działań zmierzających do zminimalizowania ryzyka;
   5. terminu realizacji proponowanych działań.

§ 10

Procedura przeprowadzania oceny skutków dla ochrony danych osobowych (DPIA)

1. Obowiązkowo DPIA przeprowadza osoba zarządzająca ryzykiem 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://monitorpolski.gov.pl/MP/2019/666).
2. Podczas szacowania ryzyka w ochronie danych osobowych osoby zarządzające ryzykiem są zobowiązane do okresowego przeglądu procesów przetwarzania pod kątem konieczności przeprowadzenia DPIA. Osoba zarządzająca ryzykiem przeprowadza również DPIA każdorazowo na żądanie Zespołu ds. oceny ryzyka bezpieczeństwa informacji i 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, Zespół ds. oceny ryzyka bezpieczeństwa informacji i danych osobowych rekomenduje, do których procesów obowiązkowe jest przeprowadzenie DPIA.
5. W przypadku planowania nowych operacji przetwarzania danych osobowych, dla których ocena skutków dla ochrony danych osobowych jest wymagana zgodnie z postanowieniami niniejszego paragrafu, DPIA powinna być dokonywana przed rozpoczęciem przetwarzania danych.
6. Osoby zarządzająca ryzykiem, 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 4 do zarządzenia.

§ 11

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

§ 12

Traci moc 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).

§ 13

Zarządzenie wchodzi w życie z dniem podpisania.

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

Załącznik nr 1 do Zarządzenia Nr 108/2025 Rektora PB

Rejestr Ryzyka w Ochronie Danych

Na rok:

(data sporządzenia rejestru ryzyka)

.....

Uzupełniamy w przypadku ryzyka na poziomie średnim i wysokim

Lp.	Aktywa	Podatność	Zagrożenie	Istniejące zabezpieczenia 1	Istniejące zabezpieczenia 2	Istniejące zabezpieczenia 3	Prawdopodobieństwo wystąpienia ryzyka	Skutki (oddziaływanie)	Poziom ryzyka	Czy ryzyko jest na akceptowalnym poziomie TAK/NIE	Postępowanie z ryzykiem	Osoba zarządzająca ryzykiem, (w przypadku ryzyka średniego i wysokiego odpowiedzialna za wdrożenie działań)	Określenie działań zaradczych - zabezpieczeń do wdrożenia (obowiązkowo dotyczy ryzyka średniego i wysokiego)	Termin zrealizowania działań	Uwagi

.....

sporządził (data i podpis)

.....

zatwierdził (data i podpis)

Osoby sporzadzające osoby zarządzające ryzykiem tj. kierownicy jednostek organizacyjnych/ pracownicy zatrudnieni na samodzielnych stanowiskach

Osoby zatwierdzające rektor, prorektorzy, kanclerz, kwestor, dziekani, dyrektor Szkoły Doktorskiej, dyrektor Akademickiego Liceum Ogólnokształcącego

UWAGA!!! Prosimy o dodawanie wierszy poprzez kopiowanie wierszy już istniejących!!

Załącznik nr 2 do Zarządzenia Nr 108 /2025 Rektora PB

Rejestr Ryzyka Bezpieczeństwa

Na rok:

(data sporządzenia rejestru ryzyka)

.....

*(Nazwa Pionu/Wydziału/Jednostki)**

Uzupełniamy w przypadku ryzyka na poziomie średnim i wysokim

Lp.	Aktywa	Podatność	Zagrożenie	Istniejące zabezpieczenia 1	Istniejące zabezpieczenia 2	Istniejące zabezpieczenia 3	Prawdopodobieństwo wystąpienia ryzyka	Skutki (oddziaływanie)	Poziom ryzyka	Czy ryzyko jest na akceptowalnym poziomie TAK/NIE	Postępowanie z ryzykiem	Osoba zarządzająca ryzykiem, (w przypadku ryzyka średniego i wysokiego odpowiedzialna za wdrożenie działań)	Określenie działań zaradczych - zabezpieczeń do wdrożenia (obowiązkowo dotyczy ryzyka średniego i wysokiego)	Termin zrealizowania działań	Uwagi

.....
sporządził (data i podpis)

.....
zatwierdził (data i podpis)

* obowiązkowo podać w kol.,,Proces" nazwę systemu teleinformatycznego (dotyczy kol. ,,Aktywa")

Osoby sporzadz osoby zarządzające ryzykiem tj. kierownicy jednostek organizacyjnych lub pracownicy zatrudnieni na samodzielnych stanowiskach
Osoby zatwierdz rektor, prorektorzy, kanclerz, kwestor, dziekani, dyrektor Szkoły Doktorskiej, dyrektor Akademickiego Liceum Ogólnokształcącego

Uwaga!!! Prosimy o dodawanie wierszy poprzez kopiowanie wierszy już istniejących!!

Załącznik nr 3 do Zarządzenia Nr 108/2025 Rektora PB

Tabela nr 1. Skala prawdopodobieństwa wystąpienia zagrożenia, którego skutkiem będzie naruszenie bezpieczeństwa informacji i ochrony danych osobowych.

Ocena Prawdopodobieństwa Wystąpienia Zagrożenia		
Wartość punktowa	**Nazwa**	**Opis**
1	Rzadkie	Zdarzenie raczej nie wystąpi lub możliwość jego wystąpienia jest znikoma (bliska zeru). Zdarzenie nie występowało w przeszłości.
2	Mało prawdopodobne	Zdarzenie może wystąpić sporadycznie. Materializowało się w ciągu ostatniego roku.
3	Możliwe	Wystąpienie zagrożenia jest realne. Zdarzenie wystąpiło w ciągu ostatniego pół roku.
4	Prawdopodobne	Istnieją racjonalne przesłanki, by ocenić, że zdarzenie wystąpi. Materializowało się w przeciągu ostatniego kwartału.
5	Prawie pewne	Istnieją racjonalne przesłanki, by ocenić, że zdarzenie wystąpi w najbliższym czasie.

Tabela nr 2. Skala poziomu skutków wystąpienia zagrożenia w ochronie danych osobowych

Ocena Skutków Wystąpienia Zagrożenia		
Wartość punktowa	**Nazwa**	**Opis**
1	Nieznaczne	Naruszenie nie będzie wpływało na prawa i wolności osób fizycznych. Brak wpływu na realizowane działania i reputację.
2	Małe	Możliwe do usunięcia w łatwy sposób konsekwencje dla osób, których dane dotyczą. Osoby, których dane dotyczą nie odczują skutków. Naruszenie nie może skutkować poważnym wpływem na prawa i wolności osób fizycznych (np. ich sferę materialną lub dobra osobiste).
3	Średnie	Możliwe do usunięcia w łatwy sposób konsekwencje dla osób, których dane dotyczą. Naruszenie, w zależności od kontekstu danego zdarzenia, w niektórych przypadkach może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową lub wszelką inną znaczną szkodą gospodarczą lub społeczną.
4	Wysokie	Istotne, trudne do odwrócenia konsekwencje dla osób, których dane dotyczą. Naruszenie może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową lub wszelką inną znaczną szkodą gospodarczą lub społeczną. Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych osób poszkodowanych.

5	Bardzo wysokie	Istotne, nieodwracalne konsekwencje dla osób, których dane dotyczą. Naruszenie może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową lub wszelką inną znaczną szkodą gospodarczą lub społeczną. Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób poszkodowanych.

Tabela nr 3. Skala poziomu skutków wystąpienia zagrożenia w bezpieczeństwie informacji

Ocena Skutków Wystąpienia Zagrożenia W Bezpieczeństwie Informacji		
Wartość punktowa	**Nazwa**	**Opis**
1	Nieznaczne	Naruszenie bezpieczeństwa nie rodzi praktycznie żadnych skutków dla Uczelni.
2	Małe	Naruszone jest bezpieczeństwo aktywa, jednak nie rodzi ono konsekwencji prawnych, wizerunkowych i innych poważnych skutków dla Uczelni.
3	Średnie	W wyniku naruszenia bezpieczeństwa aktywa, średnio zakłócone są procesy zależne od korzystania z aktywa. W wyniku zadziałania zagrożenia, Uczelnia odczuwa średnie zakłócenie natury technicznej oraz organizacyjnej.
4	Wysokie	W wyniku naruszenia bezpieczeństwa aktywa, poważnie zakłócone są procesy zależne od korzystania z aktywa. W wyniku zadziałania zagrożenia, Uczelnia odczuwa poważne zakłócenie natury technicznej oraz organizacyjnej.

5	Bardzo wysokie	Bardzo poważne naruszenie bezpieczeństwa aktywa, które może rodzić konsekwencje prawne, wizerunkowe oraz dla ciągłości działania.

Tabela nr 4. Mapa ryzyka

Skutek		**Mapa Ryzyka**				
Bardzo wysokie	**5**	**5**	**10**	**15**	**20**	**25**
Wysokie	**4**	**4**	**8**	**12**	**16**	**20**
Średnie	**3**	**3**	**6**	**9**	**12**	**15**
Małe	**2**	**2**	**4**	**6**	**8**	**10**

Nieznaczne	**1**	**1**	**2**	**3**	**4**	**5**
		1	**2**	**3**	**4**	**5**
		RZADKIE	**MAŁO PRAWDOPODOBNE**	**MOŻLIWE**	**PRAWDOPODOBNE**	**PRAWIE PEWNE**
		PRAWDOPODOBIEŃSTWO				

Poziom Ryzyka (R)	**1-9**	**10-15**	**16-25**
	NISKIE	***ŚREDNIE***	***WYSOKIE***

Poziom ryzyka (R)	**Zasady postępowania**
Niski	Poziom ryzyka akceptowalny – okresowe monitorowanie
Średni	Poziom ryzyka nieakceptowalny – niezbędne stałe monitorowanie, przygotowanie propozycji wprowadzenia działań zaradczych
Wysoki	Poziom ryzyka nieakceptowalny – niezbędne stałe monitorowanie, natychmiastowe wprowadzenie działań zaradczych

Załącznik nr 4 do Zarządzenia Nr 108/2025 Rektora PB

Arkusz Oceny DPIA

1. Informacje ogólne:

1.1.	**Cel i zakres analizy (proces/system przetwarzający dane osobowe)**	
1.2.	**Cel przetwarzania danych osobowych**	
1.3.	**Przepisy prawa, umowy i inne zobowiązania warunkujące przetwarzanie danych; podstawa prawna przetwarzania danych**	
1.4.	**Kategorie osób, których dane dotyczą**	
1.5.	**Orientacyjna ilość osób, których dane będą przetwarzane**	
1.6.	**Kategorie danych osobowych – planowany zakres przetwarzanych danych w podziale na kategorie osób**	
1.7.	**Kategorie danych osobowych – planowany zakres danych szczególnie chronionych w podziale na kategorie osób**	
1.8.	**Podmioty zaangażowane w przetwarzanie danych osobowych (inni administratorzy,**	

	współadministratorzy, podmioty przetwarzające)	
1.9.	**Okres retencji danych (kiedy dane przestaną być użyteczne do celu przetwarzania)**	
1.10.	**Korzyści oferowane podmiotowi danych w związku z przetwarzaniem jego danych**	

2. Opis operacji przetwarzania:

2.1.	**Zbieranie danych – należy dokonać opisu w jaki sposób dane będą zbierane – z jakich źródeł, jakimi kanałami będą pozyskiwane**	
2.2.	**Przechowywanie – gdzie i w jakich zasobach dane będą przechowywane**	
2.3.	**Używanie – w jaki sposób dane będą wykorzystywane i jakie operacje będą na nich wykonywane (w szczególności czy planowane jest profilowanie, zautomatyzowane podejmowanie decyzji, łącznie z innymi danymi, porównywanie), przez jakie jednostki dane będą przetwarzane, przez które podmioty przetwarzające**	

2.4.	**Przekazywanie – które podmioty zewnętrzne będą miały możliwość dostępu do danych niezależnie od postaci w jakiej te dane będą przekazane ani roli podmiotu zewnętrznego (inny ADO/podmiot przetwarzający). W jakim zakresie i w jakim celu dane będą przekazywane podmiotom zewnętrznym?**	
2.5.	**Przekazywanie danych poza EOG- jeżeli TAK to czy zidentyfikowano zabezpieczenia danych?**	
2.6.	**Usuwanie – w jakich okolicznościach, czy na czyj wniosek dane będą usuwane? W jakim zakresie będzie to następowało i z jakich zasobów?**	

3. Identyfikacja i opis aktywów wspierających przetwarzanie danych osobowych:

3.1.	**Główne systemy informatyczne wspierające analizowany proces (należy określić nazwę systemu informatycznego oraz zidentyfikować główne komponenty systemu i określić czy znajdują się w sieci informatycznej zrządzanej przez ADO czy poza nią**	
3.2.	**Aplikacje biurowe i urządzenia końcowe**	

	wykorzystywane przez użytkowników do przetwarzania danych osobowych (należy określić nazwę aplikacji/urządzenia oraz miejsce przechowywania danych (urządzenia mobilne, stacje robocze, zasób zdalny)	
3.3.	**Zasoby papierowe (należy określić czy będzie dochodziło do przetwarzania danych osobowych w formie tradycyjnej oraz miejsce przechowywania zasobu)**	

4. Opis środków zapewniających sposób realizacji praw podmiotów danych oraz zgodność z wymaganiami prywatności (konieczność ich wdrożenia jest niezależna od wyników analizy ryzyka):

4.1. Sposób realizacji praw podmiotów:

Lp.	**Prawo podmiotu danych**	**Opis planowanego sposobu realizacji z wykazem potrzeb w zakresie wdrożenia niezbędnych rozwiązań organizacyjnych i technologicznych minimalizujących prawdopodobieństwo braku realizacji praw podmiotu danych**
1.	**Informacja przekazywana osobom, których dane przetwarzamy (realizacja obowiązków informacyjnych z art. 13 i 14 RODO)**	
2.	**Zapewnienie swobodnego wyrażenia zgody przez**	

	podmiot danych (art. 7 RODO)	
3.	**Zapewnienie możliwości realizacji praw osób, których dane dotyczą (art. 15-21 RODO)**	

4.2. Zasady ochrony danych:

Lp.	**Wymagania z zakresie ochrony prywatności**	**Planowane lub istniejące działania i zabezpieczenia zapewniające spełnienie wymagania przez analizowanie operacji przetwarzania**
1.	**Czy istnieje konkretny, prawnie uzasadniony cel administratora**	
2.	**Czy przetwarzanie danych jest zgodne z prawem (legalność)**	
3.	**Ograniczanie zbierania i minimalizacja danych**	
4.	**Ograniczanie używania i ujawniania**	
5.	**Prawidłowość danych**	

5. **Szacowanie ryzyka dla prywatności:** należy dołączyć rejestr ryzyka w ochronie danych osobowych sporządzony według zasad określonych w odrębnym zarządzeniu dotyczącym oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą w związku z przetwarzaniem danych osobowych, z uwzględnieniem analizy wpływu skutków na osobę fizyczną, której dane dotyczą.

6. Standardy związane z przetwarzaniem */jeżeli dotyczy należy wymienić standardy mające zastosowanie /*

Zatwierdzone kodeksy postępowania	

Certyfikat	
ISO/IEC 27001	
Inne (wymienić)	

7. Opinia i podpis Inspektora Ochrony Danych.

……
……
……
……

……

(data i podpis IOD)

8. Opinie osób, których dane dotyczą - jeśli jest taka potrzeba.

……
……
……
……

9. Decyzja w sprawie konsultacji z Prezesem Urzędu Ochrony Danych */w przypadku ryzyka wysokiego i bardzo wysokiego – konieczna konsultacja/*

……
……
……..

10. Decyzja Rektora/osoby upoważnionej

Zatwierdzam/nie zatwierdzam