Załącznik do Zarządzenia nr 113
Rektora Uniwersytetu Przyrodniczego w Lublinie
z dnia 8 października 2020 r.
w sprawie wprowadzenia Polityki bezpieczeństwa
przetwarzania danych osobowych
Uniwersytetu Przyrodniczego w Lublinie

Polityka bezpieczeństwa przetwarzania danych osobowych

Uniwersytetu Przyrodniczego w Lublinie

UNIWERSYTET PRZYRODNICZY
w Lublinie

Polityka bezpieczeństwa przetwarzania danych osobowych Uniwersytetu Przyrodniczego w Lublinie

Polityka bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Przyrodniczym w Lublinie została opracowana w celu zapewnienia prawidłowości wdrożenia i zabezpieczenia procesu przetwarzania danych osobowych w Uczelni. Dane osobowe przetwarza się wyłącznie dla określonych celów związanych z działalnością Uniwersytetu na podstawie art. 11 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce.

§ 1
Postanowienie ogólne

1. Celem wdrożenia niniejszej polityki jest zapewnienie należytej ochrony danych osobowych będących w zasobach administratora danych, w szczególności adekwatnej do zagrożeń i kategorii danych osobowych objętych ochroną oraz uzyskanie optymalnego dla działalności Uniwersytetu Przyrodniczego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.
2. Uniwersytet Przyrodniczy w Lublinie przetwarza dane osobowe oraz wytwarza i administruje dokumentacją zawierającą takie dane, dlatego podlega **Rozporządzeniu 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)** oraz ustawie o ochronie danych osobowych. Dane osobowe przetwarzane w Uniwersytecie Przyrodniczym w Lublinie dotyczą studentów, doktorantów, pracowników naukowych oraz pracowników administracji. Nieuprawnione ujawnienie danych osobowych może narazić na szkodę prawnie chroniony interes osób, których te dane dotyczą.
3. Polityka ochrony danych Uniwersytetu Przyrodniczego w Lublinie określa sposób prowadzenia oraz zakres dokumentacji odnoszącej się do sposobu przetwarzania danych osobowych, a także określa środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych - odpowiednie do zagrożeń oraz kategorii danych objętych ochroną.
4. Zakres przedmiotowy stosowania niniejszej polityki obejmuje wszystkie zbiory danych osobowych przetwarzane przez administratora danych - odnosi się swoją treścią do informacji:
   1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
   2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

5. Zakres podmiotowy stosowania niniejszej polityki obejmuje wszystkich pracowników oraz osoby, przy pomocy, których administrator danych wykonuje swoje czynności, które posiadają dostęp do danych osobowych.

§ 2

Podstawy prawne

1. Akty prawne, które normują działanie Uniwersytetu Przyrodniczego w Lublinie
   a. Konstytucja Rzeczypospolitej Polskiej;
   b. Ustawa z dnia 30 sierpnia 2018 r. o szkolnictwie wyższym;
   c. Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 28 września 2018 r. w sprawie studiów.
   d. Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2016 r. w sprawie dokumentacji przebiegu studiów.
   e. Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 10 lutego 2017 r. w sprawie kształcenia na studiach doktoranckich w uczelniach i jednostkach naukowych.
2. Akty prawne dotyczące przetwarzania/bezpieczeństwa informacji:
   a) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
   b) Rozporządzenie 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)
   c) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
   d) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych;
   e) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji;
   f) Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego;
   g) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
   h) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany

informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

§ 3
Definicje

Użyte w niniejszej dokumentacji przetwarzania danych osobowych definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą dokumentacją oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych.

Definicje i pojęcia:

1. Polityka oznacza niniejszą Politykę ochrony danych osobowych.
2. RODO oznacza rozporządzenie 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.Urz. UE L 119, s. 1).
3. Administrator Danych Osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Uniwersytet Przyrodniczy, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego dyspozycji.
4. Dane osobowe - oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
5. Zbiór 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. Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

7. Przetwarzanie oznacza 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.
8. Ograniczenie przetwarzania oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
9. Podmiot przetwarzający oznacza organizację lub osobę, której Uniwersytet Przyrodniczy w Lublinie powierzył przetwarzanie danych osobowych.
10. Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
11. Organ nadzorczy – Minister Nauki i Szkolnictwa Wyższego.
12. IODO oznacza Inspektora Ochrony Danych Osobowych.
13. RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
14. Upoważnienie - nadawane przez Administratora Danych Osobowych wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu.
15. Ustawa - rozumie się przez to ustawę z dnia z dnia 10 maja 2018 r. o ochronie danych osobowych.
16. Użytkownik systemu - rozumie się przez to osobę upoważnioną, która otrzymała dostęp do sieci umożliwiający korzystanie z sieci Internet oraz login i hasło do systemu.
17. Login - identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
18. Hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

§ 4
Zasady ochrony danych

Uniwersytet Przyrodniczy w Lublinie przetwarza dane osobowe z poszanowaniem następujących dziesięciu zasad:

1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ("ograniczenie celu");
3) rzetelnie i uczciwie (rzetelność);

4) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
5) w konkretnych celach i nie "na zapas" (minimalizacja);
6) nie więcej niż potrzeba (adekwatność);
7) z dbałością o prawidłowość danych (prawidłowość);
8) nie dłużej niż potrzeba (czasowość);
9) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo);
10) Administrator jest odpowiedzialny za przestrzeganie obowiązujących przepisów prawa i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

§ 5

Administrator Danych Osobowych

1. Administrator Danych Osobowych dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była legalność, bezpieczeństwo, prawa jednostki i rozliczalność danych.
2. Administrator Danych Osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed: ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną.
3. Administrator Danych Osobowych deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych.
4. Administrator Danych Osobowych w szczególności zapewnia:
   a) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
   b) system i sprzęt informatyczny umożliwiający niezawodne i bezpieczne przetwarzanie danych;
   c) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadające upoważnienie do przetwarzania danych osobowych;
   d) zapoznanie z przepisami o ochronie danych osobowych każdej osoby upoważnionej do przetwarzania danych osobowych;
   e) prowadzenie ewidencji osób upoważnionych;
   f) należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji zgodnie z RODO.

5. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.
6. Administrator Danych Osobowych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.
7. Administrator Danych Osobowych na bieżąco dostosowuje systemy informatyczne służące do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w obowiązujących przepisach prawa.

§ 6

Inspektor ochrony danych osobowych

1. Inspektor Ochrony Danych Osobowych jest wyznaczany przez Administratora Danych Osobowych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.
2. Do zadań IODO należy:
   a) informowanie administratora danych osobowych , podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów i doradzanie im w tej sprawie;
   b) monitorowanie wdrażania i zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
   c) informowanie rektora o stwierdzonych naruszeniach ochrony danych osobowych oraz zagrożeniach tych naruszeń;
   d) wnioskowanie o usunięcie uchybień w razie stwierdzenia naruszenia przepisów o ochronie danych osobowych wraz z przedstawieniem propozycji rozwiązań zmierzających do usunięcia naruszeń;
   e) przeprowadzanie audytów oraz analiz stanu bezpieczeństwa ochrony danych;
   f) szkolenie pracowników uczestniczących w operacjach przetwarzania danych osobowych oraz podejmowanie działań zwiększających świadomość w zakresie ochrony tych danych;
   g) okresowa kontrola procedur, procesów i dokumentów Uczelni oraz ich obiegu pod kątem ochrony danych osobowych;

h) inicjowanie, koordynowanie i współuczestniczenie w procesie tworzenia oraz zmiany wewnętrznych aktów prawnych Uczelni z zakresu ochrony danych osobowych
i) monitorowanie przestrzegania RODO, innych przepisów o ochronie danych oraz polityk administratora danych osobowych lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków,
j) prowadzenie i utrzymywanie niezbędnej dokumentacji i ewidencji wynikającej z obowiązujących przepisów w zakresie ochrony danych, w tym w szczególności zestawienia zbiorów danych osobowych administrowanych, współadministrowanych i powierzonych oraz rejestru czynności i kategorii przetwarzania danych przetwarzanych na Uniwersytecie Przyrodniczym w Lublinie;
k) analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych;
l) identyfikowanie i analizowanie zagrożenia i ryzyka, na które może być narażone przetwarzanie danych osobowych;
m) wnioskowanie do Administrator Danych Osobowych danych o wdrożenie określonych zabezpieczeń adekwatnych do zagrożeń i ryzyka;
n) koordynacja nad procesem reagowania na naruszenia lub próby naruszenia bezpieczeństwa danych osobowych w systemie teleinformatycznym;
o) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
p) współpraca z organem nadzorczym; włączany od najwcześniejszego etapu we wszystkie kwestie związane z ochroną danych;
q) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

3. IODO wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
4. Status Inspektora Ochrony Danych Osobowych:
   a) Administrator Danych Osobowych zapewnia, by Inspektor Ochrony Danych Osobowych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
   b) Administrator Danych Osobowych wspiera Inspektora Ochrony Danych Osobowych w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby i przedsięwzięcia niezbędne do utrzymania właściwego poziomu oraz aktualizacji jego wiedzy fachowej;

c) Administrator Danych Osobowych zapewnia, aby Inspektor Ochrony Danych Osobowych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Inspektor Ochrony Danych Osobowych bezpośrednio podlega Administratorowi Danych Osobowych;
d) osoby, których dane dotyczą, mogą kontaktować się z IODO danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących;
e) IODO jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań;
f) IODO może wykonywać inne zadania i obowiązki. Administrator Danych Osobowych zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
g) IODO jest zobowiązany do zachowania tajemnicy lub poufności przy wykonywaniu swoich zadań.

§ 7

Administrator Systemu Informatycznego

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych i serwera z pozycji administratora systemów informatycznych,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3) na wniosek kierownika jednostki organizacyjnej przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6) wyrejestrowuje użytkowników na polecenie administratora danych osobowych lub kierownika jednostki organizacyjnej,
7) upoważniony jest do zmiany na stacjach roboczych haseł dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz w razie potrzeby Inspektorowi Danych Osobowych lub Administratorowi Danych Osobowych,

8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IODO o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii, zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego
11) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

§ 8

Odpowiedzialność kierowników komórek organizacyjnych oraz obowiązki pracowników

1. Każdy kierownik komórki organizacyjnej Uniwersytetu Przyrodniczego w Lublinie, w której przetwarzane są dane osobowe, odpowiedzialny jest za:
   a) zapewnienie aby bieżące przetwarzanie danych osobowych, w szczególności przetwarzanych w zbiorach danych osobowych było zgodne z powszechnie obowiązującymi przepisami prawa i aktami wewnętrznymi Uniwersytetu Przyrodniczego, w szczególności niniejszą Polityką;
   b) współdziałanie z Inspektorem Ochrony Danych Osobowych w zakresie zapewnienia przestrzegania ochrony danych osobowych;
   c) występowanie z wnioskiem o nadanie lub odebranie uprawnień do przetwarzania danych osobowych, w tym do ich przetwarzania w systemie informatycznym, jeżeli dane przetwarzane są w formie elektronicznej, zgodnie z procedurą nadawania uprawnień ujętą w dokumencie określającym szczegółowe zasady zarządzania systemami informatycznymi;
   d) zgłaszanie Inspektorowi ochrony danych zamiaru tworzenia, modyfikacji lub likwidacji zbioru, za który jest odpowiedzialny;
   e) zgłaszanie Inspektorowi Ochrony Danych Osobowych oraz Administratorowi Danych Osobowych zdarzeń zagrażających bezpieczeństwu danych osobowych.
2. Każdy pracownik Uniwersytetu Przyrodniczego obowiązany jest:
   a) zapoznać się oraz stosować postanowienia niniejszej Polityki ochrony danych osobowych;
   b) zapoznać się z obowiązującymi przepisami w zakresie ochrony danych osobowych;

c) zachować w tajemnicy wszelkie dane osobowe, które pozyskał w trakcie wykonywania obowiązków pracowniczych na rzecz Uniwersytetu;
d) przestrzegać stosowane przez Uniwersytet środki oraz sposoby zabezpieczeń danych osobowych przetwarzane przez Administrator Danych Osobowych;
e) dbać o bezpieczeństwo danych osobowych, do których ma dostęp.

3. Obowiązek zachowania w tajemnicy danych osobowych, które pracownik pozyskał w trakcie zatrudnienia w Uniwersytecie Przyrodniczym w Lublinie, nie gaśnie wraz z rozwiązaniem stosunku pracy.
4. Pracownik przed przystąpieniem do pracy, powinien odbyć przeszkolenie z zakresu danych osobowych przeprowadzone przez Inspektora Ochrony Danych Osobowych.
5. Naruszenie zasad ochrony danych osobowych wynikających z powszechnie obowiązujących przepisów prawa lub niniejszej Polityki oraz innych wewnętrznych aktów prawnych Uniwersytetu Przyrodniczego w Lublinie mogą zostać potraktowane jako naruszenie obowiązków pracowniczych.

§ 9

Bezpieczeństwo danych osobowych

1. Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:
   a) próby naruszenia ochrony danych:
      – z zewnątrz - włamania do systemu, podsłuch, kradzież danych,
      – z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych;
   b) złośliwe oprogramowanie;
   c) awarie sprzętu lub uszkodzenie oprogramowania powodujące utratę lub uszkodzenie danych;
   d) zabór sprzętu lub nośników z ważnymi danymi;
   e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.
2. W przypadku powzięcia wiadomości o zdarzeniu zagrażającym bezpieczeństwu danych osobowych lub podejrzeniu jego wystąpienia, pracownik Uniwersytetu Przyrodniczego zobowiązany jest poinformować IODO, w przypadku gdyby było to utrudnione lub niemożliwe, zobowiązany jest poinformować swojego bezpośredniego przełożonego.
3. IODO oraz bezpośredni przełożony osoby zgłaszającej zdarzenie zagrażające bezpieczeństwu informacji jest zobowiązany do niezwłocznego powiadomienia Administratora Danych Osobowych.
4. IODO niezwłocznie wszczyna postępowanie wyjaśniające i podejmuje wszystkie czynności konieczne w celu ustalenia:
   a) czasu wystąpienia naruszenia, zakresu, przyczyn, skutków, szkód;

b) osoby, która była odpowiedzialna za naruszenie;
c) opracowuje pisemny raport z przeprowadzonego postępowania zawierający wnioski na przyszłość i przedkłada go Administratorowi Danych Osobowych.

5. Ponadto, w przypadku naruszenia ochrony danych osobowych, Inspektor ochrony danych osobowych:
   a) zawiadamia osobę, której dane osobowe przetwarzane przez Administrator Danych Osobowych zostały naruszone, o każdym przypadku naruszenia jej danych osobowych przetwarzanych przez Administratora Danych Osobowych w stopniu skutkującym możliwością zaistnienia wysokiego ryzyka naruszenia praw lub wolności tej osoby fizycznej, chyba że przepisy obowiązującego prawa nie obligują Inspektora Ochrony Danych Osobowych do dokonania takiego zawiadomienia;
   b) w przypadkach przewidzianych przepisami prawa, dokonuje zgłoszenia naruszenia ochrony danych osobowych Organowi nadzorczemu oraz współpracuje z nim w toku wszczętego postępowania;
   c) współpracuje z Organem nadzorczym we wszelkich prowadzonych przez niego postępowaniach związanych z naruszeniem ochrony danych osobowych.

§ 10

Upoważnienie do przetwarzania danych

1. Do przetwarzania danych osobowych w systemie tradycyjnym i informatycznym mogą być dopuszczone osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych lub osobę upoważnioną przez Rektora do wydania upoważnienia.
1. Upoważnienia wydawane są:
   1) pracownikom - w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych.
   2) wykonawcom usług i dostawcom sprzętu lub oprogramowania - w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie.
2. Upoważnienia wydawane są na czas określony w trzech zakresach dostępu:
   a) podstawowym - przetwarzanie danych osobowych studentów i kandydatów na studia;
   b) rozszerzonym - przetwarzanie danych osobowych studentów jednostki i pracowników jednostki organizacyjnej;
   c) pełnym - przetwarzanie danych osobowych studentów i pracowników Administratora Danych Osobowych.

3. Wzór upoważnienia stanowi załącznik nr 3 do niniejszego dokumentu.
4. Zakres upoważnienia do przetwarzania danych osobowych jest adekwatny do zakresu wykonywanych zadań i nie może być on szerszy niż wynika to z realizowanych czynności zleconych przez Administratora Danych Osobowych.
5. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić zmiana zakresu upoważnienia do przetwarzania danych osobowych.
6. Upoważnienie wydaje się przy zatrudnianiu pracownika po odbyciu przez tę osobę szkolenia z zakresu ochrony danych osobowych oraz podpisaniu oświadczenia w którym zobowiązuje się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Tajemnica obowiązuje osobę upoważnioną przy przetwarzaniu danych osobowych, zarówno w trakcie trwania umowy, jak i po jej ustaniu. Wzór oświadczenia stanowi załącznik nr 4 .
7. Cofnięcie upoważnienia do przetwarzania danych następuje:
    1) wraz z rozwiązaniem stosunku łączącego go z Administratorem Danych Osobowych;
    2) na wniosek Inspektora Ochrony Danych Osobowych;
    3) na umotywowany wniosek bezpośredniego przełożonego;
    4) stwierdzenia zawinionego naruszenia ochrony danych osobowych.
8. Cofnięcie uprawnień do systemów informatycznych nadanych użytkownikowi następuje zgodnie z brzmieniem ust.1 .
9. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w formie papierowej lub elektronicznej, która odzwierciedla aktualny stan nadanych i odwołanych upoważnień do przetwarzania danych. Ewidencja powinna zawierać:
    1) nazwisko i imię osoby upoważnionej,
    1) stanowisko,
    2) datę nadania i ustania,
    3) zakres do przetwarzania danych osobowych.
10. Administrator Danych Osobowych zleca prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych Inspektorowi Ochrony Danych Osobowych.
11. Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi załącznik nr 5.
12. Inspektor Ochrony Danych Osobowych występuje do Administratora Systemu

Informatycznego o nadanie uprawnień do systemu informatycznego osobie upoważnionej do przetwarzania danych osobowych.

13. Administrator Systemu Informatycznego rejestruje użytkownika w systemie i nadaje mu określone uprawnienia, generuje użytkownikowi tymczasowe hasło oraz wpisuje osobę w ewidencję użytkowników w formie papierowej lub elektronicznej z prawami dostępu do systemów informatycznych, która zawiera:
    1) nazwisko i imię użytkownika,
    2) stanowisko,
    3) datę nadania i ustania uprawnień,
    4) systemy informatyczne do których użytkownik uzyskał uprawnienia,
    5) poziom nadanych uprawnień,
    6) informację czy użytkownik przetwarza dane osobowe w systemie informatycznym.
14. Wzór ewidencji użytkowników z uprawnieniami do systemów informatycznych stanowi załącznik nr 6 .
15. Zakres uprawnień użytkownika do systemu informatycznego jest adekwatny do zakresu wykonywanych zadań i nie może być on szerszy niż wynika to z realizowanych czynności zleconych przez Administratora Danych Osobowych. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić modyfikacja uprawnień nadanych użytkownikowi.

§ 11

Środki organizacyjne i techniczne zapewniające bezpieczeństwo przetwarzania danych osobowych i informacji w systemie tradycyjnym

1. Zabezpieczenie danych osobowych i informacji:

1) Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe i informacje odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych jednostek organizacyjnych.
2) Wszystkie dane, o których mowa w ust. 1, powinny być zabezpieczone fizycznie przed osobami nieupoważnionymi oraz przechowywane w urządzeniach gwarantujących dostęp do nich wyłącznie uprawnionych pracowników, tj. przynajmniej w pomieszczeniach zamykanych na klucz, z zastosowaniem

dodatkowego zabezpieczenia w postaci szafy drewnianej zamykanej na klucz lub szafy metalowej - w odniesieniu do szczególnie istotnych dla działalności Uniwersytetu danych.

3) Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich odpowiednie zabezpieczenie.
4) Pomieszczenia, w których przetwarzane są dane osobowe i informacje, zabezpieczone są na czas nieobecności osób zatrudnionych przy przetwarzaniu tych danych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
5) Dostęp do kluczy do pomieszczeń, w których przetwarzane są dane osobowe i informacje, posiadają wyłącznie osoby uprawnione. Przed rozpoczęciem pracy, klucze pobierane są od pracownika portierni, nadzorującego ich przechowywanie, zaś po zakończeniu pracy są one zdawane również do pracownika portierni.

1. Postępowanie z danymi osobowym i informacjami:

1) Pracownicy zobowiązani są stosować „politykę czystego biurka". Polega ona na utrzymywaniu porządku na stanowisku pracy pod nieobecność pracownika, poprzez umieszczanie dokumentów w szafie lub szufladzie zamykanej na klucz.
2) Dokumentacja zawierająca dane osobowe lub informacje podlega archiwizacji zgodnie z przepisami powszechnie obowiązującymi i aktami wewnątrzzakładowymi
3) Pracownicy zobowiązani są porządkować dokumentację pod względem jej użyteczności. Polega ona na niszczeniu wszelkiej dokumentacji roboczej lub tymczasowej zawierającej dane osobowe lub informacje niezwłocznie po ustaniu celu przetwarzania. Niszczenie polega w szczególności na:
   a) trwałym, fizycznym zniszczeniu danych osobowych i/lub ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy użyciu niszczarki lub innych skutecznych metod;
   b) anonimizacji danych osobowych i/lub ich zbiorów polegającej na pozbawieniu danych osobowych i/lub ich zbiorów cech pozwalających na identyfikacje osób fizycznych, których anonimizowane dane dotyczą.
4) Pracownicy zobowiązani są do przewożenia, przenoszenia i przekazywania dokumentów w sposób zapobiegający ich kradzieży, zagubieniu, utracie i dostępu osób nieupoważnionych.

§ 12

Dostęp do danych osobowych

1. Dostęp do danych osobowych oraz możliwość ich przetwarzania mają tylko osoby upoważnione przez Administratora Danych Osobowych do przetwarzania danych osobowych.
2. Wszystkie osoby, których praca będzie wiązała się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu przez Inspektora Ochrony Danych Osobowych z zakresu obowiązujących przepisów prawa oraz zasad dotyczących ochrony danych osobowych.

§ 13

Zasady udostępniania i powierzania przetwarzania danych osobowych

1. Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zasobach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.
3. Dane osobowe przetwarzane w Uniwersytecie Przyrodniczym udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
4. Wniosek powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
5. Wnioski w sprawie udostępnienia danych osobowych rozpatrywane są przez osobę odpowiedzialną merytorycznie za dostęp do przetwarzanych zasobów.
6. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli:
   1) spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane te dotyczą lub innych osób;
   2) dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.
7. Powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 28 RODO, wyłącznie w drodze umowy cywilnoprawnej zawartej w formie pisemnej, zgodnej w swojej zasadniczej treści z ustawą i rozporządzeniem. Niezbędnymi elementami tej umowy jest określenie celu, w jakim podmiot, któremu powierzono przetwarzanie danych może je przetwarzać oraz zakresu powierzonych do przetwarzania danych.

8. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia lub przetwarzania danych osobowych określa się przede wszystkim zobowiązania podmiotu przetwarzającego do:
   a) przetwarzania danych wyłącznie na udokumentowane polecenie administratora danych osobowych;
   b) zapewnienia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   c) podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomocy Administratorowi Danych Osobowych w wywiązywaniu się z tych obowiązków;
   d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego, w tym między innymi za zgodą Administratora Danych Osobowych;
   e) pomagania Administratorowi wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania jej praw określonych w RODO;
   f) usunięcia danych lub do zwrotu danych Administratorowi Danych Osobowych po zakończeniu przetwarzania, zgodnie z decyzją administratora;
   g) udostępniania Administratorowi Danych Osobowych wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania Administratorowi Danych Osobowych lub audytorowi upoważnionemu przez Administratora Danych Osobowych przeprowadzania audytów.
9. Odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na Administratorze Danych Osobowych, co nie wyłącza w żadnym przypadku odpowiedzialności podmiotu, z którym zawarto umowę, z tytułu przetwarzania danych niezgodnie z ustawą.

§ 14
Postanowienia końcowe

1. Polityka ochrony danych osobowych stanowi wewnętrzną regulację Uniwersytetu Przyrodniczego w Lublinie i obowiązuje wszystkich pracowników Uniwersytetu Przyrodniczego.
2. Polityka ochrony danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty w Uniwersytecie – tj. od dnia podpisania Zarządzenia przez Jego Magnificencję Rektora.
3. Każdy kto przetwarza dane posiadane przez Uniwersytet Przyrodniczy w Lublinie zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce ochrony danych osobowych.

4. W sprawach nieuregulowanych w niniejszej Polityce ochrony danych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy o ochronie danych osobowych oraz RODO.

Ustala się wykaz załączników do Polityki Bezpieczeństwa:

1. Wykaz środków technicznych i organizacyjnych stosowanych przez Uniwersytet Przyrodniczy w Lublinie w celu realizacji Polityki - zał. nr 1.
2. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych - zał. nr 2.
3. Wzór upoważnienia do przetwarzania danych osobowych – zał. nr 3
4. Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych – zał. nr 4.
5. Wzór Rejestru Upoważnień – zał. nr 5.
6. Wzór rejestru użytkowników z uprawnieniami do systemów informatycznych – zał. nr 6
7. Wzór rejestru naruszeń danych osobowych – zał. nr 7