Wyższa Szkoła Ekonomiczna
w Białymstoku
ul. Zwycięstwa 14/3, 15-703 Białystok
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Zarządzenie nr 5/2023
Rektora Wyższej Szkoły Ekonomicznej w Białymstoku
z dnia 31 marca 2023 r.

w sprawie wprowadzenia
Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w Wyższej Szkole Ekonomicznej w Białymstoku oraz
Procedury realizacji praw wynikających z ogólnego rozporządzenia o ochronie danych RODO w Wyższej Szkole Ekonomicznej w Białymstoku

Na podstawie art. 23 ust. 1 i 2 pkt 2 ustawy z 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2022 r., poz. 574) w związku z § 8 ust. 1 i 2 pkt 3 Statutu Wyższej Szkoły Ekonomicznej w Białymstoku oraz art. 24 ust. 1 i 2 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. z 2016 r. Nr 119, str. 1 z późn. zm.) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, (tj. Dz. U. z 2019 r., poz. 11781), zarządzam, co następuje:

§ 1

1. Wprowadza się w zakresie ochrony danych następujące dokumenty:
   1) **Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w Wyższej Szkole Ekonomicznej w Białymstoku**
   2) **Procedurę realizacji praw wynikających z ogólnego rozporządzenia o ochronie danych RODO w Wyższej Szkole Ekonomicznej w Białymstoku**
2. Wskazane w ust. 1 dokumenty są zgodne z Polityką ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku.

§ 2

Dokumenty, o którym mowa w § 1 mają zastosowanie na wszystkich stanowiskach pracy i innych miejscach, w których przetwarzane są dane osobowe w Wyższej Szkole Ekonomicznej w Białymstoku **i jej jednostkach organizacyjnych.**

§ 3

Zobowiązuje się kierowników jednostek organizacyjnych do zapoznania pracowników zatrudnionych w danej jednostce przy przetwarzaniu danych osobowych oraz pracujących w systemach informatycznych z treścią dokumentów, o których mowa § 1 .

§ 4

Zarządzenie wchodzi w życie z dniem 01.04.2023 r.

REKTOR
prof. WSE dr Aleksander Prokopiuk
Rektor

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w Wyższej Szkole Ekonomicznej w Białymstoku

Spis treści:

Rozdział 1
Cel wydania instrukcji i jej zakres przedmiotowy

§ 1

1. Instrukcja określa zasady postępowania wszystkich osób upoważnionych do przetwarzania danych osobowych zatrudnionych przy przetwarzaniu danych osobowych przez Administratora Danych Osobowych, dalej „ADO", tj. Wyższą Szkołę Ekonomiczną w Białymstoku, zwaną dalej „WSE" w przypadku naruszenia ich bezpieczeństwa.
2. Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:
   1) nieautoryzowany dostęp do danych;
   2) nieautoryzowane modyfikacje lub zniszczenie danych;
   3) udostępnienie danych nieautoryzowanym podmiotom;
   4) nielegalne ujawnienie danych.
3. Postanowienia instrukcji mają zastosowanie do wewnętrznych komórek organizacyjnych i dydaktycznych WSE, a także do samodzielnych stanowisk w WSE.
4. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszej instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Rozdział 2
Rodzaje incydentów świadczących o możliwości naruszenia bezpieczeństwa danych

§ 2

1. Naruszenie ochrony danych osobowych" oznacza 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.

2. Wyróżnia się następujące rodzaje naruszeń:
   1) „naruszenie poufności", które polega na ujawnieniu lub udostępnieniu danych osobie nieuprawnionej;
   2) „naruszenie integralności", które sprowadza się do zmiany treści danych osobowych, czyli ich modyfikowania, w sposób nieautoryzowany;
   3) "naruszenie dostępności", które wiąże się z trwałą utratą dostępu do danych lub ich zniszczeniem.
3. O możliwości wystąpienia naruszenia bezpieczeństwa danych osobowych mogą świadczyć:
   1) nadmierne w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów danych;
   2) niestabilna praca systemu teleinformatycznego;
   3) korzystanie z zasobów danych poza miejscem przetwarzania/godzinami pracy (bez zgody przełożonego);
   4) nowe „podejrzane" (nieznane) konta użytkowników w systemie;
   5) wysoka aktywność kont, które długo pozostawały niewykorzystane;
   6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
   7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
   8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie danych osobowych (uszkodzone zamki, okna, drzwi, itp.).
4. Prawdopodobne incydenty naruszenia bezpieczeństwa danych zostały określone w wykazie naruszeń, stanowiącym załącznik 1 do instrukcji.

Rozdział 3
Postępowanie w przypadku podejrzenia naruszenia bezpieczeństwa danych

§ 3

1. Każdy pracownik/osoba upoważniona, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu – wzór zgłoszenia stanowi załącznik nr 2. Przełożony zgłasza fakt Inspektorowi Ochrony Danych, zwanemu dalej „IOD".
2. Sytuacje, które wymagają zgłoszenia to:
   1) fizyczna obecność w budynkach WSE osób zachowujących się podejrzanie;
   2) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   3) niszczenie dokumentów bez użycia niszczarki;
   4) otwarte drzwi do pomieszczeń, szaf, w których przechowywane są dane osobowe w formie papierowej oraz na nośnikach elektronicznych;
   5) niewylogowanie się przed opuszczeniem stanowiska pracy;
   6) pozostawienie danych w drukarce, na ksero;
   7) niezamknięcie pomieszczenia z komputerem;
   8) niewykonanie w określonym terminie kopii zapasowych;
   9) prace z danymi osobowymi w celach prywatnych;
   10) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;

11) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz placówki bez upoważnienia;
12) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
13) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
14) telefoniczne próby wyłudzenia danych osobowych;
15) kradzież komputerów lub twardych dysków z danymi osobowymi;
16) utrata kontroli nad kopią danych osobowych;
17) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
18) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
19) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
20) pozostawianie niezabezpieczonych haseł w pobliżu komputera.

§ 4

Każdy pracownik/osoba upoważniona, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

§ 5

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Sieci Informatycznej, zwanym dalej „ASI" lub innej osoby upoważnionej przez ADO.

§ 6

ADO lub upoważniona przez niego osoba dokonuje wstępnej identyfikacji zaistniałego zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:

1) zdarzenie niemające cech naruszenia bezpieczeństwa, np. zaplanowana przerwa techniczna;
2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej;
3) awaria techniczna czasowo blokująca dostępność informacji;
4) zdarzenie niskiej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych, a szczególnie jej integralności i poufności, nie generujące kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu przetwarzania;
5) zdarzenie średniej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych skutkujące pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi oraz możliwością konsekwencji prawnych i/lub utraty wizerunku;
6) zdarzenie wysokiej kategorii – związane z naruszeniem bezpieczeństwa ochrony danych, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów funkcjonowania placówki.

§ 7

Przy analizie naruszeń, o których mowa w § 4 należy wziąć pod uwagę:

1) charakter zdarzenia i jego znaczenie związane z naruszeniem bezpieczeństwa ochrony danych osobowych;
2) miejsce wystąpienia zdarzenia - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja pomieszczenia, serwer, stacja robocza itp.);
3) zakres zasobów dotkniętych naruszeniem;
4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania ze zdarzeniem związanym z naruszeniem bezpieczeństwa ochrony danych;
5) możliwości rozszerzania się naruszenia i sposoby jego ograniczania;
6) rodzaj ujawnionej informacji (jeśli ma zastosowanie - np. dane osobowe);
7) szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa ochrony danych;
8) skutki organizacyjne i prawne (wstępny szacunek).

§ 8

W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie naruszenia do wysokiej kategorii, ADO powiadamia niezwłocznie Prezesa Urzędu Ochrony Danych Osobowych (PUODO), a następnie przeprowadza dochodzenie wyjaśniające.

§ 9

W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje ADO.

§ 10

ADO o każdym incydencie naruszenia bezpieczeństwa danych osobowych informuje IOD oraz sporządza raport, zgodnie ze wzorem raportu, który stanowi załącznik nr 3 do instrukcji.

§ 11

1. IOD podejmuje następujące kroki:
   1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy;
   2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
   3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).
2. IOD zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - załącznik nr 4 - Rejestr incydentów i działań korygujących i zapobiegawczych.

Rozdział 4
Ograniczanie skutków naruszeń

§ 12

1. Dokumentacja naruszenia podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów, które mają zastosowanie przy postępowaniu z naruszeniem, w tym: rejestry

urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe, bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.

2. IOD przeprowadza bieżące działania zmierzające do ograniczenia skutków naruszenia i zidentyfikowania jego źródła. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.
3. W przypadku, gdy działania opisane w ust. 2 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych WSE, IOD przedstawia decyzję do akceptacji ADO.

Rozdział 5
Odtwarzanie systemu

§ 13

1. Osoba upoważniona przez ADO przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła naruszenia.
2. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego ASI ma uzasadnioną pewność, że nie zawiera źródła naruszenia.
3. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
4. ADO, po zasięgnięciu opinii IOD, może podjąć decyzję o podjęciu przetwarzania danych mimo braku pewności usunięcia źródła naruszenia, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

Rozdział 6
Zgłaszanie naruszenia ochrony danych do UODO

§ 14

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w ust. 1, musi zawierać co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) zawierać imię i nazwisko oraz zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisywać środki zastosowane lub proponowane przez ADO w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

5. Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie **www.uodo.gov.pl** na 4 sposoby:
   1) elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie www.biznes.gov.pl;
   2) elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP
   3) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie www.biznes.gov.pl;
   4) tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Rozdział 7
Zawiadamianie osób o naruszeniu ochrony ich danych osobowych

§ 15

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.
3. Nie dokonuje się zawiadomienia osób w następujących przypadkach, gdy:

1) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załączniki:

1) Tabela naruszeń bezpieczeństwa danych osobowych – załącznik 1.

2) Wzór zgłoszenia incydentu przez pracownika – załącznik 2.

3) Raport z naruszenia bezpieczeństwa danych – załącznik 3a i 3b.

....

Inspektor Ochrony Danych Osobowych Administrator Danych Osobowych

Załącznik nr 1.

Tabela naruszeń bezpieczeństwa danych osobowych

Symbol	Formy naruszeń	Sposoby postępowania
P	**Formy naruszenia bezpieczeństwa danych przez pracownika**	
P/1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IODO.
P/2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej, stosowanych zabezpieczeniach	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić IODO.
P/3	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
P/4	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez inne osoby niż osoba, która została upoważniona.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji o naruszaniu porządku pracy. Sporządzić raport.
P/5	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić IODO. W trybie natychmiastowym dokonać zmiany hasła. Sporządzić raport.
P/6	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami, w szczególności w pracy zdalnej.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić IODO. Sporządzić raport.

P/7	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
P/8	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Zainstalować zmodyfikowane programy pliku źródłowego. Sporządzić raport.
P/9	Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o stosowaniu polityki bezpieczeństwa. Wykonać kontrolę programem antywirusowym. Sporządzić raport.
P/10	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. Sporządzić raport.
P/11	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
P/12	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie, z pominięciem niszczenia niszczarką.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
P/13	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią, w tym umożliwienie uzyskania kopii z ksero.	Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
P/14	Dopuszczanie, aby osoby postronne odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. W przypadku ujawnienia ważnych danych sporządzić raport.
P/15	Sporządzanie kopii danych na nośnikach danych bez uzasadnienia oraz braku obowiązku takiego kopiowania.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić IODO. Sporządzić raport
P/16	Opuszczanie i pozostawianie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych. Sporządzić

	używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych	raport.
P/17	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i IODO. Sporządzić raport.
P/18	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i przewodów kablowych lub dokonywały jakichkolwiek zmian.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i IOD. Sporządzić raport.
P/19	Wynoszenie dokumentacji papierowej lub dokumentacji w formie elektronicznej poza teren WSE bez zgody rektora.	Powiadomić przełożonych i IOD. Sporządzić raport.
P/20	Logowanie się do systemów w okresie choroby w miejscu przebywania w czasie trwania L4 bez upoważnienia rektora lub przełożonego.	Powiadomić przełożonych i IOD. Sporządzić raport.
P/21	Nieterminowe dokonywanie zmiany haseł I longinów.	Powiadomić przełożonych i IOD. Sporządzić raport.
P/22	Nieaktualizowanie programów użytkowych.	Powiadomić przełożonych ni IOD. Sporządzić raport.
P/23	Nieaktualizowanie programów antywirusowych.	Powiadomić przełożonych i IOD. Sporządzić raport.
P/24	Otwieranie załączników niewiadomego nadawcy.	Powiadomić przełożonych i IOD. Sporządzić raport.
N	**Zjawiska świadczące o możliwości naruszenia bezpieczeństwa danych**	
N/1		Powiadomić niezwłocznie IOD oraz służby informatyczne. Nie używać sprzętu ani

	Ślady manipulacji przy układach sieci komputerowej lub komputerach	oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
N/2	Obecność nowych kabli o nieznanym przeznaczeniu.	Powiadomić IOD. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
N/3	Zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
N/4	Nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić IOD. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
N/5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji Oprogramowania.	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji Oprogramowania Powiadomić IOD. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
N/6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie IOD. Sporządzić raport.
Z	**Ingerencja zewnętrzna**	
Z/1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej	Powiadomić IOD. Sporządzić raport.
Z/2	Zablokowanie dostępu	Powiadomić IOD. Sporządzić raport.
Z/3	Wirusy, konie trojańskie	Powiadomić IOD. Sporządzić raport.
Z/4	Telefoniczne próby wyłudzenia haseł dostępu lub danych osobowych	Powiadomić IOD. Sporządzić raport.

Załącznik nr 2

Białystok, dn. .....

Zgłoszenie incydentu naruszenia bezpieczeństwa danych przez pracownika

1. Dane zgłaszającego:

Imię i nazwisko	
Stanowisko	
Jednostka organizacyjna/dydaktyczna/ samodzielne stanowisko	
Telefon kontaktowy	
E-mail	

2. Wskazanie, w którym miejscu wystąpiło naruszenie:

Sieci	
System teleinformatyczny	
Dokumentacja papierowa, zbór danych	

3. Data i godzina stwierdzenia naruszenia: .....

4. Charakterystyka naruszenia:

Opisać szczegółowo na czym polegało naruszenie ochrony danych osobowych, w tym: - opis zdarzenia ze wskazaniem np. faktu zniszczenia, utraty, nieuprawnionej modyfikacji danych, ujawnienia danych, nieuprawnionego dostępu do danych wraz z okolicznościami tego zdarzenia: ....
Na czym polegało naruszenie? □ Zgubienie, kradzież nośnika/urządzenia □ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji □ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed

zwróceniem jej do nadawcy
□ Nieuprawnione uzyskanie dostępu do informacji/systemu
□ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
□ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych
□ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy
□ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
□ Niezamierzona publikacja
□ Dane osobowe wysłane do niewłaściwego odbiorcy
□ Ujawnienie danych niewłaściwej osoby
□ Ustne ujawnienie danych osobowych
□ Inne
.....
.....
.....

Przyczyna naruszenia:

□ Wewnętrzne działanie niezamierzone
□ Wewnętrzne działanie zamierzone
□ Zewnętrzne działanie niezamierzone
□ Zewnętrzne działanie zamierzone

Opisać możliwe konsekwencje naruszenia ochrony danych osobowych:

Naruszenie ma wpływ na:
□ poufność (nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych)
□ integralność (wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania)
□ dostępność (brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez do tego uprawnioną

Kategorie danych osobowych, których dotyczy naruszenie:

□ nazwiska i imiona
□ nazwa użytkownika i/lub hasło
□ imiona rodziców
□ dane dot. zarobków
□ data urodzenia
□ nazwisko rodowe matki
□ nr rachunku bankowego
□ seria i numer dowodu osobistego
□ adres zamieszkaniu lub pobytu
□ numer telefonu
□ numer ewidencyjny PESEL
□ wizerunek
□ adres e-mail
□ inne.....

- przybliżona liczba osób, których mogło dotyczyć naruszenie.....
- przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie.....

Dane szczególnej kategorii przetwarzania:

□ dane o pochodzeniu rasowym lub etnicznym
□ dane o poglądach politycznych
□ dane o przekonaniach religijnych lub światopoglądowych
□ dane o przynależności do związków zawodowych
□ dane dotyczące seksualności lub orientacji seksualnej
□ dane dotyczące zdrowia
□ dane genetyczne
□ dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

Możliwe konsekwencje (opisać konsekwencje dla osoby, której dane dotyczą):

□ utrata kontroli nad własnymi danymi osobowymi
□ ograniczenie możliwości realizowania praw z art. 15-22 RODO
□ ograniczenie możliwości realizowania praw
□ dyskryminacja
□ kradzież lub sfałszowanie tożsamości
□ strata finansowa
□ naruszenie dobrego imienia
□ utrata poufności danych osobowych chronionych tajemnicą zawodową
□ inne:
.....

Czy naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:

□ NIE
□ TAK (art. 33 ust.1 RODO)

niskie/ średnie/ wysokie

.....
podpis osoby zgłaszającej

Zarejestrowano w rejestrze naruszeń ochrony danych osobowych w dniu .....

godz. ..... poz. rejestru .....

Załącznik nr 3a

Raport z naruszenia ochrony danych

1. Data: ..... godzina: ..... nr zgłoszenia: .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub wysłuchane w związku z naruszeniem: .....

.....

(imię, nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia: .....

.....

(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.)

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....

.....

5. Wstępna ocena przyczyn wystąpienia naruszenia: .....

.....

.....

6. Postępowanie wyjaśniające: .....

.....

.....

.....

7. Działania podjęte w związku z wystąpieniem naruszenia - środki zaradcze i naprawcze:

1) Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych:

.....

.....

2) Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia: .....

.....

3) Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą:

.....

.....

....

data i podpis Pracownika data i podpis Inspektora Ochrony Danych

Załącznik nr 3b

Raport końcowy sporządzany przez IODO po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych

1. Sporządzający raport:

   Imię i nazwisko: .....

   Stanowisko (funkcja): .....

   Dział, pokój, nr telefonu .....

2. Kod formy naruszenia ochrony danych ..... (wg tabeli, zał. nr 1 do instrukcji)
3. Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.): .....

   .....

4. Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych): .....

   .....

5. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

   .....

   .....

   .....

6. Informacje o danych, które zostały lub mogły zostać ujawnione: .....

   .....

7. Zabezpieczone materiały lub inne dowody związane z wydarzeniem: .....

   .....

   .....

8. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania):

   .....

   .....

   .....

   .....

   .....

9. Wnioski: .....

   .....

   .....

.....
data i podpis Inspektora Ochrony Danych

.....
data i podpis Administratora Danych Osobowych

Procedura realizacji praw wynikających z ogólnego rozporządzenia o ochronie danych RODO

w Wyższej Szkole Ekonomicznej w Białymstoku

1. Wniosek, stanowiący załącznik nr 1 do niniejszej procedury, dotyczący realizacji praw można pobrać ze strony internetowej www.wse.edu.pl lub otrzymać jego wersję papierową w siedzibie Administratora, 15-703 Białystok, ul. Zwycięstwa 14/3, prawidłowo wypełnić, podpisać a następnie przesłać go bezpośrednio Administratorowi na adres: wse@wse.edu.pl, lub Inspektorowi Ochrony Danych na adres: iod@wse.edu.pl, albo za pomocą poczty tradycyjnej na adres Administratora.
2. Wniosek powinien być wypełniony czytelnie DRUKOWANYMI LITERAMI.
3. We wniosku należy podać wszystkie wymagane informacje.
4. Administrator może wymagać podania dodatkowych informacji pozwalających na weryfikację uprawnienia do złożenia ww. wniosku, w tym potwierdzenia tożsamości osoby składającej wniosek. Zakres każdego z praw oraz sytuacje, w których może skorzystać osoba składająca wniosek, wynikają z przepisów prawa. Z którego z wymienionych uprawnień może skorzystać osoba składająca wniosek, zależeć będzie m.in. od podstawy prawnej wykorzystywania danych oraz celu ich przetwarzania.
5. Administrator ma prawo odmówić przekazania danych lub zmienić formę odbioru w sytuacji, kiedy nie jest w stanie prawidłowo zidentyfikować osoby wnioskującej.
6. W sytuacji, kiedy żądania osoby zostaną uznane za nadmierne lub nieuzasadnione, Administrator może pobrać opłatę stosowną do kosztów udzielenia odpowiedzi, informując wcześniej osobę wnioskującą o wysokości opłaty.
7. Odpowiedź na zgłoszenie zostanie udzielona niezwłocznie, nie później niż w ciągu miesiąca od jego otrzymania. W razie konieczności przedłużenia tego terminu, Administrator poinformuje osobę składającą wniosek o przyczynach takiego przedłużenia.
8. Odpowiedź będzie udzielana zgodnie z wybraną opcją określoną we wniosku.
9. Szczegółowe informacje na temat udzielania odpowiedzi można uzyskać poprzez kontakt z naszym Inspektorem Ochrony Danych.

JAKIE PRAWA, WYNIKAJĄCE Z RODO, MAJĄ OSOBY, KTÓRYCH DANE PRZETWARZANE SĄ W WYŻSZEJ SZKOLE EKONOMICZNEJ W BIAŁYMSTOKU

1. Prawo dostępu przysługujące osobie, której dane dotyczą oraz uzyskania informacji

Administrator na żądanie osoby, której dane dotyczą, udziela jej informacji, czy przetwarza jej dane. Gdy ma to miejsce Administrator jest zobowiązany udzielić tej osobie dostępu do tych danych oraz następujących informacji:

a. cele przetwarzania,

b. kategorie danych osobowych,

c. odbiorcy lub kategorie odbiorców danych, w szczególności odbiorcy w państwach trzecich lub organizacjach międzynarodowych,

d. planowany okres przechowywania danych (lub kryteria ustalania tego okresu),

e. informacja o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, które go dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,

f. informacja o prawie wniesienia skargi do organu nadzorczego,

g. informacja o źródle danych jeśli nie zostały one zebrane bezpośrednio od pomiotu danych,

h. informacja o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu oraz istotne

informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (ma zastosowanie w przypadku, gdy zautomatyzowane podejmowanie decyzji wywołuje wobec j osoby skutki prawne lub w podobny sposób istotnie na nią wpływa lub gdy opiera się na szczególnych kategoriach danych osobowych), i. w przypadku gdy dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej, należy podać informacje o stosowanych zabezpieczeniach, Administrator udziela osobie, której dane dotyczą informacji dotyczących przetwarzania jej danych osobowych zarówno wtedy, gdy dane te pozyskuje bezpośrednio od osoby, której dane dotyczą (art.13 Rozporządzenia UE), jak i w sytuacji, gdy dane pozyskuje z innych źródeł (art.14 Rozporządzenia UE).

2. Prawo do sprostowania danych

W przypadku nieprawidłowości lub niekompletności przetwarzanych danych osobowych, osoba, której dane dotyczą, ma prawo żądać ich sprostowania lub uzupełnienia.

3. Prawo do usunięcia danych („prawo do bycia zapomnianym")

Administrator na żądanie osoby, której dane dotyczą usuwa jej dane, jeśli zachodzi jedna z poniższych okoliczności:
a. dane osobowe nie są już niezbędne do celów, w których zostały one zebrane,
b. osoba, której dane dotyczą wycofała zgodę, na której przetwarzanie było oparte i nie ma innej podstawy prawnej przetwarzania,
c. podmiot danych wnosi sprzeciw wobec przetwarzania,
d. dane osobowe były przetwarzane niezgodnie z prawem,
e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego (prawo Unii lub krajowe),
f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, oferowanych dziecku, które nie ukończyło 16 lat. Jeśli dane osobowe zostały upublicznione, Administrator zobowiązany jest podjąć rozsądne działania (uwzględniające dostępną technologię i koszty realizacji), aby poinformować innych administratorów przetwarzających te dane, o żądaniu podmiotu danych dotyczącym usunięcia tych danych, ich kopii i łączy do nich.
Administrator ma prawo odmówić realizacji tego żądania, jeśli oceni, że przetwarzanie danych jest niezbędne:
a. do korzystania z praw do wolności wypowiedzi i informacji,
b. do wywiązania się z obowiązków prawnych (narzuconych prawem Unii, prawem krajowym lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
c. ze względu na interes publiczny w dziedzinie zdrowia publicznego,
d. do celów archiwalnych w interesie publicznym,
e. do ustalenia, dochodzenia lub obrony roszczeń

4. Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą może żądać ograniczenia przetwarzania jej danych osobowych następujących przypadkach:
a. osoba, której dane dotyczą kwestionuje prawidłowość danych. W takim przypadku Administrator ogranicza przetwarzanie na okres pozwalający mu sprawdzić ich prawidłowość,
b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c. osoba, której dane dotyczą potrzebuje danych do ustalenia, dochodzenia lub obrony roszczeń, a nie są one już potrzebne Administratorowi,

d. rozpatrywany jest sprzeciw wobec przetwarzania danych. Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

5. Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, np. odt, xls, doc, pdf, csv dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:
a. przetwarzanie odbywa się na podstawie zgody,
b. przetwarzanie odbywa się na podstawie umowy,
c. przetwarzanie odbywa się w sposób zautomatyzowany.
Osoba, której dane dotyczą ma prawo żądania, by jego dane osobowe były przesłane przez Administratora bezpośrednio innemu Administratorowi. Rozpatrując żądanie przeniesienia danych należy rozważyć, czy ta operacja nie ma negatywnego wpływu na prawa i wolności innych.

6. Prawo do sprzeciwu

Osoba, której dane dotyczą ma prawo wnieść sprzeciw wobec przetwarzania danych z przyczyn związanych z jej szczególną sytuacją, jeśli przetwarzanie jest niezbędne:
a. do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,
b. do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Administrator zaprzestaje przetwarzania danych, chyba, że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą. W przypadku, gdy dane osobowe przetwarzane są w celu prowadzenie marketingu bezpośredniego, Administrator musi bezwzględnie zaprzestać przetwarzania danych.

7. Prawo do uzyskania kopii danych

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej. Prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych.

Załącznik nr 1

WNIOSEK O REALIZACJĘ PRAW OSÓB FIZYCZNYCH WYNIKAJĄCYCH Z RODO

Wypełnia Administrator Danych Osobowych (dalej: Administrator)

Numer wniosku .....

Data wpłynięcia wniosku ..... Miejscowość: .....

Na podstawie art. 12-22 Rozporządzenia Parlamentu Europejskiego i (Rady (UE) 2016/679 z dn. 27 kwietnia 2016 r. (RODO) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, proszę o realizację następujących praw w związku z przetwarzaniem moich danych osobowych w **Wyższej Szkole Ekonomicznej w Białymstoku**, 15-703 Białystok, ul. Zwycięstwa 14/3, będącej Administratorem Danych Osobowych:

□ dostępu do danych oraz uzyskania informacji (na podstawie art. 15 RODO)
□ do uzyskania kopii danych (na podstawie art. 15 RODO)
□ do sprostowania danych (na podstawie art. 16 RODO)
□ do usunięcia danych („prawo do bycia zapomnianym") (na podstawie art. 17 RODO)
□ do ograniczenia przetwarzania (na podstawie art. 18 RODO)
□ do przenoszenia danych do innego Administratora (na podstawie art. 20 RODO)
□ do sprzeciwu wobec przetwarzania danych (na podstawie art. 21 RODO)

I. Dane osoby wnioskującej niezbędne do identyfikacji tożsamości w zbiorach Administratora:

Imię ..... **Nazwisko** .....

Adres e-mail/numer telefonu .....

II. Dodatkowe informacje umożliwiające identyfikację osoby przez Administratora:

.....

.....

III. Uzasadnienie wniosku:

.....

.....

IV. Wnioskowany sposób odbioru:

□ Osobiście w siedzibie Administratora

□ Listownie na adres: .....

□ Pocztą elektroniczną na podany adres e-mail: .....

.....
czytelny podpis osoby składającej wniosek

Wyjaśnienia

1. Prosimy o czytelne wypełnienie formularza DRUKOWANYMI LITERAMI.
2. Administrator ma prawo odmówić przekazania danych lub zmienić formę odbioru w sytuacji, kiedy nie jest w stanie prawidłowo zidentyfikować osoby wnioskującej.
3. Na potrzeby rozpatrzenia wniosku i jego dalszej realizacji może być wymagane podanie dodatkowych danych Pani/Pana identyfikujących.
4. W sytuacji, kiedy żądania osoby zostaną uznane za nadmierne lub nieuzasadnione, Administrator może pobrać opłatę stosowną do kosztów udzielenia odpowiedzi, informując wcześniej osobę wnioskującą o wysokości opłaty. (np. udostępniane kolejnej kopii danych)
5. Szczegółowe informacje na temat udzielania odpowiedzi można uzyskać poprzez kontakt z naszym Inspektorem Ochrony Danych.
6. Odpowiedź na zgłoszenie zostanie udzielona niezwłocznie, nie później niż wciągu 30 dni od jego otrzymania. W razie konieczności przedłużenia tego terminu o kolejny miesiąc, Administrator poinformuje osobę składającą wniosek o przyczynach takiego przedłużenia.
7. Odpowiedź będzie udzielana zgodnie wybraną opcją określoną we wniosku.

Informacja Administratora Danych Osobowych
dla osób składających wniosek o realizację praw wynikających z RODO

Na podstawie art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. z 2016 r. Nr 119, str. 1), zwanym dalej „RODO" informujemy, że:

1. Administratorem Państwa danych osobowych jest Wyższa Szkoła Ekonomiczna w Białymstoku z siedzibą w Białymstoku, 15-703 Białystok, ul. Zwycięstwa 14/3, reprezentowana przez Rektora Uczelni.
2. Na podstawie obowiązujących przepisów, wyznaczyliśmy Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: iod@wse.edu.pl
3. Pani/Pana dane osobowe przetwarzane będą:
   a) w celu realizacji złożonego wniosku - zgodnie z art. 6 ust. 1 lit. c RODO w związku z art. 15, art., 16, art. 17, art. 18, art. 20, art. 21, art. 22 RODO;
   b) w celu wypełnienia obowiązków prawnych ciążących na administratorze w szczególności związanych z archiwizacją dokumentacji - zgodnie z art. 6. ust. 1 lit. c RODO w związku z Ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.
4. Odbiorcami Pani/Pana danych osobowych mogą być operatorzy pocztowi, dostawcy systemów informatycznych i usług IT, instytucje upoważnione z mocy przepisów prawa oraz instytucje na mocy wiążących umów.
5. Okres przetwarzania Pani/Pana danych osobowych jest uzależniony od celu, w jakim dane są przetwarzane. Okres przechowywania wynikał będzie z przepisów prawa dotyczących archiwizacji, instrukcji kancelaryjnej na podstawie Jednolitego Rzeczowego Wykazu Akt obowiązującego w WSE w Białymstoku.
6. Ma Pani/Pan prawo żądać od Administratora dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania danych.
7. Ma Pani/Pana prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO.
8. Podanie danych osobowych jest warunkiem realizacji wniosku. Odmowa podania danych osobowych uniemożliwia realizację wniosku.

.....
czytelny podpis osoby składającej wniosek