Zarządzenie Nr 31/2019/2020
Rektora Uniwersytetu Kazimierza Wielkiego
z dnia 2 stycznia 2020 r.

w sprawie zmiany instrukcji regulujących zagadnienia ochrony danych osobowych oraz pracy w systemach informatycznych służących do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego

Na podstawie art. 23 ust. 2 pkt 2) ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r., poz. 1668 z późn. zm.) oraz art. 24 ust. 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)

zarządzam,

co następuje:

§ 1

Wprowadzam do użytku służbowego:

1) „Politykę bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego", której treść stanowi załącznik nr 1 do niniejszego zarządzenia.
2) „Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego", której treść stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 2

Instrukcje, o których mowa w § 1 pkt 1 i 2 mają zastosowanie na wszystkich stanowiskach pracy i innych miejscach, w których przetwarzane są dane osobowe w Uniwersytecie Kazimierza Wielkiego.

§ 3

Z treścią instrukcji, o których mowa w § 1 kierownicy jednostek organizacyjnych zapoznają wszystkich pracowników zatrudnionych w danej jednostce przy przetwarzaniu danych osobowych lub pracujących w systemach informatycznych.

§ 4

Traci moc obowiązującą Zarządzenie Nr 51/2017/2018 Rektora Uniwersytetu Kazimierza Wielkiego z dnia 25 maja 2018 r. w sprawie wprowadzenia instrukcji regulujących zagadnienia ochrony danych osobowych oraz pracy w systemach informatycznych służących do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego oraz Zarządzenie Nr 2/2018/2019 Rektora Uniwersytetu Kazimierza Wielkiego z dnia 1 października 2018 r. zmieniające Zarządzenie Nr 51/2017/2018 Rektora Uniwersytetu Kazimierza Wielkiego z dnia 25 maja 2018 r.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

prof. dr hab. Jacek Woźny

Załącznik Nr 1
do Zarządzenia Nr 31/2019/2020
Rektora UKW
z dnia 2 stycznia 2020 r.

POLITYKA BEZPIECZEŃSTWA
przetwarzania danych osobowych
w Uniwersytecie Kazimierza Wielkiego

I. Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego w Bydgoszczy, zwana dalej „Polityką", jest dokumentem określającym zasady postępowania, stosowane środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa w zakresie ochrony danych osobowych przetwarzanych w formie papierowej oraz w systemach informatycznych.
2. Uniwersytet Kazimierza Wielkiego w Bydgoszczy, zwany dalej „Uniwersytetem", realizując Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby te dane były:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania.
3. Uniwersytet realizując Politykę dąży do systematycznego unowocześniania stosowanych w jego strukturze fizycznych, informatycznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Szczegółowe zasady ochrony danych osobowych przetwarzanych w zbiorach informatycznych Uniwersytetu określa Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

5. Niniejszy dokument przeznaczony jest dla pracowników Uniwersytetu zatrudnionych przy przetwarzaniu danych osobowych, dla pozostałych pracowników Uniwersytetu oraz dla osób współpracujących z Uniwersytetem przy przetwarzaniu danych osobowych i stanowić ma praktyczną wykładnię stosownych przepisów.

§ 2

1. Wyjaśnienia używanych pojęć:
    1. dane osobowe – **wszelkie** informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (nazwisko, imię, numer PESEL, data urodzenia, adres, numer konta bankowego, wysokość wynagrodzenia, wysokość stypendium, zaległości w opłatach za czesne, numer telefonu, adres e-mail itd.),
    2. Inspektor Ochrony Danych – osoba wyznaczona przez Rektora, nadzorującą przestrzeganie zasad ochrony danych osobowych w Uniwersytecie,
    3. administrator systemu informatycznego – osoba nadzorująca funkcjonowanie systemu komputerowego; w szczególnych przypadkach administratorem systemu informatycznego może być osoba odpowiedzialna za funkcjonowanie aplikacji przetwarzających dane osobowe na pojedynczym komputerze (np. obsługującym komunikację z bankiem),
    4. zbiór danych – każdy uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie; w przypadku Uniwersytetu takimi zbiorami są zbiory studentów, kandydatów na studia, pracowników, czytelników biblioteki itp.,
    5. przetwarzanie danych osobowych – **jakiekolwiek** operacje wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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,
    6. osoba współpracująca – osoba wykonująca na podstawie umowy cywilno-prawnej usługę, w ramach której przetwarzane są dane osobowe lub osoba realizująca w Uniwersytecie praktykę studencką, praktykę zawodową lub osoba w inny sposób związana z Uniwersytetem, niebędąca pracownikiem,
    7. osoba upoważniona do przetwarzania danych osobowych – pracownik Uniwersytetu lub osoba współpracująca, który został przeszkolony w zakresie ochrony danych osobowych i uzyskał upoważnienie do ich przetwarzania,
    8. dysponent danych – osoba fizyczna, której dane dotyczą,
    9. osoba nieuprawniona – osoba niezatrudniona lub nie współpracująca przy przetwarzaniu danych osobowych (z wyłączeniem osoby uprawnionej do ich przeglądania i przetwarzania na mocy odrębnych przepisów),
    10. Rozporządzenie UE 2016/679 – 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 „RODO”).

II. Zasady dopuszczania osób do przetwarzania danych osobowych

§ 3

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych.
2. Upoważnienia nadaje Rektor.
3. Rektor może udzielić Prorektorom, Kanclerzowi, Kwestorowi oraz Dyrektorowi Biblioteki pełnomocnictwa do nadawania upoważnień, o których mowa w ust. 1. Pełnomocnictwo takie stanowi jednocześnie upoważnienie do przetwarzania danych osobowych dla Pełnomocnika we wszystkich zbiorach danych.
4. Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do Polityki.
5. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 2 do Polityki.
6. Inspektor Ochrony Danych prowadzi rejestr upoważnień nadanych przez Rektora.
7. Osoby wymienione w ust. 3 prowadzą rejestr upoważnień nadanych przez siebie lub poprzedników pełniących wcześniej daną funkcję.
8. W przypadku jakiejkolwiek zmiany w rejestrze (wpisanie upoważnienia, odebranie upoważnienia) osoby wymienione w ust. 3 przekazują kopię swojego zaktualizowanego rejestru Inspektorowi Ochrony Danych, który przechowuje wszystkie rejestry lub ich kopie, to jest rejestr upoważnień nadanych przez Rektora oraz kopie rejestrów wymienionych w ust. 7.
9. Wzór rejestru upoważnień stanowi załącznik nr 3 do Polityki.

§ 4

1. Upoważnienie nadawane jest pracownikowi na pisemny wniosek przełożonego upoważnianej osoby.
2. W przypadku osoby wykonującej na podstawie umowy cywilno-prawnej usługę, w ramach której przetwarzane są dane osobowe lub osoby realizującej w Uniwersytecie praktykę studencką, praktykę zawodową lub osoby w inny sposób związanej z Uniwersytetem (osoba współpracująca), z pisemnym wnioskiem o nadanie upoważnienia występuje kierownik jednostki organizacyjnej zlecającej usługę lub inne zadania związane z przetwarzaniem danych osobowych.
3. Jeżeli osoba upoważniana (pracownik, osoba współpracująca) **podlega nadającemu upoważnienie bezpośrednio**, upoważnienie nadaje się bez wniosku.
4. Rektor lub osoby wymienione w § 3 ust. 3 mogą:
   1) wyrazić zgodę na nadanie uprawnień zgodnie z wnioskowanym zakresem,
   2) wyrazić zgodę na nadanie ograniczonych uprawnień zawierających się we wnioskowanym zakresie,

3) nie wyrazić zgody na nadanie uprawnień.

5. Decyzja przekazywana jest osobie wnioskującej. W przypadku wydania decyzji o ograniczeniu uprawnień lub odmowy wydania upoważnienia, decyzja musi być sporządzona w formie pisemnej i zawierać uzasadnienie.
6. Od decyzji osób wymienionych w § 3 ust. 3 wnioskujący może odwołać się do Rektora. Decyzja Rektora jest ostateczna.
7. Osoba wnioskująca przekazuje decyzję osobie uprawnianej.

§ 5

1. Nadanie upoważnienia do przetwarzania danych osobowych (w szczególności w systemie informatycznym) obejmuje:
   1) przeprowadzenie przez Inspektora Ochrony Danych szkolenia w zakresie bezpieczeństwa danych osobowych oraz prawnych aspektów ochrony tych danych lub
   2) ukończenie przez osobę internetowego kursu udostępnianego przez Uniwersytet na stronie odo.ukw.edu.pl i zdanie zamieszczonego tam testu,
   3) wydanie osobie upoważnianej upoważnienia do przetwarzania danych osobowych, zawierającego zakres nadawanych uprawnień do przetwarzania danych osobowych, informację o zbiorze osób, do którego nadawane są uprawnienia, systemie informatycznym, w którym dane będą przetwarzane (jeśli dotyczy), datę nadania upoważnienia oraz, jeśli upoważnienie nadawane jest terminowo, datę wygaśnięcia upoważnienia,
   4) w przypadku przetwarzania danych osobowych w systemie informatycznym - nadanie osobie przez administratora systemu informatycznego identyfikatora oraz hasła, a także skonfigurowanie uprawnień w systemie.
2. W przypadku konieczności zmiany zakresu upoważnienia (inny lub kolejny zbiór osób, inny zakres przetwarzania danych osobowych, zmiana stanowiska pracy przez pracownika) należy przedłożyć Rektorowi lub osobie wymienionej w § 3 ust. 3 nowy wniosek o nadanie upoważnienia, stosując odpowiednio zapisy § 4.
3. W przypadku nadania osobie nowego upoważnienia dla danego zbioru osób, wygasa poprzednie upoważnienie.

§ 6

1. Odebranie upoważnienia do przetwarzania danych osobowych może mieć miejsce, gdy:
   1) z pracownikiem została rozwiązana (zakończona) umowa o pracę,
   2) zakres obowiązków służbowych pracownika uległ zmianie, która spowodowała utratę potrzeby przetwarzania danych osobowych,
   3) osoba spowodowała swoim celowym działaniem incydent mający negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych,
   4) istnieje uzasadniona obawa, że przetwarzanie danych osobowych przez osobę wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.
2. Odebranie upoważnienia może nastąpić na wniosek:
   1) Rektora,

2) osoby wymienionej w § 3 ust. 3,

3) przełożonego pracownika lub zwierzchnika osoby współpracującej,

4) kierownika Działu Kadr i Szkolenia,

5) Inspektora Ochrony Danych,

6) kierownika działu odpowiedzialnego za informatyzację Uczelni.

3. Proces odebrania upoważnienia obejmuje:

1) przekazanie Inspektorowi Ochrony Danych pisemnego wniosku o odebranie upoważnienia (za wyjątkiem sytuacji, gdy wnioskującym jest Inspektor Ochrony Danych) z określeniem imienia i nazwiska pracownika oraz jego identyfikatora w systemie informatycznym (jeśli pracownik posiada dostęp do systemu informatycznego), zakresu upoważnienia, które ma zostać odebrane, a także przyczyny konieczności odebrania upoważnienia,

2) jeśli wnioskującym jest Inspektor Ochrony Danych, przygotowanie przez niego pisemnej notatki zawierającej informacje wskazane w pkt. 1),

3) w przypadku posiadania przez pracownika, któremu upoważnienie jest odbierane uprawnień do systemu informatycznego, przekazanie przez Inspektora Ochrony Danych administratorowi systemu informatycznego polecenia unieważnienia hasła, zablokowania konta użytkownika, odebrania wszelkich uprawnień do systemu; administrator systemu winien bez zbędnej zwłoki wykonać niezbędne czynności,

4) poinformowanie przez Inspektora Ochrony Danych wnioskodawcy o odebraniu pracownikowi upoważnienia do przetwarzania danych osobowych i o odebraniu (jeśli nastąpiło) uprawnień do systemu informatycznego.

§ 7

Upoważnienie do przetwarzania danych osobowych przygotowywane jest w trzech egzemplarzach: po jednym dla upoważnianej osoby, wnioskodawcy oraz dla Inspektora Ochrony Danych (jeśli upoważnienie nadane zostało przez Rektora) lub dla osoby wymienionej w § 3 ust. 3. Jeśli upoważnienie nadawane jest bez wniosku, przygotowuje się je w dwóch egzemplarzach: po jednym dla upoważnianej osoby oraz dla Inspektora Ochrony Danych (jeśli upoważnienie nadane zostało przez Rektora) lub dla osoby wymienionej w § 3 ust. 3.

§ 8

Pracownicy nieposiadający w zakresie swoich obowiązków czynności związanych z przetwarzaniem danych osobowych (osoby sprzątające, portierzy, pracownicy techniczni, konserwatorzy, elektrycy itp.), a których obowiązki wymuszają pracę - pod nieobecność osób upoważnionych do przetwarzania danych osobowych - w pomieszczeniach, w których dane osobowe są przetwarzane, muszą zostać zapoznane z zasadami dotyczącymi ochrony danych osobowych oraz uzyskać upoważnienie do przebywania w w/w pomieszczeniach.

III. Szkolenia w zakresie bezpieczeństwa danych osobowych

§ 9

1. Przed dopuszczeniem do przetwarzania danych osobowych pracownik Uniwersytetu (lub osoba współpracująca z Uniwersytetem) musi zostać przeszkolony w zakresie przepisów prawnych dotyczących ochrony danych osobowych oraz zasad ochrony danych osobowych obowiązujących w Uniwersytecie.
2. Za przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych, a za zorganizowanie szkolenia odpowiada wnioskujący wymieniony w § 4 ust. 1 lub ust. 2.
3. Szkolenie w szczególności powinno obejmować:
   1) przedstawienie Rozporządzenia UE 2016/679 oraz ustawy o ochronie danych osobowych i ich wpływu na przebieg procesów związanych z przetwarzaniem danych osobowych w Uniwersytecie,
   2) przedstawienie przepisów wewnętrznych obowiązujących w Uniwersytecie, regulujących zasady ochrony danych osobowych,
   3) w przypadku szkoleń prowadzonych przez Inspektora Ochrony Danych przedstawienie praktycznych rozwiązań ochrony danych osobowych na danym stanowisku pracy.

IV. Zasady obowiązujące przy zbieraniu danych

§ 10

1. Każda osoba, której dane osobowe mają być przetwarzane w Uniwersytecie **musi zostać poinformowana** przez administratora danych (Uniwersytet) o:
   1) adresie siedziby Uniwersytetu i jego pełnej nazwie,
   2) danych kontaktowych Inspektora Ochrony Danych,
   3) celach oraz podstawie prawnej przetwarzania danych,
   4) prawnie uzasadnionych interesach realizowanych przez Uniwersytet (jeśli dotyczy),
   5) znanych lub potencjalnych odbiorcach danych,
   6) gdy ma to zastosowanie – zamiarze przekazania danych osobowych do państwa trzeciego (poza obszar Unii Europejskiej) lub organizacji międzynarodowej,
   7) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu,
   8) prawie do żądania od Uniwersytetu dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   9) jeśli przetwarzanie odbywać się będzie na podstawie zgody osoby – prawie osoby do wycofania zgody,
   10) prawie wniesienia skargi do organu nadzorczego (PUODO),

11) tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,

12) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,

13) jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą – źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

2. Informacji należy udzielić przed uzyskaniem od osoby jej danych.
3. Jeżeli planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane zostały zebrane, przed takim dalszym przetwarzaniem należy poinformować osobę, której dane dotyczą, o tym innym celu.
4. W przypadku kandydatów na pracowników oświadczenie o poinformowaniu osoby przez Uniwersytet o okolicznościach wskazanych w ust. 1. wraz z podpisem kandydata na pracownika przyjmuje i przechowuje Dział Kadr i Szkolenia. Dokument tworzony jest w jednym egzemplarzu, przechowywanym wraz z dokumentacją kandydata.
5. W przypadku osób zatrudnianych na podstawie umowy o pracę (nowych pracowników) informacja określona w ust. 1 oraz oświadczenie osoby o jej poinformowaniu przez Uniwersytet zawarte muszą być na druku kwestionariusza osobowego.
6. W przypadku kandydatów na studia informacja określona w ust. 1. umieszczona musi być na pierwszej stronie rejestracji internetowego systemu rekrutacji. By przejść do kolejnych etapów rejestracji, kandydat musi potwierdzić, że został o w/w okolicznościach poinformowany. Oświadczenie osoby o jej poinformowaniu przez Uniwersytet przechowywane jest w formie elektronicznej.
7. W przypadku osób zatrudnianych na podstawie umowy cywilno-prawnej informacja określona w ust. 1 oraz oświadczenie osoby o jej poinformowaniu przez Uniwersytet zawarte muszą być na druku umowy.
8. W przypadku pozostałych kategorii osób obowiązek informacyjny musi być zrealizowany z wykorzystaniem druku zawierającego informację określoną w ust. 1 oraz oświadczenie osoby o jej poinformowaniu przez Uniwersytet. Druk przekazuje osobie do podpisu i później przechowuje jednostka przyjmująca do przetwarzania dane osoby.
9. **Bezwzględnie zabronione jest kopiowanie (skanowanie, kserowanie itp.) dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, jak również żądanie od osoby pozostawienia takiego dokumentu (na przykład jako „zastawu”).**

V. Zasady ochrony danych osobowych

§ 11

1. Osoby upoważnione do przetwarzania danych osobowych przetwarzają je tylko w zakresie wynikającym z udzielonego im upoważnienia.

2. Przetwarzający dane zobowiązani są do zachowania w tajemnicy treści przetwarzanych danych oraz sposobów ich zabezpieczania.

§ 12

1. Zabronione jest wywieszanie w miejscach ogólnodostępnych (np. gablotach na korytarzach) jakichkolwiek list lub innych dokumentów zawierających dane osobowe. Wyjątkiem są przypadki wynikające z przepisów prawa określających jawność danego procesu (np. listy z wynikami rekrutacji na studia, wyniki postępowań w ramach zamówień publicznych, w których zwycięzcami są osoby fizyczne).
2. Dopuszczalne jest wywieszanie w miejscach ogólnodostępnych list studentów z podziałem na grupy ćwiczeniowe, laboratoryjne itp. Jednak na listach mogą zostać podane wyłącznie imię i nazwisko studenta. Niedopuszczalne jest podawanie na takich listach jakichkolwiek innych danych osobowych (np. adresu, numeru PESEL, daty urodzenia, numeru albumu itd.).
3. Dozwolone jest publikowanie na stronach internetowych Uniwersytetu lub w jakiejkolwiek innej formie następujących danych osobowych pracowników: imię, nazwisko, stanowisko, służbowy numer telefonu, służbowy adres e-mail.
4. Zabronione jest publikowanie na stronach internetowych Uniwersytetu lub w jakiejkolwiek innej formie innych danych pracowników (w tym prywatnych numerów telefonów, prywatnych adresów e-mail, adresów prywatnych stron WWW, wizerunku pracownika itp.), chyba, że pracownik wyrazi na to zgodę w formie pisemnej.
5. Zgoda, o której mowa w ust. 4 przechowywana jest przez osoby wymienione w § 3 ust. 3 oraz Inspektora Ochrony Danych.
6. Zabronione jest przekazywanie danych osobowych osobom nieuprawnionym telefonicznie, elektronicznie lub w jakiejkolwiek innej formie.
7. Dokumenty zawierające dane osobowe, przenoszone lub przewożone pomiędzy jednostkami Uniwersytetu znajdującymi się w różnych lokalizacjach muszą być zamknięte w zaklejonej kopercie lub w zamkniętym pojemniku (skrzyni, kartonie) zabezpieczonym taśmą z pieczątką jednostki przekazującej do transportu dokumenty, w taki sposób, że otwarcie pojemnika spowoduje zerwanie taśmy.
8. Przekazywanie w ramach jednostki organizacyjnej lub pomiędzy jednostkami nośników informatycznych lub dokumentów zawierających dane osobowe, może odbywać się tylko pomiędzy osobami posiadającymi upoważnienia do przetwarzania danych osobowych określonych zbiorów osób.
9. Pracowników przetwarzających dane osobowe obowiązuje zasada „czystego biurka”, a więc niepozostawianie „na wierzchu”, w szczególności w miejscu dostępnym dla osób nieuprawnionych, niezabezpieczonych dokumentów oraz nośników zawierających dane osobowe.
10. Osoby nieuprawnione mogą przebywać w pomieszczeniu, w którym przetwarzane są dane osobowe jedynie w obecności pracownika Uniwersytetu upoważnionego do przetwarzania tych danych.
11. Klucze oraz uprawnienia (na przykład kody alarmu) do pomieszczeń, w których przetwarzane są dane osobowe, mogą być udostępniane jedynie osobom upoważnionym do przetwarzania danych osobowych lub osobom posiadającym upoważnienie do przebywania w takich pomieszczeniach.

§ 13

1. Użytkownik systemu informatycznego nie może udostępniać identyfikatora, hasła i stanowiska roboczego innym osobom, w szczególności osobom nieuprawnionym.

2. Zabronione jest zapisywanie hasła w sposób umożliwiający dostęp do niego innym osobom.
3. W jednostkach organizacyjnych i systemach informatycznych, w których jest to możliwe, należy użytkownikom ograniczyć uprawnienia czasowe do pracy tylko w godzinach roboczych.
4. Podłączenie urządzenia końcowego (komputera, terminala, drukarki) do sieci informatycznej Uniwersytetu dokonywane jest przez administratora systemu informatycznego (sieci) lub osobę przez niego wyznaczoną. Wyjątek stanowią miejsca, w których stosowana jest polityka otwartego dostępu do sieci w trybie ograniczonym (np. Sala Senatu UKW, miejsca organizacji konferencji), gdzie dopuszczalne jest podłączenie urządzenia końcowego przez osoby inne, niż administrator systemu informatycznego (sieci), czy osoba przez niego wyznaczona.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, w których mogą przebywać osoby nieuprawnione, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Niedozwolone jest przesyłanie danych osobowych lub dokumentów je zawierających z wykorzystaniem kont pocztowych spoza domeny *ukw.edu.pl*.
7. Serwis sprzętu komputerowego zawierającego dane osobowe wykonywany jest wyłącznie przez pracowników działu odpowiedzialnego za informatyzację Uczelni. Jeśli zaistnieje konieczność przekazania takiego sprzętu do serwisu zewnętrznego, bezwzględnie należy z przekazywanych twardych dysków i innych nośników informatycznych usunąć dane osobowe w sposób uniemożliwiający ich odczyt.
8. Serwery lub inne istotne dla przetwarzania danych osobowych elementy systemów informatycznych nie mogą być umieszczane bezpośrednio na podłodze ze względu na możliwość zniszczenia przez wodę w przypadku awarii sieci wodociągowej i zalania pomieszczenia. Serwerownie muszą być także wyposażone w odpowiedni sprzęt gaśniczy.
9. Serwery systemów informatycznych, w których przetwarzane są dane osobowe oraz inne urządzenia informatyczne przechowujące te dane muszą być zabezpieczone przed nieprzewidzianymi przerwami w zasilaniu przy pomocy zasilaczy awaryjnych (UPS)..
10. Komputery oraz inne urządzenia informatyczne, przy pomocy których przetwarzane są dane osobowe, powinny posiadać wydzielony obwód zasilania, dedykowany dla sprzętu informatycznego. Szczególnie niedopuszczalne jest zasilanie z tych samych gniazd, listew zasilających lub przeciwprzepięciowych urządzeń o dużym poborze mocy (na przykład czajników elektrycznych, grzejników itp.).
11. W przypadku planowanych wyłączeń zasilania/energii elektrycznej, pracownicy działu przeprowadzającego wyłączenie muszą o nim bezwzględnie poinformować odpowiednio wcześniej wszystkie jednostki organizacyjne, których wyłączenie może dotyczyć, a w których dane osobowe przetwarzane są z wykorzystaniem systemów informatycznych, tak by przed wyłączeniem zasilania można było w bezpieczny sposób zakończyć przetwarzanie danych w systemie.
12. **Zabronione jest przetwarzanie danych osobowych w zewnętrznych systemach informatycznych (np. w „chmurze") bez zgody Rektora.**

§ 14

1. Dane osobowe przetwarzane w systemie informatycznym muszą być zabezpieczane poprzez tworzenie kopii zapasowych umożliwiających odtworzenie danych w przypadku awarii. Za wykonywanie kopii odpowiadają

administratorzy systemów informatycznych lub osoby wyznaczone do zarządzania systemem (na przykład w przypadku pozasieciowych, jednostanowiskowych systemów).

2. Kopie zapasowe tworzone na zewnętrznych nośnikach informatycznych (na taśmach, pendrive'ach, płytach CD, DVD itp.) muszą być przechowywane w szafach, szufladach lub pomieszczeniach zamykanych na klucz, do których dostęp mają jedynie osoby odpowiedzialne za wykonywanie i zabezpieczanie tych kopii. Kopie należy przechowywać w innym pomieszczeniu (a w miarę możliwości innym budynku), niż to, w którym znajduje się (na przykład na serwerze) oryginalny, wykorzystywany w bieżącej pracy zbiór danych.
3. Dane osobowe wykorzystywane poza systemem informatycznym (na pendrive'ach, płytach CD, DVD itp.) po zakończeniu pracy muszą być przechowywane w zamykanych na klucz meblach biurowych. Klucze do mebli należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych
4. W komputerach, w których nie ma potrzeby wykorzystywania zewnętrznych nośników danych (pendrive'ów, płyt CD/DVD, dysków zewnętrznych itp.) należy w miarę możliwości zablokować możliwość zapisu na płytach CD/DVD oraz porty USB, by ograniczyć możliwość kopiowania danych osobowych na takie nośniki.
5. Dokumenty w formie papierowej zawierające dane osobowe winny być przechowywane w szafach zamykanych na klucz, do których dostęp mają jedynie osoby upoważnione do przetwarzania danych osobowych.
6. Jeśli przechowywanie dokumentów w formie papierowej w szafach nie jest możliwe, należy uniemożliwić dostęp do tych dokumentów osobom nieupoważnionym, przy czym dokumenty nie mogą być przechowywane na podłodze, ze względu na możliwość zniszczenia ich przez wodę w przypadku awarii sieci wodociągowej i zalania pomieszczenia.
7. Robocze, błędne lub nieaktualne wydruki oraz kopie danych tworzone na nośnikach informatycznych należy usuwać (niszczyć) natychmiast po ustaniu ich przydatności.
8. Niedopuszczalne jest pozostawianie po zakończeniu pracy w danym dniu dokumentów, wydruków zawierających dane osobowe w drukarkach, kserokopiarkach, skanerach i tym podobnych urządzeniach.
9. Niepotrzebne już dokumenty w formie papierowej zawierające dane osobowe muszą zostać zniszczone w sposób uniemożliwiający ich odczytanie, to jest przy pomocy niszczarki. **Nie wolno wyrzucać takich dokumentów bez odpowiedniego ich zniszczenia!**
10. **Zabronione jest wynoszenie poza obiekty Uniwersytetu danych osobowych w jakiejkolwiek formie, zarówno papierowej, jak i elektronicznej**. Wyjątkiem są sytuacje wymagające przekazania danych osobowych pomiędzy jednostkami organizacyjnymi Uniwersytetu znajdującymi się w różnych lokalizacjach.
11. Pomieszczenia zawierające kluczowe z punktu widzenia ochrony danych osobowych zbiory, jak archiwa lub serwerownie, należy w miarę możliwości zabezpieczyć dodatkowo poprzez instalację zamków wyższej klasy, systemów alarmowych i krat w oknach (jeśli pomieszczenie posiada okna). Pomieszczenia takie muszą być całodobowo nadzorowane przez pracowników ochrony bezpośrednio lub z wykorzystaniem systemu monitoringu.

VI. Udostępnianie danych osobowych

§ 15

1. Uniwersytet udostępnia przetwarzane dane osobowe osobom do tego upoważnionym na mocy uregulowań wewnętrznych obowiązujących w tym zakresie.
2. Nadanie upoważnienia, o którym mowa w ust. 1., wynikać może w szczególności:
   1) z charakteru pracy wykonywanej na danym stanowisku,
   2) z dokumentu określającego zakres obowiązków danego pracownika,
   3) z zakresu czynności wykonywanych przez osobę współpracującą z Uniwersytetem, z którego wynika konieczność dostępu do danych osobowych.

3. Uniwersytet udostępnia dane osobowe podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
4. Dane osobowe udostępnia się podmiotom określonym w ust. 3 na pisemny wniosek. Wniosek powinien zawierać podaną podstawę prawną, z której wynika uprawnienie podmiotu, informacje umożliwiające wyszukanie w zbiorze osoby, której dotyczy wniosek oraz wskazywać ich zakres i przeznaczenie.
5. Dane udostępniane na podstawie określonego w ust. 4 wniosku przekazywane są w formie pisemnej, na adres wnioskującego podmiotu.
6. Uniwersytet zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych.
7. Osoby niezatrudnione przy przetwarzaniu danych osobowych określonej kategorii, w tym dysponenci danych osobowych, osoby mające interes prawny w uzyskaniu dostępu do tych danych mogą mieć do nich **wgląd wyłącznie** w obecności upoważnionego pracownika Uniwersytetu.
8. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia Rektora lub upoważnienia nadanego przez osobę wymienioną w § 3 ust. 3 może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
9. W szczególności dostęp do danych osobowych na wskazanej w ust. 8. zasadzie mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Straż Graniczna, Służba Celna, Żandarmeria Wojskowa, prokuratura, Najwyższa Izba Kontroli, Prezes Urzędu Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień - wszystkie wyżej wymienione po okazaniu dokumentów potwierdzających te uprawnienia.
10. **W przypadku studentów udostępnianie dokumentacji oraz informacji dotyczących przebiegu studiów osobom innym, niż student lub osoba upoważniona przez niego na piśmie, jest niedozwolone**.

§ 16

1. Dysponent danych osobowych (osoba, której dane są przetwarzane) może upoważnić inną osobę do dostępu do jej danych osobowych, w tym do odbioru dokumentów zawierających dane. Upoważnienie musi być sporządzone w formie pisemnej. Upoważnienie takie przechowywane jest bezterminowo przez jednostkę organizacyjną udostępniającą dane osobowe.

2. Autentyczność upoważnienia, o którym mowa w ust. 1, powinna zostać potwierdzona:

   1) poprzez osobiste przedłożenie w jednostce organizacyjnej Uniwersytetu upoważnienia **przez osobę upoważniającą** lub
   2) w przypadku przedkładania upoważnienia **przez osobę upoważnianą**, poprzez **przesłanie przez osobę upoważniającą** do jednostki Uniwersytetu oświadczenia o potwierdzaniu autentyczności z adresu e-mail uznawanego przez Uniwersytet za oficjalny kanał komunikacji z osobą (w przypadku pracowników są to adresy e-mail z domeny ukw.edu.pl, w przypadku studentów są to adresy e-mail wprowadzone do systemu USOS).

3. Pracownik Uniwersytetu udostępniający dane na podstawie takiego upoważnienia ma obowiązek potwierdzić tożsamość osoby, której udostępnia się te dane.

§ 17

1. W przypadku studentów zalecane jest dokonanie na początku każdego roku akademickiego upoważnienia starosty przez pozostałe osoby studiujące na danym roku, do dostępu do ich danych osobowych, w tym do odbioru dokumentów zawierających dane.
2. **Nadanie takiego upoważnienia przez studenta staroście roku jest całkowicie dobrowolne.**
3. Upoważnienie przekazywane jest przez starostę do właściwego Dziekanatu.
4. **Zabronione jest udostępnianie przez pracowników Uniwersytetu lub osoby współpracujące danych osobowych studenta innym studentom (np. w postaci wspólnej listy z ocenami z egzaminów, listy z adresami e-mail itp.), chyba że student wyraził na to zgodę w formie pisemnej.**

VII. Powierzanie przetwarzania danych osobowych

§ 18

1. W przypadku przekazywania danych osobowych, których administratorem jest Uniwersytet, do przetwarzania podmiotom zewnętrznym konieczne jest zawarcie z podmiotem zewnętrznym (podmiotem przetwarzającym) **pisemnej umowy** o powierzeniu przez Uniwersytet przetwarzania danych osobowych. Może to być odrębna umowa lub integralna część umowy pierwotnej (umowy, z której wynika konieczność powierzenia przetwarzania danych osobowych).
2. Umowę przygotowuje jednostka organizacyjna powierzająca przetwarzanie danych osobowych, we współpracy z Radcą Prawnym Uniwersytetu oraz Inspektorem Ochrony Danych.
3. Warunki umowy dotyczące ochrony powierzanych danych osobowych akceptuje Inspektor Ochrony Danych.
4. Umowa musi w szczególności określać:
   1) przedmiot przetwarzania,
   2) czas trwania przetwarzania,
   3) charakter i cel przetwarzania,
   4) rodzaj danych osobowych,

5) kategorię osób, których dane dotyczą,
6) obowiązki i prawa administratora,
7) obowiązki podmiotu przetwarzającego.

5. W uzasadnionych przypadkach Inspektor Ochrony Danych może nie wyrazić zgody na powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu.

VIII. Monitorowanie zagrożeń, analiza ryzyka i wdrażanie rozwiązań minimalizujących ryzyko

§ 19

1. Kierownicy jednostek organizacyjnych, w których przetwarzane są dane osobowe zobowiązani są do stałego monitorowania zagrożeń związanych z przetwarzaniem w ramach ich jednostki danych osobowych, a następnie do analizy ryzyka w tym obszarze.
2. W szczególności wzrost ryzyka przetwarzania danych może być związany z:

   1) wynikającej ze zmian w przepisach prawa konieczności wprowadzania nowych rozwiązań technicznych lub organizacyjnych w zakresie przetwarzania danych,
   2) stwierdzeniem naruszeń ochrony danych,
   3) wprowadzaniem modyfikacji procesu przetwarzania danych osobowych w określonym istniejącym zbiorze,
   4) planowaniem przetwarzania danych osobowych w nowym zbiorze,
   5) planowaniem powierzenia przetwarzania danych podmiotowi zewnętrznemu,
   6) planowaniem przyjęcia powierzenia przetwarzania danych od podmiotu zewnętrznego.

3. W przypadku stwierdzenia wzrostu ryzyka, kierownik jednostki organizacyjnej w uzgodnieniu z Inspektorem Ochrony Danych ustala, a następnie wdraża rozwiązania minimalizujące ryzyko.

IX. Zasady rejestracji zbiorów danych w rejestrze czynności oraz w rejestrze kategorii czynności

§ 20

1. Rejestr czynności przetwarzania oraz rejestr kategorii przetwarzania dla Uniwersytetu prowadzi Inspektor Ochrony Danych.
2. W przypadku planowanego utworzenia nowego zbioru (kategorii osób) lub zmian w zakresie czynności dla istniejącego zbioru kierownik jednostki tworzącej lub modyfikującej zbiór jest przed utworzeniem zbioru lub wprowadzeniem zmian zobowiązany do przekazania Inspektorowi Ochrony Danych wszelkich informacji niezbędnych do rejestracji zbioru lub modyfikacji informacji na temat zbioru w rejestrze czynności przetwarzania.
3. W przypadku planowanego przyjęcia powierzenia przetwarzania kierownik jednostki przyjmującej powierzenie jest przed przyjęciem powierzenia

zobowiązany do przekazania Inspektorowi Ochrony Danych wszelkich informacji niezbędnych do rejestracji zbioru w rejestrze kategorii czynności przetwarzania, w tym informacji o podmiocie powierzającym przetwarzanie.
4. W przypadku zakończenia przetwarzania danych w zbiorze lub zakończenia przetwarzania danych na podstawie przyjętego powierzenia przetwarzania danych kierownik jednostki decydujący o zakończeniu przetwarzania danych w zbiorze zobowiązany jest do przekazania Inspektorowi Ochrony Danych informacji o dacie zakończenia przetwarzania.

X. Monitoring wizyjny

§ 21

Celem prowadzenia monitoringu jest:

1. podniesienie stanu bezpieczeństwa studentów, pracowników oraz innych osób przebywających na terenie Uczelni,
2. zapobieganie dewastacjom i kradzieżom na terenie Uczelni,
3. rejestracja zdarzeń mająca na celu ustaleniu sprawcy szkody lub kradzieży i odzyskaniu utraconego mienia.

§ 22

Monitoringiem objęte są:

1. wejścia i wyjścia z budynków,
2. elewacje budynków,
3. ciągi komunikacyjne w budynkach,
4. parkingi oraz bramy wjazdowe,
5. tereny przyległe do nieruchomości uczelni objęte zasięgiem kamer, z zastrzeżeniem, że zakres przestrzeni objętej monitoringiem poza terenem Uczelni jest ograniczony do minimum i wynika wyłącznie z parametrów technicznych urządzeń wykorzystywanych do wideo rejestracji.

§ 23

1. Na system monitoringu składają się:
   - kamery
   - rejestratory z twardymi dyskami i monitorami.
2. Obiekty i tereny objęte systemem monitoringu muszą być oznaczone tablicami lub naklejkami informującymi o monitorowaniu i rejestracji obrazu wraz z podaniem danych Uniwersytetu, innymi informacjami wymaganymi przy realizacji obowiązku informacyjnego oraz znakami graficznymi (piktogramami) informującymi o monitoringu.
3. Powyższe tablice lub naklejki umieszcza się w miejscach widocznych – tak aby można je było łatwo dostrzec.

§ 24

1. Monitoring funkcjonuje całodobowo.
2. Rejestracji i zapisowi danych na nośniku danych podlega tylko obraz (bez dźwięku) pochodzący z kamer systemu monitoringu wizyjnego.
3. Dane pochodzące z nagrań umożliwiające identyfikację osoby, zarejestrowane i przechowywane uważane są za dane osobowe.
4. Okres przechowywania danych z monitoringu jest nie dłuższy niż 3 miesiące od dnia nagrania.

5. Dostęp do danych z monitoringu wizyjnego posiadają Rektor oraz osoby przez niego upoważnione.
6. Udostępnianie danych osobowych związanych z systemem monitoringu wizyjnego odbywa się na zasadach określonych w przepisach prawa oraz przyjętych w niniejszej Polityce bezpieczeństwa (§ 15).

XI. Opis zdarzeń naruszających ochronę danych osobowych oraz zasady postępowania w sytuacji naruszenia ochrony danych osobowych

§ 25

1. Rodzaje zagrożeń naruszających ochronę danych osobowych:

   1) zagrożenia losowe:

      a) zewnętrzne (np. klęski żywiołowe, pożary, zalania, przerwy w zasilaniu energii) – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia (zarówno danych przetwarzanych w formie tradycyjnej papierowej, jak i elektronicznej) lub uszkodzenia infrastruktury technicznej systemu informatycznego, przy czym ciągłość pracy systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych;
      b) wewnętrzne (np. niezamierzone pomyłki użytkowników, administratora, awarie sprzętowe, błędy oprogramowania) – w wyniku ich wystąpienia może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu informatycznego, może nastąpić naruszenie poufności danych;

   2) zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy; w ramach tej kategorii zagrożeń wyróżnia się:
      a) nieuprawniony dostęp do systemu informatycznego z zewnątrz sieci uczelnianej (włamanie do systemu),
      b) nieuprawniony dostęp do systemu informatycznego z wewnątrz sieci uczelnianej,
      c) nieuprawnione przekazanie danych,
      d) bezpośrednie zagrożenie materialnych składników (np. kradzież sprzętu informatycznego zawierającego dane osobowe, kradzież dokumentów).

2. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to w szczególności:

   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej);
   2) niewłaściwe parametry środowiska (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych);
   3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych;
   4) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu informatycznego lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
7) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
8) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń (np. identyfikatora i hasła w systemie informatycznym);
9) praca w systemie informatycznym, wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych (np. dowody na pracę przy komputerze osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu);
10) podmienienie albo zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
11) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub kserokopiarce, wyrzucenie do śmieci dokumentów w formie papierowej niezniszczonych w sposób uniemożliwiający odczytanie danych, niezamknięcie na klucz pomieszczenia, w którym znajduje się komputer, niewykonanie w określonym terminie kopii zapasowych, przetwarzanie danych osobowych w celach prywatnych, itp.)

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych znajdujących się na dyskach, pamięciach zewnętrznych, płytach CD, DVD, taśmach magnetycznych, kartach pamięci itp. oraz wydrukach komputerowych oraz wszelkie stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych (niezabezpieczone pomieszczenia, otwarte szafy, biurka, regały, urządzenia archiwizujące, dokumenty pozostawione w drukarkach, kserokopiarkach, niezniszczone w odpowiedni sposób dokumenty w śmietnikach itp.).

§ 26

1. Każdy pracownik (w szczególności osoba zatrudniona z racji wykonywanych obowiązków przy przetwarzaniu danych osobowych), który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych przetwarzanych w Uniwersytecie zobowiązany jest do niezwłocznego poinformowania o tym swojego przełożonego, a ten do poinformowania administratora systemu informatycznego, jeśli zdarzenie dotyczy systemu informatycznego oraz **Inspektora Ochrony Danych**.
2. Administrator systemu informatycznego, który stwierdził naruszenie lub uzyskał informację wskazującą na naruszenie w systemie ochrony danych osobowych zobowiązany jest do niezwłocznego:

1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,

2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,
4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:

   a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do danych osobie niepowołanej,
   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,
   c) zmianę hasła użytkownika, poprzez którego uzyskano nielegalny dostęp, w celu uniemożliwienia ponownej skutecznej próby uzyskania takiego dostępu,

5) analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną w ten sam sposób.

3. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
4. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić ponowne szkolenie w zakresie ochrony danych osobowych w systemie informatycznym.
5. Jeżeli przyczyną zdarzenia była infekcja wirusem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
6. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.
7. Administrator bazy danych osobowych (np. administrator systemu informatycznego), w której nastąpiło naruszenie ochrony danych osobowych przygotowuje bezpośrednio po zabezpieczeniu systemu i przywróceniu jego normalnej pracy **wstępny raport** o przyczynach, przebiegu i wnioskach ze zdarzenia i niezwłocznie przekazuje Inspektorowi Ochrony Danych.
8. Wymieniony w ust. 7 administrator przygotowuje następnie **szczegółowy raport** o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 7 dni od daty zaistnienia zdarzenia przekazuje Inspektorowi Ochrony Danych.
9. Inspektor Ochrony Danych przeprowadza analizę raportów i stosownie do sytuacji rekomenduje do realizacji odpowiednie działania mające na celu zabezpieczenie przed ponownym wystąpieniem zdarzenia w przyszłości.

XII. Sprawdzenia

§ 27

1. Inspektor Ochrony Danych zawiadamia kierownika jednostki objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem rozpoczęcia sprawdzenia.
2. Inspektor Ochrony Danych ma prawo dostępu w sprawdzanej jednostce do wszelkich dokumentów, urządzeń informatycznych oraz systemów związanych z przetwarzaniem danych osobowych.
3. Po zakończeniu sprawdzenia Inspektor Ochrony Danych przygotowuje sprawozdanie, które przekazywane jest Rektorowi oraz kierownikowi sprawdzanej jednostki.
4. Sprawozdanie jest sporządzane w formie papierowej.
5. Inspektor Ochrony Danych przedstawia w sprawozdaniu stwierdzone w wyniku sprawdzenia uchybienia, wnioski i zalecenia mające służyć usunięciu uchybień oraz termin realizacji zaleceń.
6. Kierownik jednostki ma prawo w ciągu 7 dni od daty dostarczenia sprawozdania nie przyjąć sprawozdania i pisemne zastrzeżenia w sprawie wyników sprawdzenia.
7. Jeśli w ciągu 7 dni kierownik sprawdzanej jednostki nie zgłosi zastrzeżenia, uznaje się, że przyjął sprawozdanie.
8. Rektor decyduje, czy przyjąć do realizacji zalecenia Inspektora Ochrony Danych, czy też uwzględnić zastrzeżenia kierownika jednostki.

XIII. Postanowienia końcowe

§ 28

Polityka bezpieczeństwa przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego wchodzi w życie z dniem 25.05.2018 r.

Załącznik Nr 2
do Zarządzenia Nr 31/2019/2020
Rektora UKW
z dnia 2 stycznia 2020 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI służącymi do przetwarzania danych osobowych w Uniwersytecie Kazimierza Wielkiego

Rozdział 1

Postanowienia ogólne

1. Instrukcja zarządzania systemami informatycznymi, zwana dalej „Instrukcją", określa procedury dotyczące zasad pracy i zachowania bezpieczeństwa w systemach informatycznych wykorzystywanych w Uniwersytecie Kazimierza Wielkiego, jak również przetwarzania w nich danych osobowych.
2. Możliwe jest wprowadzanie szczegółowych instrukcji lub polityk bezpieczeństwa dotyczących poszczególnych systemów informatycznych. W takim przypadku zapisy instrukcji (polityk) szczegółowych są nadrzędne w stosunku do zapisów niniejszej instrukcji, jednak nie mogą one ustanawiać niższego poziomu zabezpieczeń, niż niniejsza instrukcja jak również nie mogą być z nią sprzeczne.
3. Dokumentację, o której mowa w ust. 2 zatwierdza Inspektor Ochrony Danych.
4. Dla każdego wielostanowiskowego systemu informatycznego musi zostać wyznaczony przynajmniej jeden administrator systemu, posiadający między innymi uprawnienia do tworzenia w systemie kont użytkowników i nadawania im uprawnień.
5. System jednostanowiskowy – w szczególnych przypadkach administratorem systemu informatycznego może być osoba odpowiedzialna za funkcjonowanie aplikacji przetwarzających dane osobowe na pojedynczym komputerze (np. obsługującym komunikację z bankiem)

Rozdział 2

Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. Przed dopuszczeniem do pracy w systemach informatycznych oraz do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez przełożonego, administratora systemu oraz Inspektora Ochrony Danych z zasadami obowiązującymi podczas pracy w systemach

informatycznych, przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Uniwersytecie wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Rektora lub Prorektorów, Dziekanów, Kanclerza, Dyrektora Biblioteki.
3. Nadanie upoważnienia oraz nadanie osobie uprawnień w systemie informatycznym przetwarzającym dane osobowe następuje na wniosek przełożonego użytkownika.
4. Jeżeli osoba mająca przetwarzać dane osobowe nie jest pracownikiem Uczelni, z wnioskiem o nadanie jej upoważnienia oraz uprawnień w systemie informatycznym występuje kierownik jednostki zlecającej upoważnianej osobie przetwarzanie danych osobowych.
5. Po udzieleniu upoważnienia do przetwarzania danych osobowych, administrator systemu informatycznego nadaje użytkownikowi uprawnienia do systemu.
6. Jeżeli dane osobowe przetwarzane są systemie jednostanowiskowym, identyfikator i hasło dostępu do danych ustala użytkownik.
7. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na wprowadzeniu do systemu przez jego administratora dla użytkownika unikatowego identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji, przy czym o brzmieniu identyfikatora administrator systemu informuje osobę nadającą upoważnienie do przetwarzania danych osobowych lub Inspektora Ochrony Danych, jeśli osobą nadającą upoważnienie jest Rektor.
8. Za przydzielenie identyfikatora i wygenerowanie hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator systemu. Późniejsze cykliczne zmiany hasła, jeśli są wymagane w danym systemie, muszą być wymuszane poprzez mechanizmy zawarte w systemie informatycznym lub poprzez działanie administratora systemu.
9. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego (zamknięciu dostępu do systemu), nie może być przydzielany innej osobie. W przypadku wyrejestrowania użytkownika z systemu, administrator systemu pozostawia w systemie identyfikator i zmienia hasło dostępu dla identyfikatora.
10. Wyrejestrowania użytkownika z wielostanowiskowego systemu informatycznego (pozbawienia dostępu do systemu) dokonuje, na wniosek Inspektora Ochrony Danych lub przełożonego użytkownika, administrator systemu informatycznego.

Rozdział 3

Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownik uzyskuje dostęp do wielostanowiskowego systemu informatycznego, w którym przetwarzane są dane osobowe, wyłącznie poprzez podanie własnego identyfikatora (loginu) i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu jego identyfikatora.
3. Identyfikator składa się z dowolnej liczby znaków, musi być jednak unikatowy w danym systemie i jednoznacznie identyfikować w nim użytkownika.

4. Jeśli system nie umożliwia użytkownikowi przy tworzeniu konta (rejestracji użytkownika) podania hasła, użytkownik otrzymuje od administratora systemu hasło początkowe z chwilą przystąpienia do pracy w systemie informatycznym i jest zobowiązany zmienić je po pierwszym zalogowaniu na sobie tylko znany ciąg znaków.
5. Hasło składa się z co najmniej 8 znaków.
6. Hasło musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. Hasło nie powinno się składać z kombinacji znaków mogących ułatwić jego odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika).
8. Inspektor Ochrony Danych określa dla danego systemu ewentualne dodatkowe wymagania co do stosowanych metod i środków uwierzytelniania użytkownika, na przykład konieczność cyklicznego wymuszania przez system zmiany hasła.
9. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie ważności.
10. Użytkownik nie może udostępniać osobom nieuprawnionym (w tym również innym pracownikom upoważnionym do przetwarzania danych osobowych w danym systemie, z wyłączeniem w szczególnych przypadkach administratorów systemu) swojego identyfikatora oraz hasła.
11. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło oraz powiadomić o tym fakcie administratora systemu (a ten Inspektora Ochrony Danych) lub bezpośrednio Inspektora Ochrony Danych.
12. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym (zwykle administratorzy systemu) posiadają własne konta administracyjne oraz hasła.
13. Komputery, na których przetwarza się (w tym przechowuje) dane osobowe muszą być zabezpieczone przed nieuprawnionym dostępem poprzez ustanowienie hasła w systemie operacyjnym (np. Windows, Linux).

Rozdział 4

Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu informatycznego

1. Użytkownik rozpoczynając pracę w wielostanowiskowym systemie informatycznym loguje się do niego podając swój identyfikator oraz hasło dostępu do systemu.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. Komputer wykorzystywany do przetwarzania danych osobowych musi być wyposażony w wygaszasz ekranu zabezpieczony hasłem. Najpóźniej po 10 minutach braku aktywności użytkownika na komputerze, musi nastąpić automatyczne włączenie wygaszacza ekranu. Za działanie wygaszacza odpowiada użytkownik komputera.
4. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, w których mogą przebywać osoby nieuprawnione, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
5. Przebywanie osób nieuprawnionych w pomieszczeniach, w których przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych.

6. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
7. Przed czasowym opuszczeniem stanowiska pracy użytkownik zobowiązany jest:
   1) wylogować się z sytemu informatycznego lub
   2) wywołać blokowany hasłem wygaszasz ekranu.
8. Kończąc pracę użytkownik zobowiązany jest:
   1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   2) zabezpieczyć stanowisko pracy, w tym przede wszystkim złożyć w szafie lub szufladzie biurka zamykanych na klucz wszelką dokumentację związaną z danymi osobowymi oraz nośniki magnetyczne, optyczne i inne, na których znajdują się dane osobowe.

Rozdział 5

Zabezpieczenia systemów informatycznych, tworzenie kopii zapasowych zbiorów danych osobowych oraz systemów służących do ich przetwarzania

1. Serwery systemów informatycznych (wielostanowiskowych), w których przetwarzane są dane osobowe oraz urządzenia przechowujące te dane muszą być zabezpieczone przy pomocy zasilaczy awaryjnych przed nieprzewidzianymi awariami zasilania.
2. Dane osobowe przetwarzane w systemie informatycznym oraz systemy (aplikacje) przetwarzające dane osobowe podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
3. Za tworzenie kopii zapasowych zbiorów danych osobowych oraz systemów odpowiedzialny jest administrator systemu lub inna osoba przez niego wyznaczona.
4. Kopie zapasowe zbiorów danych oraz systemów należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury odpowiedzialny jest administrator systemu.
5. Częstotliwość procedury sprawdzenia przydatności kopii ustala dla poszczególnych systemów, w uzgodnieniu z administratorem systemu, Inspektor Ochrony Danych.
6. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   1) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest przed i po wprowadzeniu zmian do aplikacji (na przykład instalacji uaktualnień, nowych wersji itp.),
   2) kopia zapasowa danych osobowych przetwarzanych przez aplikację – kopia wykonywana jest co najmniej raz w tygodniu, a w przypadku wprowadzenia znacznych zmian w danych osobowych po dniu roboczym, w którym dokonano zmian; dla poszczególnych systemów Inspektor Ochrony Danych może ustalić inny harmonogram wykonywania kopii,
   3) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu, jeśli przechowywana są odrębnie od systemu lub od bazy danych – kopia wykonywana jest po każdym dniu roboczym, w którym dokonano modyfikacji uprawnień (w tym dopisania nowych użytkowników).

Rozdział 6
Zabezpieczanie komputerów przenośnych oraz zewnętrznych nośników danych

1. Użytkownicy nie mogą wynosić poza obiekty Uniwersytetu urządzeń (w tym również komputerów przenośnych) oraz nośników danych zawierających dane osobowe bez pisemnej zgody Rektora lub Inspektora Ochrony Danych, lub Prorektora, Dziekana, Kanclerza, Dyrektora Biblioteki, jeśli otrzymali pełnomocnictwo Rektora do nadawania upoważnień do przetwarzania danych osobowych.
2. Znajdujące się na komputerach przenośnych oraz na nośnikach zewnętrznych (dyskach zewnętrznych, dyskietkach, pamięciach flash, płytach CD, DVD, taśmach magnetycznych, kartach pamięci itp.) zbiory zawierające dane osobowe muszą być zabezpieczone poprzez ich zaszyfrowanie uniemożliwiające odczyt osobom nieuprawnionym.
3. Za to, by komputery przenośne oraz nośniki zewnętrzne były zaszyfrowane odpowiada ich użytkownik.
4. Instalacji rozwiązań szyfrujących na komputerach przenośnych oraz nośnikach zewnętrznych dokonuje dział odpowiedzialny za informatyzację Uczelni.
5. Zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności użytkownika (osoby upoważnionej do korzystania z komputera).
6. Jeśli komputer przenośny **pozostawiony jest** w miejscu dostępnym dla osób nieuprawnionych, konieczne jest zabezpieczenie dostępu hasłem, na przykład poprzez aktywację wygaszacza ekranu. Dotyczy to przede wszystkim zabezpieczenia komputera przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkoleń itp.
7. Zabronione jest przetwarzanie danych osobowych (praca z danymi) na komputerze przenośnym w miejscach, w których wgląd do zawartości ekranu komputera miałyby osoby postronne..
8. W przypadku kradzieży, zgubienia komputera przenośnego lub naruszenia ochrony zawartych w nim danych osobowych użytkownik zobowiązany jest do niezwłocznego zgłoszenia zdarzenia Inspektorowi Ochrony Danych.

Rozdział 7

Sposób i miejsce przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Kopie zapasowe danych z systemu informatycznego wykonywane na taśmach, płytach CD, DVD, dyskietkach lub innych nośnikach danych przechowuje się w innych pomieszczeniach i o ile to możliwe w innych budynkach, niż te, w których przechowywane są zbiory danych wykorzystywane do bieżącej pracy. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników danych z kopiami zapasowymi danych osobowych przetwarzanych w systemach informatycznych mają wyłącznie administrator systemu (lub osoba wyznaczona przez niego do wykonywania kopii zapasowych) oraz Inspektor Ochrony Danych.
3. Za zniszczenie kopii zapasowych sporządzanych indywidualnie (lokalnie) przez użytkownika systemu odpowiada użytkownik.
4. Kopie takie należy niszczyć niezwłocznie po ustaniu ich przydatności.

5. Przeznaczone do likwidacji nośniki danych zawierające dane osobowe, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie, to jest trwale i nieodwracalnie niszczy fizycznie do stanu uniemożliwiającego rekonstrukcję nośnika i odzyskanie danych.
6. Likwidację takich nośników nadzoruje uczelniana komisja likwidacyjna, w skład której wchodzi pracownik działu odpowiedzialnego za informatyzację Uczelni.
7. Nośniki danych zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania tych danych osobowych pozbawia się wcześniej zapisu danych osobowych w sposób uniemożliwiający ich odczytanie.
8. Nośniki danych zawierające dane osobowe, przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych i informacji w sposób uniemożliwiający ich odzyskanie albo naprawia pod nadzorem osoby do tego upoważnionej przez Inspektora Ochrony Danych lub administratora systemu informatycznego.

Rozdział 8

Sposób zabezpieczenia systemu informatycznego przed działaniem złośliwego oprogramowania

1. Za **ochronę systemu informatycznego** (w tym jednostanowiskowego) przed złośliwym oprogramowaniem (przed wirusami komputerowymi, końmi trojańskimi, robakami komputerowymi, oprogramowaniem szpiegującym, wykradajacym dane lub hasła dostępu itp.) odpowiada administrator systemu.
2. Na każdym komputerze, na którym przetwarzane są dane osobowe musi być zainstalowane oprogramowanie chroniące komputer przed złośliwym oprogramowaniem (program antywirusowy).
3. Za działanie programu antywirusowego na komputerze, na którym przetwarzane są dane osobowe odpowiada użytkownik komputera.
4. Program antywirusowy musi być aktywny przez cały czas pracy komputera, na którym przetwarzane są dane osobowe.
5. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie przez użytkownika oprogramowania zabezpieczającego komputer przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem z zewnątrz (skaner, program antywirusowy, firewall itp.).
6. W przypadku stwierdzenia na komputerze złośliwego oprogramowania, użytkownik zobowiązany jest do zaprzestania wykonywania jakichkolwiek czynności w komputerze i niezwłocznego powiadomienia o stwierdzeniu złośliwego oprogramowania administratora systemu (jeśli dotyczy) lub Inspektora Ochrony Danych.
7. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych” nadawców.

Rozdział 9

Wykonywanie przeglądów i konserwacji systemów oraz nośników danych służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego lub komputera, na którym przetwarzane są dane osobowe wykonywane są wyłącznie przez pracowników działu odpowiedzialnego za

informatyzację Uczelni lub przez osoby wyznaczone przez kierownika działu odpowiedzialnego za informatyzację Uczelni.
2. Administrator systemu okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z Inspektorem Ochrony Danych.
3. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator systemu.
4. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są usuwane przez pracowników działu odpowiedzialnego za informatyzację Uczelni, a ich przyczyny analizowane w celu uniknięcia podobnych zdarzeń w przyszłości.

Rozdział 10

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy pracownik (w szczególności osoba, która z racji wykonywanych obowiązków zatrudniona przy przetwarzaniu danych osobowych w systemie informatycznym), jeżeli stwierdzi lub podejrzewa naruszenie ochrony danych osobowych przetwarzanych w Uniwersytecie zobowiązany jest do niezwłocznego poinformowania o tym swojego przełożonego, a ten do poinformowania administratora systemu informatycznego, jeśli zdarzenie dotyczy systemu informatycznego oraz Inspektora Ochrony Danych Uniwersytetu.
2. Administrator systemu informatycznego, który stwierdził lub uzyskał informację wskazującą na naruszenie w systemie ochrony danych osobowych zobowiązany jest do niezwłocznego:

    1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
    2) jeżeli właściwości systemu na to pozwalają, wygenerowania i wydrukowania dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia oraz opatrzenia ich datą i podpisania,
    3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby nieuprawnionej do danych itp.,
    4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:

        a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
        b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,
        c) zmianę hasła użytkownika, poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu,

    5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
    6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii zapasowej z zachowaniem wszelkich środków ostrożności mających na celu

uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną w ten sam sposób.

3. Po przywróceniu normalnego stanu bazy danych osobowych administrator systemu musi przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
4. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić ponowne szkolenie w zakresie ochrony danych osobowych w systemie informatycznym. Za zorganizowanie szkolenia odpowiada przełożony (zwierzchnik) użytkownika.
5. Jeżeli przyczyną zdarzenia była infekcja złośliwym oprogramowaniem, administrator systemu musi ustalić źródło pochodzenia tego oprogramowania oraz wdrożyć zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.