Zarządzenie nr 161 /2025
Rektora Uniwersytetu Rzeszowskiego
z dnia 8 lipca 2025 r.
w sprawie wprowadzenia Regulaminu Ochrony Danych Osobowych Uniwersytetu Rzeszowskiego

Na podstawie 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 związku z zarządzeniem nr 159/2025 Rektora Uniwersytetu Rzeszowskiego z dnia 8 lipca 2025r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych, Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz wytycznych w zakresie naruszenia ochrony danych osobowych w Uniwersytecie Rzeszowskim zarządzam, co następuje:

§1

1. Wprowadza się „Regulamin Ochrony Danych Osobowych Uniwersytetu Rzeszowskiego" stanowiący załącznik nr 1 do niniejszego zarządzenia.

§2

1. Regulamin podlega okresowym przeglądom i aktualizacjom.
2. Każdy pracownik, student i współpracownik Uniwersytetu jest zobowiązany do zapoznania się z niniejszym Regulaminem i jego przestrzegania.

§3

1. Nadzór nad wykonaniem niniejszego zarządzenia powierzam Inspektorowi Ochrony Danych Uniwersytetu Rzeszowskiego.

§4

1. Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR
UNIWERSYTETU RZESZOWSKIEGO

prof. dr hab. Adam Reich

załącznik nr 1 do Zarządzenie nr 161 /2025 Rektora Uniwersytetu Rzeszowskiego z dnia 8 lipca 2025 r. w sprawie wprowadzenia Regulaminu Ochrony Danych Osobowych Uniwersytetu Rzeszowskiego

Regulamin Ochrony Danych Osobowych Uniwersytetu Rzeszowskiego

§ 1
Postanowienia ogólne

1. Niniejszy Regulamin określa zasady przetwarzania i ochrony danych osobowych w Uniwersytecie Rzeszowskim (dalej: „Uniwersytet").
2. Celem Regulaminu jest zapewnienie zgodności działań Uniwersytetu z przepisami dotyczącymi ochrony danych osobowych, w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, innymi przepisami krajowymi i unijnymi regulującymi przetwarzanie danych oraz jak najlepsze zapoznanie pracowników i współpracowników z zasadami ochrony danych osobowych. W treść niniejszego regulaminu wchodzą postanowienia zawarte w polityce bezpieczeństwa oraz instrukcji zarządzania systemami informatycznymi, które są przydatne każdej osobie przetwarzającej dane podczas codziennego wykonywania obowiązków służbowych.
3. Regulamin obowiązuje wszystkich pracowników, doktorantów, studentów oraz inne osoby, które w jakikolwiek sposób przetwarzają dane osobowe w związku z działalnością Uniwersytetu.
4. Regulamin obejmuje dane osobowe przetwarzane w formie papierowej i elektronicznej.
5. Ilekroć w niniejszym regulaminie jest mowa o:
   1) Administratorze – rozumie się przez to Administratora danych, którym jest Uniwersytet Rzeszowski, reprezentowany przez Rektora.
   2) Inspektorze Ochrony Danych (IOD) – rozumie się przez to osobę wyznaczoną przez Administratora do nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych.
   3) Administratorze systemów informatycznych (lub „ASI") – rozumie się przez to osobę fizyczną wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane ustawą i Rozporządzeniem.
   4) Lokalnym administratorze systemów informatycznych (lub „LASI") – rozumie się przez to osobę fizyczną, powołaną zarządzeniem przez Rektora, odpowiedzialną za ścisłą współpracę z Inspektorem Ochrony Danych (IOD) oraz Administratorem Sieci Informatycznych (ASI) lokalnie tj. w skali właściwej jednostki.
   5) Danych osobowych (lub „dane") – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
   6) Użytkowniku danych – rozumie się przez to osobę, która przetwarza dane osobowe w imieniu i na polecenie Administratora (pracownik, student, współpracownik itp.).
   7) Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;

8) Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowania, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;

9) Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym upoważnieniu;
10) Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

6. W przypadku wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IOD z wnioskiem o rozstrzygnięcie wątpliwości.
7. Przed udzieleniem przez IOD odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych, których wątpliwość dotyczy, należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

§ 2

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych, jak również wszelkie informacje, z którymi miał styczność w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej.
5. Wszelkie dokumenty zwierające dane osobowe przechowywane są, w miarę możliwości, w szafach lub pomieszczeniach zamykanych na klucz.
6. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
7. Osoba, która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tę okoliczność Inspektorowi Ochrony Danych oraz Administratorowi.

8. Inspektor Ochrony Danych lub Administrator w zakresie swoich kompetencji podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.
9. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
10. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
11. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
12. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
13. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

§ 3
ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających dane osobowe lub informacje poufne.
6. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji zawierających dane osobowe lub informacji poufnych u Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
7. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności Osoby upoważnionej.
8. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić Inspektora Ochrony Danych lub Administratora.

§ 4
POLITYKA HASEŁ

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora systemu informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemów informatycznych Administratora jest obowiązany do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ich ujawnienia;
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora systemu informatycznego;
   4) poinformowania administratora systemu informatycznego oraz Inspektora ochrony danych o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
   6) stosowania haseł nieposiadających w swojej strukturze części loginu;
   7) stosowania haseł niebędących zbliżonymi do poprzednich (np. Uniwersytet25! - Uniwersytet26!);
5. W przypadku długotrwałej nieobecności pracownika, braku możliwości skontaktowania się z pracownikiem lub odmową przekazania hasła do sprzętu służbowego, upoważniony pracownik Uczelnianego Centrum Informatyzacji na wniosek bezpośredniego przełożonego pracownika, dokonuje ściągnięcia hasła z komputera i założenia nowego.
6. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
7. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   4) udostępnianie haseł innym użytkownikom;
   5) przeprowadzanie prób łamania haseł;
   6) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);

§ 5
ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym, tj. brak wykonywania jakichkolwiek czynności przez okres 15 minut w systemie informatycznym, powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem przed odejściem od stanowiska.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć ich utraty.
5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:
   1) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
   2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

§ 6
KORZYSTANIE Z SYSTEMU SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ ORAZ SIECI PUBLICZEJ

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki poczty elektronicznej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna prowadzona przez pracownika, a niezwiązana z działalnością Administratora, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej.

6. Użytkownicy dokonujący wysyłki korespondencji masowej poza Uniwersytet Rzeszowski, zobowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW). sytuacji stanowiących naruszenie przyjętych zasad bezpieczeństwa.
7. Zabronione jest:
   1) wysyłanie materiałów służbowych zawierających dane osobowe lub dane poufne na konta prywatne (np. celem pracy nad dokumentami w domu);
   2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;
   3) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   4) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe;
   5) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
   6) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
   7) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem – w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi systemu informatycznego;
   8) posługiwanie się służbowym adresem skrzynki pocztowej w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
   9) wykorzystywanie służbowej poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.
8. Dostęp użytkowników do sieci publicznej (Internet) jest ograniczony do niezbędnego minimum na danym stanowisku pracy.
9. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

§ 7
NOŚNIKI ELEKTRONICZNE, KORZYSTANIE Z SIECI VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH ORAZ OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

1. Każdy użytkownik wymiennych nośników elektronicznych, użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do zasad określonych w ust. 2.
2. Podczas korzystania z nośników elektronicznych, zdalnych dostępów do sieci służbowej VPN oraz elektronicznych kart dostępu poza obszarem przetwarzania danych:
   1) zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
   2) komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować;
   3) użytkownik wykonując czynności zawodowe lub umowne w domu dba o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
   4) zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
   5) zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora;

6) w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub Administratora systemu informatycznego. Bezpośredni przełożony lub Administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Inspektora Ochrony Danych, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez administratora danych;
7) problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi systemu informatycznego oraz Lokalnemu Administratorowi Systemów Informatycznych.

3. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
4. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
5. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
6. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik skontaktuje się z Administratorem systemu informatycznego oraz Lokalnym Administratorem Systemów Informatycznych.

§ 8
SPRZĘT KOMPUTEROWY, NOŚNIKI DANYCH

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,
   3) tablety,
   4) smartphony,
   5) drukarki,
   6) modemy,
   7) monitory,
   8) routery,
   9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator Systemów Informatycznych oraz Lokalny Administrator Systemów Informatycznych udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, Administrator systemu informatycznego informuje o powyższym Inspektora Ochrony Danych.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik przed dokonaniem zmiany konfiguracji przekazanego sprzętu komputerowego oraz przed instalacją lub usunięciem oprogramowania (w tym też prywatnego oprogramowania) musi powiadomić dział IT o chęci dokonania takiego działania.

§ 9
POSTANOWIENIA KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, w efekcie którego nastąpiło udostępnienie informacji zawierających dane osobowe lub informacji poufnych osobie nieupoważnionej, potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych zgodnie z obowiązującym Regulaminem pracy UR lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

R e k t o r

Uniwersytetu Rzeszowskiego

prof. dr hab. Adam Reich

HR EXCELLENCE IN RESEARCH