Załącznik nr 1 do Zarządzenia nr R021.1.34.2026
Rektora UJD w Częstochowie z dnia 16 marca 2026 r.
w sprawie wprowadzenia wersji 2 dokumentacji bezpieczeństwa informacji: Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym w Uniwersytecie Jana Długosza w Częstochowie

POLITYKA BEZPIECZEŃSTWA

w

Uniwersytecie Jana Długosza w Częstochowie

Dokument do użytku wewnętrznego

marzec 2026 r.

Wersja 02

SPIS TREŚCI

WSTĘP

Tworzy się niniejszą dokumentację bezpieczeństwa informacji celem zapewnienia funkcjonowania systemu zarządzania bezpieczeństwem informacji w jednostce, w tym realizacji obowiązków wynikających z powszechnie obowiązującego prawa, tj. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz.U.2019 poz. 1781), rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773), ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz.1077), dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (Dz.U.UE.L.2022.333.80), a polegających na wdrożeniu przez administratora danych dokumentacji bezpieczeństwa informacji.

Celem wdrożenia niniejszej dokumentacji jest zapewnienie należytej ochrony informacji, w tym danych osobowych będących w zasobach administratora danych, w szczególności odpowiedniej do zagrożeń i kategorii danych objętych ochroną.

Poprzez bezpieczeństwo informacji, w tym danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.

Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszelkie informacje, w tym zbiory danych osobowych przetwarzane przez administratora danych, zarówno w sposób zautomatyzowany jak i niezautomatyzowany oraz dane osobowe przetwarzane poza zbiorami danych.

Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby, przy pomocy których administrator danych wykonuje swoje czynności, mające dostęp do danych.

DEFINICJE

§1

Użyte w niniejszej dokumentacji bezpieczeństwa informacji definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą dokumentacją oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez administratora danych w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych. Ilekroć w niniejszej Polityce bezpieczeństwa jest mowa o:

1. Administratorze danych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji przez administratora danych rozumie się Uniwersytet Jana Długosza w Częstochowie reprezentowany przez rektora, dalej

zwany „administratorem”. W przypadku przetwarzania danych innych niż dane osobowe przez administratora rozumie się kierownika jednostki (rektora) w kontekście ustawy o cyberbezpieczeństwie;

2. Lokalnym administratorze danych osobowych (lub „LADO”) – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, której administrator przekazuje obowiązki wynikające z ogólnego rozporządzenia o ochronie danych. W niniejszej dokumentacji przez Lokalnego administratora danych osobowych rozumie się: dziekanów w zakresie działalności podległych wydziałów, prorektorów w zakresie działalności podległych jednostek, kanclerza w zakresie działalności administracji centralnej i w innych obszarach niepodlegających dziekanom i prorektorom. Podczas nieobecności obowiązki poszczególnych LADO przejmują ich zastępcy;
3. Administratorze systemów informatycznych (lub „ASI”) – rozumie się przez to osobę wyznaczoną przez administratora, która odpowiada za zapewnianie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby przetwarzanie w systemach informatycznych odbywało się zgodnie z obowiązującymi przepisami prawa, w tym ogólnym rozporządzeniem o ochronie danych. Podczas nieobecności ASI obowiązki przejmuje przełożony osoby pełniącej tę funkcję;
4. Koordynatorze systemów komputerowych (lub „KSK”) – rozumie się przez to informatyka, który odpowiada za zapewnianie sprawności i konserwacji sprzętu komputerowego oraz prawidłowe zabezpieczanie stanowisk komputerowych na poszczególnych wydziałach, w administracji centralnej i jednostkach ogólnouczelnianych. Realizację zadań KSK nadzoruje ASI;
5. Zabezpieczeniu stanowisk komputerowych przeznaczonych do pracy w wewnętrznych systemach uczelni – rozumie się przez to instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ blokada/ odblokowywanie zewnętrznych nośników pamięci/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;
6. Zabezpieczeniu stanowisk komputerowych nieprzeznaczonych do pracy w wewnętrznych systemach uczelni (np. stanowiska komputerowe kadry dydaktycznej) – rozumie się przez to instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;
7. Wewnętrznych systemach uczelni – rozumie się przez to systemy zlokalizowane na serwerach uczelni;
8. Danych osobowych – rozumie się przez to 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;

9. Dokumentacji bezpieczeństwa informacji – rozumie się przez to Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych;
10. Organie nadzorczym – rozumie się przez to prezesa Urzędu Ochrony Danych Osobowych;
11. Identyfikatorze (loginie) użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do pracy w systemie informatycznym;
12. Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od administratora upoważnienie do przetwarzania danych;
13. Przetwarzaniu danych – rozumie się przez to proces przekształcania danych wejściowych w pożądane wyniki w sposób zautomatyzowany lub niezautomatyzowany. Obejmuje to m.in. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych;
14. Przetwarzaniu danych osobowych – rozumie się przez to 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;
15. Pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
16. Profilowaniu – rozumie się przez to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
17. Systemie informacyjnym – rozumie się przez to system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
18. Cyberbezpieczeństwie – rozumie się przez to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
19. Incydencie/ naruszeniu bezpieczeństwa informacji – rozumie się przez to zdarzenie zagrażające bezpieczeństwu informacji, naruszające poufność, integralność lub dostępność danych lub systemów informatycznych. Odnosi się do nagłego i nieoczekiwanego zdarzenia, które może mieć

negatywne skutki dla osób, mienia, danych lub infrastruktury. Incydenty bezpieczeństwa mogą dotyczyć różnych aspektów organizacji, w tym danych osobowych, sprzętu, czy oprogramowania;

20. Incydencie krytycznym – rozumie się przez to incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Ministra Obrony Narodowej (lub „CSIRT MON"), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (lub „CSIRT NASK") lub Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego (lub „CSIRT GOV");
21. Naruszeniu ochrony danych osobowych – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
22. Danych genetycznych – rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
23. Danych biometrycznych – rozumie się przez to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
24. Rozporządzeniu – rozumie się przez to 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) (Dz.U.UE.L.2016.119.1);
25. Ustawie o ochronie danych – rozumie się przez to ustawę o ochronie danych osobowych z dnia 10 maja 2018 r. (tj. Dz.U.2019 poz. 1781);
26. Dyrektywie NIS 2 – rozumie się przez to dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (Dz.U.UE.L.2022.333.80);
27. Rozporządzeniu KRI – rozumie się przez to Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773);
28. Ustawie o cyberbezpieczeństwie – rozumie się przez to ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077);

29. Upoważnieniu – rozumie się przez to upoważnienie nadawane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym upoważnieniu;
30. Użytkowniku uprzywilejowanym – należy przez to rozumieć osobę upoważnioną, posiadającą nadane uprawnienia administrowania danym systemem informatycznym;
31. Użytkowniku systemu – rozumie się przez to osobę upoważnioną, która otrzymała dostęp do danego systemu informatycznego w postaci loginu i hasła;
32. Zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
33. Bezpośrednim przełożonym - rozumie się przez to: rektora, prorektorów, kanclerza, zastępcę kanclerza, kwestora, zastępcę kwestora, dziekanów, dyrektorów Instytutów, kierowników katedr, kierowników zakładów, dyrektorów jednostek ogólnouczelnianych, redaktora naczelnego wydawnictwa, kierowników jednostek administracyjnych (działów, biur, zespołów, administracji wydziału, domu studenta), administratorów obiektów, kierownika kancelarii ogólnej.

POSTANOWIENIA OGÓLNE

§2

1. W celu zapewnienia bezpieczeństwa informacji, w tym ochrony przetwarzanych danych osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej administrator wdraża niniejszą Politykę bezpieczeństwa.
2. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane były:
    a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
    b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; za wyjątkiem dalszego przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych („ograniczenie celu”);
    c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
    d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
    e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i

organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

3. Administrator jest odpowiedzialny za przestrzeganie przepisów punktu 2 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

§3

1. Polityka bezpieczeństwa jest dokumentem wewnętrznym, poufnym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody administratora, z możliwością wyciągnięcia konsekwencji służbowych.

ADMINISTRATOR

§4

1. Administrator wdraża odpowiednie środki techniczne i organizacyjne przy uwzględnieniu obecnego stanu wiedzy technicznej oraz kosztów takiego wdrażania. Podejmując decyzję co do wdrożenia przedmiotowych środków administrator bierze pod uwagę:

   a) charakter przetwarzania;
   b) kontekst przetwarzania;
   c) cele przetwarzania;
   d) ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

2. Administrator dokonuje oceny ryzyka wiążącego się z przetwarzaniem danych. Ocena ta uwzględnia m.in. ryzyko wynikające z:

   a) przypadkowego lub niezgodnego z prawem zniszczenia danych;
   b) przypadkowej lub niezgodnej z prawem utraty danych;
   c) przypadkowej lub niezgodnej z prawem modyfikacji danych;
   d) nieuprawnionego ujawnienia danych;
   e) nieuprawnionego dostępu do danych.

3. Administrator w celu zapewnienia odpowiedniego stopnia bezpieczeństwa przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem danych stosuje m.in. następujące narzędzia:

   a) pseudonimizację i szyfrowanie danych;
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c) zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

4. Administrator zapewnia, by każda osoba działająca z upoważnienia administratora i mająca dostęp do danych przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego prawo. Administrator prowadzi ewidencję osób upoważnionych.
5. Administrator uwzględnia ochronę danych w fazie projektowania, bierze przy tym pod uwagę stan obecnej wiedzy technicznej, koszt wdrożenia danego mechanizmu, a ponadto charakter, zakres, kontekst, i cele przetwarzania, w tym także ryzyko naruszenia praw lub wolności osób fizycznych. Administrator stosuje przy tym takie mechanizmy jak minimalizacja danych czy też ich jak najszybsza pseudonimizacja, przejrzystość co do funkcji i przetwarzania danych osobowych, umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwienie administratorowi tworzenia i doskonalenia zabezpieczeń.
6. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane, bez interwencji danej osoby, nieokreślonej liczbie osób fizycznych.
7. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. Rejestr ma formę elektroniczną. Administrator udostępnia rejestr na żądanie organu nadzorczego. W rejestrze tym zamieszcza się wszystkie następujące informacje:
    a) nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów oraz inspektora ochrony danych;
    b) cele przetwarzania;
    c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
    d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
    e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
    f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
    g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa odpowiadających istniejącemu ryzyku wiążącego się z przetwarzaniem.
8. Administrator na żądanie współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań.
9. Administrator zgłasza naruszenie ochrony danych osobowych organowi nadzorczemu – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenie musi co najmniej:
    a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszych wymogów.

10. Administrator zawiadamia osobę, której dane dotyczą, bez zbędnej zwłoki, o naruszeniu ochrony danych osobowych jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Zawiadomienie to jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 4 pkt 9 lit. b), c) i d). Zawiadomienie to nie jest wymagane, w następujących przypadkach:

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

11. Administrator przeprowadza ocenę skutków planowanych operacji przetwarzania dla ochrony danych jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;

12. Administrator wyznacza inspektora ochrony danych. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań; może być on członkiem personelu administratora lub wykonywać zadania na podstawie umowy o świadczenie usług. Administrator publikuje dane kontaktowe inspektora ochrony danych i zawiadamia o nich organ nadzorczy.

INSPEKTOR OCHRONY DANYCH

§5

1. Administrator zapewnia, aby inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

2. Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
3. Administrator zapewnia, aby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora za wypełnianie swoich zadań.
4. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora.
5. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia.
6. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
7. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator zapewnia, aby takie zadania i obowiązki nie powodowały konfliktu interesów i nie wpływały negatywnie na niezależność inspektora, a zadania związane z ochroną danych mają pierwszeństwo nad innymi zadaniami zawodowymi. Administrator zapewnia inspektorowi ochrony danych wystarczająco dużo czasu na wykonywanie swoich obowiązków, biorąc pod uwagę złożoność i skalę przetwarzania danych.
8. Zadania inspektora ochrony danych:
    a) informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów prawa o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania rozporządzenia, innych przepisów prawa o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania w przypadku, gdy administrator przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych;
    d) współpraca z organem nadzorczym;
    e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, w przypadku gdy ocena skutków pod kątem przetwarzania niosłaby duże zagrożenia dla podmiotu danych, gdyby administrator nie przedsięwziął środków w celu zminimalizowania tego ryzyka, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

LOKALNY ADMINISTRATOR DANYCH OSOBOWYCH

§6

1. Administrator powierza obowiązki wynikające z rozporządzenia oraz ustawy o ochronie danych lokalnym administratorom danych osobowych:
   a) dziekanom – w zakresie działalności podległych wydziałów;
   b) prorektorom – w zakresie działalności podległych jednostek;
   c) kanclerzowi – w zakresie działalności administracji centralnej i w innych obszarach niepodlegających dziekanom i prorektorom.

2. Zadania lokalnych administratorów danych osobowych:
   1) zapewnienie przetwarzania danych osobowych w podległych sobie obszarach zgodnie z przepisami ochrony danych osobowych, w tym rozporządzeniem oraz ustawą o ochronie danych, w szczególności poprzez:
      a) zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w uczelni, a w szczególności zabezpieczenie danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem,
      b) wypełnianie względem osób, których dane są przetwarzane obowiązku informacyjnego, w tym realizowanie praw osób, których dane dotyczą,
      c) zapewnienie, że do przetwarzania dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez administratora oraz przeszkolone z zasad bezpiecznego przetwarzania danych osobowych,
      d) zapewnienie, aby dane przechowywane były przez okres nie dłuższy niż jest to niezbędne do celów, w których są przetwarzane oraz aby były ograniczone do tego, co niezbędne do celów, w których są przetwarzane i dalej nieprzetwarzane w sposób niezgodny z tymi celami,
      e) przeprowadzanie oceny ryzyka związanego z przetwarzaniem danych osobowych oraz oceny skutków dla ochrony danych w przypadku, gdy administrator przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych;
   2) nadzorowanie przestrzegania Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym UJD w podległych obszarach;
   3) zatwierdzanie wniosków o nadanie/ zmianę/ odebranie podległym pracownikom stosownych upoważnień do przetwarzania danych osobowych oraz zdalnych dostępów do systemów informatycznych administratora;
   4) identyfikowanie nowych zbiorów danych osobowych oraz systemów informatycznych do przetwarzania danych osobowych w podległych sobie jednostkach i przekazywanie informacji o nich administratorowi, przed rozpoczęciem przetwarzania;
   5) identyfikowanie nowych czynności przetwarzania i zgłaszanie ich administratorowi przed rozpoczęciem przetwarzania oraz dokonywanie okresowej weryfikacji wykonywanych czynności przetwarzania w podległych obszarach;

6) zgłaszanie incydentów i naruszeń ochrony danych osobowych w podległych sobie obszarach administratorowi;
7) wykonywanie zaleceń inspektora ochrony danych uczelni w zakresie ochrony danych osobowych przetwarzanych w podległych obszarach;

3. Lokalni administratorzy danych osobowych wykonują w podległych sobie obszarach wszystkie zadania i obowiązki administratora danych, z wyłączeniem zawierania umów powierzenia przetwarzania danych.

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH I KOORDYNATOR SYSTEMÓW KOMPUTEROWYCH

§7

1. Administrator wyznacza administratora systemów informatycznych.
2. ASI odpowiada za zapewnianie przestrzegania zasad ochrony danych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych, w szczególności:
   a) realizację procedur nadawania, modyfikacji i odbierania uprawnień oraz przeciwdziałanie dostępowi osób nieupoważnionych do systemów informatycznych służących do przetwarzania danych;
   b) prowadzenia rejestru użytkowników wraz z uprawnieniami do systemu;
   c) kontrolę funkcjonowania mechanizmów uwierzytelniania użytkowników;
   d) realizację procedur tworzenia kopii zapasowych zbiorów danych oraz systemu informatycznego używanego do ich przetwarzania oraz testowych sprawdzeń odtworzenia z kopii;
   e) zapewnianie nadzoru nad naprawami i likwidacją sprzętu komputerowego oraz elektronicznych nośników informacji, na których zapisane są dane;
   f) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych przetwarzanych w systemie informatycznym, identyfikowanie zagrożeń o charakterze wewnętrznym i zewnętrznym;
   g) regularne, raz w roku, dokonywanie oceny ryzyka dla bezpieczeństwa danych w systemach informatycznych oraz proponowanie administratorowi zabezpieczeń adekwatnych do oszacowanego ryzyka.
3. ASI odpowiada za zapewnianie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane spełniały wymagania nałożone przepisami powszechnie obowiązującego prawa.
4. ASI podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio administratorowi.
5. Informatycy jako koordynatorzy systemów komputerowych są odpowiedzialni za zapewnianie sprawności i konserwacji sprzętu komputerowego oraz prawidłowe zabezpieczanie stanowisk komputerowych na poszczególnych wydziałach, w administracji centralnej i jednostkach ogólnouczelnianych.

6. KSK prawidłowo zabezpiecza stanowiska komputerowe użytkowników:
    a) przeznaczone do pracy w wewnętrznych systemach uczelni poprzez: instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ blokada/ odblokowywanie zewnętrznych nośników pamięci/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu;
    b) nieprzeznaczone do pracy w wewnętrznych systemach uczelni (np. stanowiska komputerowe kadry dydaktycznej) poprzez: instalację wspieranego systemu operacyjnego oraz stworzenie kont z odpowiednimi uprawnieniami (administrator – instalacja/ odinstalowanie oprogramowania/ zdalny dostęp do komputera użytkownika; użytkownik – praca na zainstalowanym oprogramowaniu, brak możliwości ingerencji w konfigurację systemu), zainstalowanie aktualnego oprogramowania antywirusowego, stworzenie zaszyfrowanej przestrzeni dyskowej, konfiguracja systemowego wygaszacza ekranu.
7. KSK prowadzą:
    a) ewidencję przenośnych nośników informacji wraz z wyszczególnieniem użytkownika;
    b) spis wraz ze specyfikacją (na wzorze stanowiącym załącznik nr 4 „Kartoteka komputera” do Instrukcji zarządzania systemem informatycznym) posiadanego pod opieką sprzętu komputerowego oraz oprogramowania z wyszczególnieniem użytkownika.

PRZETWARZANIE DANYCH
§8

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
    a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
    b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
    c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
    d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
    e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Podstawa przetwarzania, o którym mowa w pkt 1 lit. c) i e), musi być określona:

a) w prawie Unii; lub
b) w prawie krajowym.

Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w pkt 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

2. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Jeżeli osoba, której dane dotyczą, wyrazi zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy. Zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, gdy istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele.
3. Zabrania się przetwarzania danych osobowych szczególnych kategorii ujawniających:

   a) pochodzenie rasowe lub etniczne,
   b) poglądy polityczne,
   c) przekonania religijne lub światopoglądowe,
   d) przynależność do związków zawodowych,
   e) danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej,
   f) danych dotyczących zdrowia,
   g) danych dotyczących seksualności lub orientacji seksualnej,

   chyba że:

   a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych,
   b) jest to niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
   c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osób, których dane dotyczą, lub innej osoby fizycznej, która jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
   d) przetwarzania dokonuje się wyłącznie w stosunku do członków organizacji (fundacja, stowarzyszenia lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych,

religijnych lub związkowych) oraz osób utrzymujących z nimi stałe kontakty, pod warunkiem zachowania odpowiednich zabezpieczeń przetwarzanych danych,

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,
h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa krajowego,
i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych,
j) lub jest to niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii lub prawa krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

§9

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

PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

§10

1. Administrator w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem:

a) dostępu do danych osobowych jej dotyczących,
b) sprostowania nieprawidłowych danych,
c) usunięcia danych (prawo do bycia zapomnianym),
d) ograniczenia przetwarzania,
e) przeniesienia danych,

f) dotyczącym prawa do sprzeciwu wobec przetwarzania dotyczących jej danych osobowych,
g) dotyczącym prawa do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu

lub o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

2. W razie potrzeby termin udzielenia informacji można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
3. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
4. Informacji udziela się po skutecznym potwierdzeniu tożsamości osoby, której dane dotyczą. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
5. Informacje, komunikacja i działania są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:
   a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
   b) odmówić podjęcia działań w związku z żądaniem.
6. Decyzję o podjęciu lub niepodjęciu działań w związku z żądaniem każdorazowo podejmuje wyłącznie administrator.
7. Informacji o działaniach podjętych w związku z żądaniem lub o powodach niepodjęcia działań, po uzyskaniu decyzji administratora, udziela kierownik jednostki, do której wpłynęło żądanie, w przypadku wątpliwości co do ewentualnej zgodności z prawem planowanych działań, po konsultacji z inspektorem ochrony danych.
8. Sprostowanie danych osobowych przetwarzanych przez administratora, w przypadku gdy stają się one nieprawidłowe (np. nieaktualne) oraz uzupełnienie niekompletnych danych odbywa się na podstawie Formularza sprostowania danych stanowiącego załącznik nr 7 „Formularz sprostowania danych osobowych” do niniejszej Polityki bezpieczeństwa.
9. Pracownicy zobowiązani są do przedkładania do Działu Kadr i Spraw Socjalnych Formularza sprostowania danych osobowych bezzwłocznie, nie później niż w ciągu 7 dni po wystąpieniu zmiany ich danych osobowych.

OBOWIĄZEK INFORMACYJNY
§11

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator jest obowiązany, podczas pozyskiwania danych osobowych, podać jej wszystkie następujące informacje:

   a) swoją tożsamość i dane kontaktowe;
   b) dane kontaktowe inspektora ochrony danych;
   c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
   d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   e) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi rozporządzenia, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
   f) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   g) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących 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;
   h) jeżeli przetwarzanie odbywa się na podstawie zgody lub wyraźnej zgody (w przypadku szczególnych kategorii danych osobowych) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   i) informacje o prawie wniesienia skargi do organu nadzorczego;
   j) informację, 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;
   k) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a w przypadku decyzji opierających się na szczególnych kategoriach danych osobowych (jedynie gdy zachodzi przesłanka wyraźnej zgody lub ważnego interesu publicznego) – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

   Wzór informacji podawanej osobie której dane dotyczą podczas pozyskiwania jej danych osobowych stanowi załącznik nr 1 „Informacja dot. przetwarzania danych osobowych – wzór ogólny" do niniejszej Polityki bezpieczeństwa.

2. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w pkt 1 lit. f)-k).

3. Pkt 1 i 2 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

§12

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, zakres informacji wskazany w § 11 pkt 1, z wyjątkiem informacji z pkt j) oraz dodatkowo wskazuje źródło pochodzenia danych osobowych, a gdy ma to zastosowanie informuje czy pochodzą one ze źródeł publicznie dostępnych oraz kategorie przetwarzanych danych osobowych.
2. Informacje, o których mowa w pkt 1, administrator podaje:
   a) najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
   b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
   c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w §11 pkt 1 lit. f)-i), k) oraz dodatkowo źródło pochodzenia danych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.
4. Pkt. 1–3 nie mają zastosowania, gdy – i w zakresie, w jakim:
   a) osoba, której dane dotyczą, dysponuje już tymi informacjami;
   b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem odpowiednich warunków i zabezpieczeń (np. minimalizacja, pseudonimizacja danych), lub o ile udzielenie takich informacji może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
   c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem; lub
   d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie, w tym ustawowym obowiązkiem zachowania tajemnicy.

UDOSTĘPNIANIE DANYCH OSOBOWYCH

§13

1. Administrator nie udostępnia żadnych danych osobowych będących w jego posiadaniu osobom/ podmiotom, których dane nie dotyczą, bez wykazania przez te osoby/ podmioty właściwej podstawy prawnej udostępnienia. Po wykazaniu podstawy prawnej dane mogą zostać udostępnione jedynie w odpowiedzi na wniosek złożony w formie pisemnej.
2. Dane osobowe mogą być udostępnione na pisemny wniosek organom państwowym lub organom samorządu terytorialnego w związku z prowadzonymi przez te organy postępowaniami.

3. Decyzję o udostępnieniu lub nieudostępnieniu danych osobowych każdorazowo podejmuje wyłącznie administrator.
4. Po uzyskaniu zgody administratora dane do udostępnienia przygotowuje kierownik jednostki, do której wpłynął wniosek.
5. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.

POWIERZENIE PRZETWARZANIA DANYCH
§14

1. Administrator może powierzyć podmiotowi przetwarzającemu, w drodze umowy zawartej na piśmie, przetwarzanie danych. Administrator wybiera wyłącznie podmioty przetwarzające, które zapewniają wystarczające gwarancje, w szczególności jeśli chodzi o wiedzę fachową, wiarygodność i zasoby, wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom przepisów rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania.
2. Podmiot przetwarzający, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie na udokumentowane polecenie administratora, w zakresie i w celu przewidzianym w umowie.
3. Wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 5 „Umowa powierzenia” do Polityki bezpieczeństwa.
4. Decyzję powierzenia przetwarzania danych podmiotowi przetwarzającemu podejmuje wyłącznie administrator.

WERYFIKACJA TOŻSAMOŚCI OSOBY FIZYCZNEJ
§15

1. Zabrania się pobierania od osób fizycznych i zatrzymywania dokumentów tożsamości, takich jak dowód osobisty, paszport lub jakichkolwiek innych urzędowych dokumentów osobistych.
2. W celu dokonania weryfikacji tożsamości osoby dokumenty te są przedstawiane jedynie do wglądu, właściciel dokumentu tożsamości nie może tracić go z oczu.

ZBIORY DANYCH OSOBOWYCH
§16

1. Wykaz zbiorów danych osobowych przetwarzanych przez administratora znajduje się w Katalogu zakresów uprawnień stanowiącym załącznik nr 3 „Katalog zakresów uprawnień” do Instrukcji zarządzania systemem informatycznym.
2. Każdy nowy zidentyfikowany zbiór danych osobowych oraz program do przetwarzania danych osobowych należy bezzwłocznie zgłosić, przed rozpoczęciem przetwarzania w tym zbiorze/ programie administratorowi.

AUDYTY OPERACJI PRZETWARZANIA

§17

1. Inspektor ochrony danych, celem monitorowania zgodnego z prawem przetwarzania danych osobowych nie rzadziej niż raz w roku przeprowadza dla administratora audyt zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdanie w tym zakresie.
2. Inspektor ochrony danych zawiadamia administratora o rozpoczęciu audytu przed podjęciem pierwszej czynności.
3. Inspektor ochrony danych zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 5 dni przed dniem przeprowadzenia czynności.
4. Przy dokonywaniu audytu inspektorowi ochrony danych przysługuje prawo, m.in. do:
   a) utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych,
   b) sporządzenia notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych,
   c) odebrania wyjaśnień osoby, której czynności objęto audytem,
   d) sporządzenia kopii otrzymanego dokumentu,
   e) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych,
   f) sporządzenia kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.
5. Po zakończeniu audytu inspektor ochrony danych przygotowuje sprawozdanie.
6. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.
7. Inspektor ochrony danych przekazuje administratorowi sprawozdanie z audytu - nie później niż w terminie 30 dni od zakończenia sprawdzenia.
8. Zawiadomienia nie przekazuje się jeżeli kierownik jednostki organizacyjnej objętej sprawdzeniem posiada informacje o zakresie planowanych czynności.

KONTROLE OPERACJI PRZETWARZANIA

§18

1. Inspektor ochrony danych, celem monitorowania zgodnego z prawem przetwarzania danych osobowych może przeprowadzać dla administratora kontrole zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych:

a) okresową kontrolę wewnętrzną stanu fizycznego zabezpieczenia dokumentów zawierających dane osobowe,

b) okresową weryfikację stanu zatrudnienia w celu sprawdzenia czy wszystkie osoby przetwarzające dane osobowe mają wydane aktualne upoważnienia do przetwarzania danych osobowych,

c) kontrolę doraźną.

2. Niniejsze kontrole nie wymagają uprzedniego zawiadomienia.
3. Niezwłocznie po zakończeniu niniejszych kontroli inspektor ochrony danych przekazuje administratorowi zawiadomienie o wynikach kontroli.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

§19

1. Administrator obowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona.
2. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą odwołania albo upływu terminu wypowiedzenia, rozwiązania lub wygaśnięcia stosunku pracy, umowy zlecenia, umowy o dzieło lub innej umowy zawartej przez administratora z osobą, której zostało nadane. W przypadku zawierania kolejnych stosunków pracy, umów zlecenia, umów o dzieło lub innych umów z osobą upoważnioną do przetwarzania danych osobowych z zachowaniem ciągłości zatrudnienia, upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia/ rozwiązania/ wygaśnięcia ostatniego stosunku pracy/ umowy zlecenia/ umowy o dzieło/ innej umowy zawartej przez administratora z osobą, której zostało nadane. W przypadku nadawania upoważnień do przetwarzania danych osobowych studentom/ doktorantom upoważnienie wygasa z chwilą utraty statusu studenta/ doktoranta przez osobę której zostało nadane.
3. Osoba upoważniona przez administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez administratora zawiera upoważnienie do nadawania dalszych upoważnień.
4. Wzór upoważnienia do przetwarzania danych stanowi załącznik nr 3 „Upoważnienie i oświadczenie” do niniejszej Polityki bezpieczeństwa.
5. Upoważnienie dla każdej osoby, która będzie dopuszczona do przetwarzania danych osobowych przygotowuje w 2 egzemplarzach Dział Kadr i Spraw Socjalnych na podstawie wniosku bezpośredniego przełożonego tej osoby, zatwierdzonego przez lokalnego administratora danych osobowych. W przypadku osób zatrudnionych na podstawie umowy cywilnoprawnej wniosek przygotowuje osoba upoważniona do zawarcia tej umowy. W przypadku konieczności nadania upoważnień studentom/ doktorantom wniosek przygotowuje prorektor ds. kształcenia i spraw studenckich/ dziekan. Wniosek przekazywany jest do Działu Kadr i Spraw Socjalnych w 1 egzemplarzu.

6. Bezpośredni przełożony/ osoba upoważniona do zawarcia umowy cywilnoprawnej/ prorektor ds. kształcenia i spraw studenckich / dziekan jest odpowiedzialny za zapewnienie przetwarzania danych osobowych w podległych sobie obszarach tylko przez osoby do tego upoważnione.
7. Wzór ww. wniosku stanowi:

   1) załącznik nr 1 „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" do Instrukcji zarządzania systemem informatycznym – w przypadku wnioskowania o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych i tożsamych danych osobowych w formie papierowej;

   2) załącznik nr 2 „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych poza systemami informatycznymi" do niniejszej Polityki bezpieczeństwa – w przypadku wnioskowania o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w formie elektronicznej i papierowej poza systemami informatycznymi (bez konieczności nadawania uprawnień do systemów).
8. Dział Kadr i Spraw Socjalnych, po przygotowaniu upoważnienia do przetwarzania danych osobowych, przekazuje „Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" administratorowi systemu informatycznego do realizacji. Upoważnienie obowiązuje od dnia podpisania przez administratora.
9. ASI po zrealizowaniu „Wniosku o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych w systemach informatycznych" i uzupełnieniu go o nazwy systemów informatycznych, do których użytkownik otrzymał dostęp oraz o nadane identyfikatory przekazuje wniosek do Działu Kadr i Spraw Socjalnych.
10. Upoważnienia wraz z wnioskami przechowywane są w oddzielnych segregatorach w Dziale Kadr i Spraw Socjalnych.
11. Osoba upoważniona otrzymuje jeden egzemplarz upoważnienia po:

    1) odbyciu przez nią wstępnego szkolenia z ochrony danych osobowych celem:

       a) zapoznania z przepisami dotyczącymi ochrony danych osobowych,
       b) zapoznania z niniejszą dokumentacją przetwarzania danych osobowych;

    2) podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy).
12. Fakt odbycia przez pracownika wstępnego szkolenia odnotowywany jest przez inspektora ochrony danych na karcie obiegowej pracownika. W przypadku osób niebędących pracownikami – w systemie e-learningowym na Platformie Moodle lub na dokumencie „Potwierdzenie przeprowadzenia szkolenia" stanowiącym załącznik nr 4 do niniejszej Polityki bezpieczeństwa.
13. Inspektor ochrony danych wspólnie z Działem Kadr i Spraw Socjalnych oraz osobami zawierającymi umowy cywilnoprawne prowadzi okresową (raz na semestr) weryfikację stanu zatrudnienia, o której mowa w § 18 pkt 1 lit. b, w celu sprawdzenia czy wszystkie osoby przetwarzające dane osobowe mają wydane aktualne upoważnienia do przetwarzania danych osobowych.

EWIDENCJA OSÓB UPOWAŻNIONYCH

§20

1. Administrator prowadzi ewidencję osób upoważnionych.
2. Ewidencja osób upoważnionych jest prowadzona i przechowywana w Dziale Kadr i Spraw Socjalnych.
3. Ewidencja może być prowadzona w wersji papierowej lub elektronicznej z możliwością jej wydruku.
4. Ewidencja zawiera:
   1) imię i nazwisko osoby upoważnionej;
   2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
   3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

SZKOLENIA

§21

1. Administrator zapewnia szkolenia wstępne oraz okresowe dla osób upoważnionych do przetwarzania danych osobowych w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych.
2. Szkolenie wstępne jest przeprowadzane w miarę możliwości przed dopuszczeniem osoby upoważnionej do czynności przetwarzania danych oraz przed nadaniem upoważnienia.
3. Przeprowadzenie szkolenia wstępnego dla pracownika jest odnotowywane na karcie obiegowej. W przypadku osób niebędących pracownikami – w systemie e-learningowym na Platformie Moodle lub na dokumencie „Potwierdzenie przeprowadzenia szkolenia" stanowiącym załącznik nr 4 do niniejszej Polityki bezpieczeństwa.
4. Szkolenia okresowe przeprowadzane są corocznie. Odbycie szkolenia odnotowywane jest w systemie e-learningowym na Platformie Moodle lub na dokumencie „Potwierdzenie przeprowadzenia szkolenia" stanowiącym załącznik nr 4 do niniejszej Polityki bezpieczeństwa.
5. Szkolenia prowadzi inspektor ochrony danych lub osoba posiadająca wiadomości z zakresu ochrony danych. Szkolenia mogą się odbywać również w formie e-learningowej.
6. Bezpośredni przełożony/ osoba upoważniona do zawarcia umowy cywilnoprawnej/ prorektor ds. kształcenia i spraw studenckich/ dziekan jest odpowiedzialny za zapewnienie przetwarzania danych osobowych w podległych sobie obszarach tylko przez osoby przeszkolone z zasad ochrony danych osobowych.
7. Administrator stosuje praktyki dotyczące cyberhigieny, takie jak zasady zerowego zaufania, aktualizacje oprogramowania, konfiguracja urządzeń, segmentacja sieci, zarządzanie tożsamością i dostępem lub świadomość użytkowników, organizuje szkolenia dla pracowników oraz szerzy wiedzę na temat cyberzagrożeń, phishingu lub technik inżynierii społecznej w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej. Szkolenia z

cyberbezpieczeństwa mogą być elementem szkoleń wstępnych lub okresowych z zakresu ochrony danych osobowych.

OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

§22

1. Administrator przetwarza dane jedynie w pomieszczeniach do tego przeznaczonych w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.
2. Wykaz budynków tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik nr 6 „Obszar przetwarzania danych" do niniejszej Polityki bezpieczeństwa.

ŚRODKI TECHNICZNE, ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§23

1. Każdy jest zobowiązany zachować w tajemnicy dane, do których posiada dostęp, sposoby zabezpieczania danych jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności. Użytkownik systemu ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego hasła i loginu.
4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe i dane wymagające szczególnej ochrony, przesyłany dokument należy zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.

§24

1. Wszelkie dokumenty zawierające dane osobowe i dane wymagające szczególnej ochrony przechowywane są w szafach lub pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Klucze do pomieszczeń wydawane są wyłącznie osobom do tego uprawnionym. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych. Każdorazowe zdanie i pobranie kluczy zapasowych podlega wpisowi do rejestru, w

którym odnotowuje się datę, godzinę, nazwisko osoby zdającej lub pobierającej klucze oraz potwierdza jej podpisem.

4. Klucze do pomieszczeń, w których znajdują się serwery są przechowywane na portierni i codziennie w momencie rozpoczęcia pracy pobierane przez administratora systemów informatycznych lub przez osoby przez niego upoważnione.
5. Osoba, która utraciła posiadane klucze do pomieszczeń administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność administratorowi na formularzu zgłoszenia. Wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu" do niniejszej Polityki bezpieczeństwa. Administrator dokumentuje wszelkie naruszenia w rejestrze, wzór rejestru stanowi załącznik nr 9 „Rejestr naruszeń bezpieczeństwa informacji" do niniejszej Polityki bezpieczeństwa.
6. Administrator podejmuje wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.
7. Szczegółowy wykaz środków technicznych i organizacyjnych stosowanych przez administratora celem zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zawarty został w załączniku nr 6 „Obszar przetwarzania danych" do niniejszej Polityki bezpieczeństwa.

§25

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach zamykanych na klucz.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia (zaleca się, aby niszczarka spełniała wymogi normy DIN 66399, klasa bezpieczeństwa nie niższa niż 3) lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą administratora lub w obecności osoby upoważnionej.
6. W przypadku przenoszenia dokumentów z danymi, w szczególności danymi osobowymi poza obszar przetwarzania pracownik ponosi pełną odpowiedzialność za odpowiednie zabezpieczenie dokumentów w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.
7. Bezpośredni przełożeni są odpowiedzialni za prowadzenie bieżącego nadzoru nad stosowaniem środków bezpieczeństwa przez podległych im pracowników podczas pracy z danymi.

8. Za bezpieczeństwo danych osobowych i zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w podległych sobie obszarach odpowiadają LADO.
9. Szczegółowy opis środków bezpieczeństwa zastosowanych przez administratora wskazany został w załączniku nr 6 „Obszar przetwarzania danych" do niniejszej Polityki bezpieczeństwa.

POSTĘPOWANIE W RAZIE ZAISTNIENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTU BEZPIECZEŃSTWA INFORMACJI

§26

1. W związku z obowiązkiem zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osoby, której dane dotyczą, o których mowa w § 4 pkt 9 i 10 niniejszej Polityki bezpieczeństwa administrator przyjmuje następującą politykę w zakresie zarządzania incydentami ochrony danych osobowych:
   a) pracownik przekazuje administratorowi pisemną informację o wystąpieniu naruszenia ochrony danych osobowych niezwłocznie, najpóźniej w przeciągu 24 godzin od zaistnienia zdarzenia, wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu" do niniejszej Polityki bezpieczeństwa;
   b) administrator ustala czy nastąpiło naruszenie danych osobowych. Jeśli stwierdzi, że nastąpiło, ocenia ryzyko dla osób fizycznych;
   c) jeśli administrator stwierdzi, że naruszenie może narazić prawa i wolności osób fizycznych na ryzyko, powiadamia organ nadzorczy;
   d) jeśli administrator stwierdzi, że naruszenie może narazić prawa i wolności osób fizycznych na wysokie ryzyko, powiadamia poszkodowane osoby, a w odpowiednich przypadkach przekazuje im informacje o krokach, które mogą podjąć, by chronić się przed konsekwencjami naruszenia;
   e) administrator dokumentuje naruszenie w rejestrze, wzór rejestru stanowi załącznik nr 9 „Rejestr naruszeń bezpieczeństwa informacji" do niniejszej Polityki bezpieczeństwa.
2. Administrator realizując zadanie publiczne zależne od systemu informacyjnego wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
3. Administrator odpowiadając za bezpieczeństwo informacji w systemach informatycznych:
   a) zapewnia zarządzanie incydentem;
   b) zgłasza incydent, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT NASK;
   c) zapewnia obsługę incydentu i incydentu krytycznego we współpracy z CSIRT NASK, przekazując niezbędne dane, w tym dane osobowe;
   d) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;
   e) przekazuje do CSIRT NASK dane osoby, o której mowa w pkt 2, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

4. Postępowanie w przypadku wystąpienia incydentu bezpieczeństwa informacji w systemie informacyjnym:
   a) pracownik przekazuje ASI/ KSK/ pracownikowi odpowiedzialnemu za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa informację pisemną/ ustną/ mailową o wystąpieniu incydentu niezwłocznie po wykryciu zdarzenia;
   b) pracownik odpowiedzialny za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa zgłasza incydent, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT NASK;
   c) użytkownik uprzywilejowany izoluje maszynę/ system od dostępu do sieci Internet/ intranet;
   d) użytkownik uprzywilejowany zabezpiecza wszelkie możliwe dane (logi) dotyczące wystąpienia danego incydentu;
   e) Administrator dokumentuje naruszenie w rejestrze, wzór rejestru stanowi załącznik nr 9 „Rejestr naruszeń bezpieczeństwa informacji" do niniejszej Polityki bezpieczeństwa.

OBOWIĄZKI UCZELNI W ZWIĄZKU Z ZARZĄDZANIEM BEZPIECZEŃSTWEM INFORMACJI

§27

1. Administrator zarządzając bezpieczeństwem informacji zapewnia:
   a) aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
   b) aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację – za bieżące aktualizacje odpowiedzialny jest KSK;
   c) okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmuje działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy – za regularne, raz w roku, dokonywanie oceny ryzyka dla bezpieczeństwa danych w systemach informatycznych oraz proponowanie administratorowi zabezpieczeń adekwatnych do oszacowanego ryzyka odpowiedzialny jest ASI;
   d) stosowne uprawnienia dla osób zaangażowanych w proces przetwarzania informacji, w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, w celu zapewnienie bezpieczeństwa informacji oraz bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób;
   e) szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
      a) zagrożenia bezpieczeństwa informacji,
      b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
      c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
   f) ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
      a) monitorowanie dostępu do informacji,
      b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

g) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
h) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
i) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
j) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
k) odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegający w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,
   f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
l) zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących, zgodnie z procedurą wskazaną w § 26 niniejszej Polityki bezpieczeństwa;
m) okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

POSTANOWIENIA KOŃCOWE

§28

1. Dokumentacja bezpieczeństwa informacji stanowi wewnętrzną regulację administratora i obowiązuje wszystkich pracowników i współpracowników administratora.
2. Dokumentacja bezpieczeństwa informacji jest poufna i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody administratora, z możliwością wyciągnięcia konsekwencji służbowych.
3. Dokumentacja bezpieczeństwa informacji obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u administratora. Wszelkie jej zmiany obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u administratora.

4. Każdy kto przetwarza dane posiadane przez administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej dokumentacji.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
6. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.

WYKAZ ZAŁĄCZNIKÓW:

Załącznik nr 1 *„Informacja dot. przetwarzania danych osobowych – wzór ogólny”*

Załącznik nr 2 *„Wniosek o nadanie/ odebranie upoważnienia do przetwarzania danych osobowych poza systemami informatycznymi”*

Załącznik nr 3 *„Upoważnienie i oświadczenie”*

Załącznik nr 4 *„Potwierdzenie przeprowadzenia szkolenia”*

Załącznik nr 5 *„Umowa powierzenia przetwarzania danych osobowych”*

Załącznik nr 6 *„Obszar przetwarzania danych”*

Załącznik nr 7 *„Formularz sprostowania danych osobowych”*

Załącznik nr 8 *„Zgłoszenie wystąpienia incydentu”*

Załącznik nr 9 *„Rejestr naruszeń bezpieczeństwa informacji”*