Polityka bezpieczeństwa danych osobowych

przyjęta w dniu 24.05.2018

dla:

ITELUS Szymon Prus

wersja 1.0

SPIS TREŚCI

1 INFORMACJE OGÓLNE

Polityka Bezpieczeństwa danych osobowych określa zasady przetwarzania danych osobowych w ITELUS Szymon Prus w celu zapewnienia ich bezpieczeństwa. Bezpieczeństwo danych jest rozumiane jako zapewnienie:

- poufności – dane nie są dostępne dla osób nieupoważnionych;
- dostępności – dane są dostępne i użyteczne na żądanie osób upoważnionych;
- integralności danych i systemów, w których dane są przetwarzane – dane nie są zmienione lub zniszczone w sposób nieautoryzowany.

Politykę stosuje się do wszystkich danych osobowych przetwarzanych w organizacji, niezależnie od formy, zakresu przetwarzania oraz lokalizacji zbioru.

W przedstawionej dokumentacji za Administratora Danych (AD) rozumie się ITELUS Szymon Prus z siedzibą w Gliwicach.

Ochrona danych osobowych przetwarzanych w firmie ITELUS Szymon Prus (zwana dalej AD lub Organizacją) obowiązuje wszystkie osoby (bez względu na zajmowane stanowisko oraz miejsce wykonywania, jak również charakter stosunku pracy), które mają dostęp do danych osobowych zbieranych, przetwarzanych oraz przechowywanych w Organizacji w związku z prowadzoną działalnością. Na potrzeby niniejszej polityki, za pracownika uznaje się wszystkie te osoby (w tym stażystów, praktykantów oraz osoby zatrudnione na umowę zlecenie lub o dzieło).

Osoby mające dostęp do danych osobowych zobowiązane są do stosowania środków określonych w niniejszej polityce, regulacjach wewnętrznych Organizacji, oraz innych aktach prawnych, z którymi pracownik został zapoznany. Środki te mogą wiązać pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

2 PODSTAWA PRAWNA

Podstawą do opracowania niniejszego dokumentu i jego wdrożenia są następujące przepisy prawa:

a) Konstytucja Rzeczypospolitej Polskiej;
b) Rozporządzenie 2016/679 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.

3 TERMINOLOGIA

1) **RODO** - Rozporządzenie 2016/679 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.
2) **Dane osobowe** –wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Za osobę możliwą do zidentyfikowania przyjmuje się osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
3) **Zbiór danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
4) **Przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, organizowanie, przechowywanie, opracowywanie, przeglądanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych.
5) **System informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
7) **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych osoby, która składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
8) **Administrator Danych (AD)** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 4, ust. 7 RODO, decydujący o celach i środkach przetwarzania danych osobowych.
9) **Administrator Systemu Informatycznego (ASI)** – osoba lub dział zajmujący się w szczególności nadzorowaniem pracy serwerów, zarządzaniem kontami użytkowników, konfiguracją komputerów, instalowaniem oprogramowania, dbaniem o bezpieczeństwo systemu i opcjonalnie samych danych, nadzorowanie, wykrywanie i eliminowanie nieprawidłowości, asystowaniem i współpracą z zewnętrznymi

specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych oraz innych zadań wynikających z zaleconych obowiązków.

10) **Inspektor Ochrony Danych (IOD)** - osoba nadzorująca z upoważnienia AD przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
11) **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawniane są dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów publicznych lub podmiotów, w stosunku do których ujawnianie danych osobowych realizowane jest w ramach konkretnego postępowania zgodnie z prawem Unii lub państwa członkowskiego. *[def. RODO]*
12) **Użytkownik systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych zarejestrowaną w systemie informatycznym AD,
13) **Sieć lokalna** – należy przez to rozumieć połączenie systemów informatycznych AD wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
14) **Sieć publiczna** – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późń. zm.),
15) **Użytkownik zdalny** - użytkownik systemu łączący się z sieci rozległej z systemem informatycznym AD znajdującym się w sieci lokalnej, lub pracujący zdalnie na danych poza siedzibą AD,
16) **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. dyskietka, dysk twardy, pendrive.
17) **Program komputerowy** – zbiór instrukcji, które po umieszczeniu na rozpoznawalnym przez maszynę nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tej maszyny powoduje, że osiąga on zdolność do wykonywania danej czynności lub też wykonuje daną czynność.
18) **Serwer** - wyróżniony komputer świadczący usługi na rzecz mających z nim łączność innych komputerów np. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.
19) **Baza danych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane jednostkowych obiektów.
20) **Kopie bezpieczeństwa (zapasowe)** – kopie plików danych lub plików programowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych.
21) **Teletransmisja (przesyłanie) danych** - przesyłanie danych przy pomocy dostępnych łączy.
22) **Plik** – nośnik informacji, ciąg bajtów posiadający swoją nazwę odróżniającą ją od innych plików i parametry: rozmiar, datę powstania lub datę ostatniej modyfikacji itp.
23) **Nośnik komputerowy (wymienny, lub pamięć/nośnik przenośny)** – nośnik służący do zapisu informacji, np. dyskietka, taśma, płyta CD, wymienny dysk twardy, pamięć typu „pen-drive" lub jakakolwiek inna forma pamięci nadająca się do przenoszenia danych (np. pamięć w urządzeniach tj. smartphone).
24) **Szkodliwe oprogramowanie** – (np. tzw. wirus, koń trojański itd.) program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych, program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. fałszywy program „login" kradnie hasło użytkownika).

4 ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

4.1 ADMINISTRATOR DANYCH

Do zadań Administratora Danych (AD), reprezentowanego przez Szymona Prusa – właściciela, należy:

- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności decyzji o wyznaczeniu Inspektora Ochrony Danych (IOD),
- podejmowanie decyzji o celach i środkach przetwarzania, zwłaszcza z uwzględnieniem zmian w obowiązujących przepisach prawa, organizacji AD oraz technik zabezpieczenia danych osobowych;
- podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych;
- wydawanie upoważnień do przetwarzania danych osobowych dla wszystkich osób mających dostęp do danych osobowych przetwarzanych w Organizacji. Upoważnienia wydawane są przez AD lub przez osobę posiadającą pełnomocnictwo AD,
- wdrażanie wewnętrznych procedur i regulacji dotyczących bezpieczeństwa danych;
- regularna ocena ryzyka oraz ocena skutków przetwarzania danych osobowych;
- zapewnienie niezbędnych środków w celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

4.2 INSPEKTOR OCHRONY DANYCH

Do zadań Inspektora Ochrony Danych należy:

- informowanie AD oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz polityk AD w dziedzinie ochrony danych osobowych, w tym przeprowadzanie audytów;
- prowadzenie działań zwiększających świadomość pracowników w dziedzinie ochrony danych osobowych oraz przeprowadzanie szkoleń personelu uczestniczącego w operacjach przetwarzania;
- sprawowanie nadzoru nad procesem udostępniania danych osobowych;
- sprawowanie nadzoru nad dokumentacją przetwarzania danych osobowych;
- prowadzenie rejestru czynności przetwarzania u AD - w wypadku, gdy zaistnieje taki wymóg;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
- przeprowadzanie analizy przypadków stwierdzonych lub podejrzewanych o naruszenie bezpieczeństwa danych osobowych oraz przedstawianie raportu i zaleceń dla AD w tym zakresie;
- współpraca z Organem Nadzorczym i pełnienie funkcji punktu kontaktowego dla tego Organu, zwanego Urzędem Ochrony Danych Osobowych (UODO).

W wypadku niepowołania IOD jego obowiązki pełni AD

4.3 Administrator Systemu Informatycznego

Do zadań Administratora Systemu Informatycznego (ASI) należy realizacja obowiązków przewidzianych w dokumentacji ochrony danych osobowych, w szczególności:

- przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe, w ramach posiadanych uprawnień;
- przydzielenie każdemu użytkownikowi identyfikatora i hasła oraz nadawanie, modyfikacja oraz odbieranie uprawnienia;
- prowadzenie ewidencji użytkowników systemów informatycznych i uprawnień w tych systemach;
- nadzorowanie działania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do systemów służących do przetwarzania danych osobowych;
- podejmowanie działań służących zapewnieniu niezawodności działania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
- prowadzenie rejestru incydentów naruszenia bezpieczeństwa systemu informatycznego i przedstawianie w tym zakresie kwartalnego sprawozdania IOD.

W wypadku niepowołania ASI jego obowiązki pełni AD

4.4 Osoby upoważnione do przetwarzania danych

Do obowiązków wszystkich osób upoważnionych do przetwarzania danych osobowych należy:

- przetwarzanie danych wyłącznie w takim zakresie i w takim celu, jaki wynika bezpośrednio z obowiązków służbowych oraz nadanego upoważnienia do przetwarzania danych osobowych;
- zachowanie poufności i nieujawnianie osobom, stronom trzecim żadnych informacji, z jakimi zapoznały się w związku z pełnionymi obowiązkami służbowymi, w tym danych uwierzytelniających (np. haseł, loginów);
- dbałość o bezpieczeństwo nośników i urządzeń służących do przetwarzania danych zarówno w siedzibie Organizacji jak i poza nią;
- zgłaszanie wszystkich podejrzanych lub faktycznych nieprawidłowości w procesie przetwarzania danych kierownikowi działu;
- postępowanie zgodnie z wewnętrznymi regulacjami dotyczącymi przetwarzania danych osobowych w szczególności dotyczących zabezpieczenia danych i nośników danych osobowych opisanymi w punkcie 9.4 niniejszej Polityki.

5 Przetwarzane dane osobowe

Wykaz przetwarzanych danych osobowych znajduje się w **Rejestrze czynności przetwarzania,** stanowiącym **Załącznik** do niniejszej Polityki.

6 Udostępnianie danych osobowych

AD udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub na podstawie zgody właściciela danych. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej. Wniosek powinien zawierać następujące informacje:

1. Odbiorcę danych - wnioskodawca,
2. Podstawę do uzyskania informacji (zgoda, przepis prawa),
3. Informację dotyczącą właściciela danych,
4. Zakres wymaganych informacji zgodny z uzyskaną zgodą lub przepisem prawa,
5. Cel uzyskania informacji.

Wniosek jest rozpatrywany przez AD lub upoważnionego przez niego pracownika. Osoba, która dokonała udostępnienia zachowuje wniosek i kopię pisma, w którym udostępniła dane do celów prawidłowego wykonania obowiązku informacyjnego wobec właściciela danych oraz do celów dowodowych.

AD może odmówić udostępnienia danych osobowych w następujących przypadkach:

1. Udostępnienie danych osobowych spowodowałoby istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób (z wyłączeniem sytuacji, w której do udostępnienia obliguje AD przepis prawa).
2. Dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania Wnioskodawcy.

7 WYPEŁNIANIE OBOWIĄZKU INFORMACYJNEGO

Każda osoba, której dane zbiera bezpośrednio AD, musi zostać poinformowana w momencie zbierania tych danych o następujących informacjach:

- nazwie i adresie Administratora Danych (AD);
- danych kontaktowych Inspektora Ochrony Danych (IOD);
- celu i podstawie prawnej przetwarzania;
- ewentualnych odbiorcach danych;
- ewentualnym przekazaniu danych do państwa trzeciego;
- okresie w jakim dane będą przetwarzane;
- prawach przysługujących osobie (prawie dostępu do danych, do sprzeciwu i ewentualnego usunięcia oraz przenoszenia danych;
- prawie do wniesienia skargi do organu nadzorczego;
- obowiązku lub dobrowolności podania danych;
- ewentualnym zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu.

W przypadku pozyskania danych nie od osoby, której dane dotyczą, ale z innych źródeł, konieczne jest podanie także źródła pozyskania tych danych. Informacji udziela się przy pierwszym kontakcie z osobą lub w uzasadnionych przypadkach korespondencyjnie.

Informacje podane powyżej powinny znajdować się na wszystkich formularzach, na których zbierane są dane osobowe, zarówno w formie papierowej jak i elektronicznej (np. formularze kontaktowe na stronach internetowych).

Każda osoba, której dane przetwarza AD, ma prawo uzyskać powyższe informacje na żądanie. Odpowiedzi udziela się w terminie 30 dni. AD ma prawo odmówić udzielenia informacji, jeśli nie jest możliwe potwierdzenie tożsamości wnioskodawcy.

Każde zapytanie odnotowywane jest w **Załączniku** do niniejszej Polityki - **Rejestrze udostępnień i realizacji zapytań.**

8 REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ, W TYM PRAWA DO SPRZECIWU, USUNIĘCIA, PRZENOSZENIA LUB UZYSKANIA KOPII DANYCH

Prawa do sprzeciwu wobec przetwarzania danych przysługują każdej osobie. Realizacja prawa może nastąpić na pisemny (w tym elektroniczny) wniosek osoby, który jest rozpatrywany przez Inspektora Ochrony Danych. Rozpatruje on również wnioski o usunięcie, sprostowanie oraz ograniczenie przetwarzania danych. Podczas oceny wniosku należy brać pod uwagę przede wszystkim to, czy:

1. Można ustalić i potwierdzić tożsamość wnioskodawcy;
2. Dane wnioskodawcy są przetwarzane w zasobach Organizacji;
3. Wniosek jest zasadny zgodnie z zapisami art. 16 – 19 RODO.

Jeśli IOD potwierdzi wszystkie powyższe ustalenia, konsultuje możliwość i sposób wykonania wniosku z Kierownikiem działu, w którym przetwarzane są dane, których wniosek dotyczy oraz z ASI. Po ustaleniu sposobu realizacji wniosku, IOD nadzoruje jego wykonanie oraz odpowiedź dla wnioskodawcy.

IOD rejestruje napływające wnioski oraz ewentualnie sposób i czas ich realizacji.

W celu prawidłowej weryfikacji osób wnioskujących o oddzielenie informacji lub o realizację praw osób, Organizacja ma prawo żądać od osoby wnioskującej dodatkowego potwierdzeniu swojej tożsamości. W

przypadku, gdy Organizacja nie może zagwarantować prawidłowej weryfikacji, może zażądać osobistego stawiennictwa w celu realizacji przysługującej jej praw.

W przypadku, gdy osoba wnioskująca wielokrotnie występuje z wnioskiem o udzielenie informacji lub o realizację praw w zakresie niewnoszącym zmian co do sposobu przetwarzania danych, AD informuje osobę wnioskującą o wysokości opłaty za udzielenie tych informacji. Jeżeli kontakt z osobą wnioskującą możliwy jest przy wykorzystaniu kanałów elektronicznych, kontakt z tą osobą może być prowadzony w ten sposób. Każdy wniosek odnotowywany jest w **Rejestrze udostępnień i realizacji zapytań**, który stanowi **Załącznik** do niniejszej Polityki.

9 ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZY PRZETWARZANIU DANYCH

W celu zapewnienia poufności, integralności i rozliczalności przetwarzania danych, AD stosuje środki techniczne i organizacyjne właściwe dla wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, stosownie do wymogów określonych w RODO oraz zgodnie z okresowo sporządzaną analizą ryzyka.

9.1 ZABEZPIECZENIA FIZYCZNE OBSZARU BEZPIECZNEGO

AD stosuje zabezpieczenia pomieszczeń, biur, miejsc i nośników danych, bez względu na ich formę, które chronią przetwarzane dane przed dostępem osób nieupoważnionych. Do pomieszczeń, w których przetwarzane są dane osobowe dostęp mają wyłącznie osoby posiadające upoważnienie od AD.

9.2 ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

Zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych opisane są poniżej:

1. Zarządzanie uprawnieniami i kontroli dostępu

1) W przypadku nowego użytkownika systemu informatycznego zastosowanie mają zasady określone w pkt 9.3. niniejszej Polityki. Po udzieleniu upoważnienia ASI tworzy konto w systemie i nadaje uprawnienia zgodnie z treścią upoważnienia. W wypadku zmiany uprawnień ASI dokonuje zmiany w systemie.

2) Odebranie uprawnień polega na zablokowaniu konta użytkownika we wszystkich systemach, do których użytkownik miał dostęp. Identyfikator osoby nie jest przydzielany ponownie żadnej innej osobie.

3) Dostęp do wszystkich systemów przetwarzających dane osobowe wymaga uwierzytelnienia. Jeśli do uwierzytelnienia wymagane jest hasło, musi się ono składać min. z 8 znaków oraz zawierać małą i dużą literę oraz cyfrę lub znak specjalny. Pierwsze hasło podawane jest użytkownikowi ustnie przez ASI, po pierwszym logowaniu wymagana jest zmiana hasła. **Hasła do systemów są zmieniane okresowo– zmiana ta jest wymuszona systemowo lub inicjowana ręcznie.**

4) Na komputerach przenośnych stosuje się dodatkowe zabezpieczenia w postaci hasła na BIOS oraz szyfrowania dysku twardego.

5) ASI prowadzi cykliczne, nie rzadziej niż raz w roku sprawdzenie poprawności nadanych uprawnień w systemach. Ze sprawdzenia sporządza notatkę, którą przekazuje AD oraz IOD.

6) Po 10 minutach nieaktywności użytkownika w systemie następuje automatyczne wylogowanie. System jest automatycznie blokowany po 10 nieudanych próbach zalogowania się do systemu.

7) Hasła do kont służących do dostępu administracyjnego zapisane są na kartce, zamknięte w zapieczętowanej kopercie oraz przechowywane w bezpiecznym miejscu do wiadomości AD.

2. Zarządzanie aktywami

1) ASI prowadzi aktualny spis oprogramowania i sprzętu służącego do przetwarzania danych osobowych. W przypadku zmian w tym spisie ASI informuje IOD.

2) Każdy pracownik potwierdza otrzymanie oraz zwrot sprzętu i nośników do przetwarzania danych osobowych. Za przekazanie i odebranie tych aktywów odpowiedzialny jest ASI.

3) W organizacji użycie pamięci pendrive zezwolone jest dla określonych osób. Osoby te otrzymują służbowe pamięci przenośne i zobowiązane są do stosowania zabezpieczeń kryptograficznych nośników lub danych, zgodnie z instrukcjami otrzymanymi od ASI. ASI prowadzi rejestr osób posiadających służbowa pamięci przenośne.

4) Komputery, laptopy, serwery i inne urządzenia będące nośnikami danych osobowych przekazywane do naprawy pozbawiane są wcześniej dysków. W przypadku niemożliwości wymontowania dysku naprawa odbywa się w siedzibie ADO przy obecności upoważnionego pracownika.

5) Po ustaniu użyteczności wszystkie nośniki pamięci, dyski twarde, pamięci przenośne, płyty, taśmy są fizycznie niszczone lub przekazywane do zniszczenia przez wyspecjalizowane podmioty.

3. Zasady bezpiecznej eksploatacji

Organizacja określiła następujące zasady bezpiecznej eksploatacji infrastruktury teleinformatycznej:

1) Wszystkie stacje robocze wyposażone są w działający stale system antywirusowy. Za aktualność wersji oraz prawidłowość działania systemu antywirusowego odpowiada ASI;

2) Wszystkie działania administratorów oraz określone działania użytkowników są nadzorowane i dokumentowane w postaci logów. Logi systemowe przechowuje się przez okres 2 lat;

3) Instalacja nowego oprogramowania dokonywana jest wyłącznie przez ASI, który nadzoruje legalność oprogramowania, oraz sposób wykorzystania zgodnie z licencją na komputerach należących do organizacji.

4) W celu ochrony danych osobowych przed skutkami awarii stosuje się kopie bezpieczeństwa, zgodnie z poniższą procedurą;

   - Za archiwizację i backup danych odpowiadają Administratorzy Systemów Informatycznych (ASI) Organizacji,
   - Za określenie zasobów podlegających archiwizacji odpowiada właściciel systemu w zakresie wskazania zasobu oraz ASI w zakresie wdrożenia mechanizmów gwarantujących pełne odzyskanie danych i odtworzenie systemu,
   - Backup podlegają wszystkie kluczowe zasoby systemowe, w tym:
     - bazy danych;
     - zasoby plikowe (dokumenty, pliki transferowe,);
     - pliki binarne aplikacji;
     - serwery i serwery wirtualne;
     - ustawienia, konfiguracje systemów;
     - ustawienia i konfiguracje urządzeń sieciowych;
     - logi systemowe i dzienniki zdarzeń;
     - dokumentacja systemowa.
   - Backup nie podlegają:
     - lokalne pliki poczty elektronicznej;
     - lokalne bazy danych;
     - pliki zlokalizowane na komputerach użytkowników (np. pulpit, „moje dokumenty”);
     - nośniki wymienne;
     - urządzenia przenośne.
   - Kopie zapasowe przekazywane lub transmitowane poza obszar bezpieczny są zabezpieczane środkami kryptograficznymi,
   - Wszędzie gdzie to możliwe stosuje się kontrolę CRC wykonanych kopii,
   - Błędne, lub nieaktualne kopie zapasowa należy niszczyć zgodnie z ustalonymi zasadami.
   - Kopie zapasowe podlegają weryfikacji i regularnym testom,
   - Testy kopii mogą polegać na próbie odtworzenia lub przeglądu struktury kopii,
   - Testy wykonuje się nie rzadziej niż:
     - raz na pół roku dla określonego zasobu,
     - wszystkie zasoby muszą zostać sprawdzone nie rzadziej niż raz na dwa lata.
   - O wynikach testowania kopii zostaje poinformowany właściciel zasobu oraz ASI, na podstawie notatki wykonanej przez pracownika odpowiedzialnego za wykonanie testu.
   - Wyniki testowania kopii podlegają kontroli i audytom w ramach przeglądów systemu zarządzania.

4. Zachowanie bezpieczeństwa komunikacji

1) Dostęp do Internetu jest możliwy dla pracowników poprzez sieć LAN oraz sieć Wi-Fi. Dostęp do sieci jest ograniczony za pomocą mechanizmów uwierzytelniania;

2) W Organizacji nie ma wydzielonej odrębnej sieci Wi-Fi przeznaczonej dla Gości – Goście korzystają z własnych połączeń sieciowych i nie otrzymują dostępu do sieci Organizacji.

3) Na styku z siecią zewnętrzną zainstalowany jest router brzegowy. ASI odpowiada za właściwą konfigurację reguł przepływu na styku oraz wewnątrz sieci;

4) Dostęp do sieci z zewnątrz ograniczony jest do uprawnionych osób i podmiotów. ASI prowadzi rejestr podmiotów posiadających dostęp zdalny do zasobów, oraz odpowiada za bezpieczeństwo tej komunikacji;

5) Korespondencja elektroniczna może być prowadzona wyłącznie ze służbowych skrzynek pocztowych. Jeśli zawartość korespondencji obejmuje dane osobowe, użytkownik zobowiązany jest umieścić te dane w załączniku do wiadomości oraz go zaszyfrować. Hasło do pliku należy podać inną drogą (smsem, telefonicznie).

4. Zapewnienie ciągłości działania

Administrator Danych (AD), w celu zagwarantowania zdolności do ciągłego zapewnienia poufności, integralności, dostępności, i odporności systemów i usług przetwarzania, wdraża plany ciągłości działania dla wszystkich procesów, systemów i czynności przetwarzania, dla których występuje wysokie ryzyko naruszenia bezpieczeństwa danych zgodnie z przeprowadzoną oceną skutków przetwarzania dla tych danych.

9.3 ZABEZPIECZENIA ORGANIZACYJNE

Zabezpieczenia organizacyjne powinny być realizowane w sposób następujący:

1. Wszystkie osoby posiadające dostęp do danych osobowych, osoby przed podjęciem pracy i okresowo zatrudnione, powinny zostać przeszkolone z zasad przetwarzania danych, wymagań RODO oraz wewnętrznych regulacji Organizacji, tj m.in. poprzez zapoznanie się z niniejszym dokumentem w tym zasadami opisanymi w pkt 9.4. niniejszej Polityki oraz przeprowadzenie szkoleń, m.in. zgodnie z Prezentacją stanowiącą **Załącznik do niniejszej Polityki**
2. Wszystkie osoby posiadające dostęp do danych osobowych posiadają pisemne upoważnienie AD, zobowiązane zostały do zachowania ich w tajemnicy i podpisały stosowne oświadczenie według wzoru stanowiącego **Załącznik** do niniejszej Polityki - **Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniami**, Dokument ten uzupełniany jest w momencie podpisywania umowy o pracę, staż, praktykę, zlecenie, o dzieło lub inną formę współpracy. Za wydanie tych dokumentów odpowiedzialna jest osoba przygotowująca umowę z tą osobą. oraz prowadzona jest ewidencja osób upoważnionych do przetwarzania danych (zawierająca imię i nazwisko osoby upoważnionej oraz datę nadania i ustania, i zakres upoważnienia do przetwarzania danych osobowych) według wzoru stanowiącego **Załącznik** do niniejszej Polityki – **Rejestr osób upoważnionych do przetwarzania danych osobowych.**
3. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały przeszkolone w zakresie zabezpieczeń systemu informatycznego, gdzie za przeszkolenie w zakresie pracy w systemie informatycznym odpowiada ASI.

9.4 ZASADY ZABEZPIECZEŃ DLA PRACOWNIKÓW

1.Monitorowanie pracowników w systemach informatycznych

W związku z zapewnieniem prawidłowego przestrzegania zasad pracy na danych osobowych, Administrator Danych może monitorować działania użytkowników w systemach informatycznych poprzez gromadzenie informacji o:

- fakcie logowania i czasie trwania sesji użytkownika, oraz miejscu i sposobie jej nawiązania;
- dostępie do zasobów i danych oraz sposobie ich wykorzystywania, w szczególności kopiowania i przesyłania poza Organizację;
- sposobie wykorzystywania systemów, wykorzystywanych aplikacji, plików oraz poczty email;
- dostępnie do zasobów sieci publicznej;
- czasie pracy i czasie wykorzystania poszczególnych systemów i aplikacji;
- plikach zgromadzonych na komputerach użytkowników;
- wydrukach.

Monitorowanie nie naraża użytkownika na utratę prywatności (np. w związku z wykorzystywaniem systemów do celów prywatnych) dlatego zabronione jest np:

- wykonywanie okresowych zrzutów ekranu użytkownika;
- podgląd ekranu użytkownika bez jego wiedzy i zgody;
- analiza ruchu sieciowego w celu uzyskania danych użytkownika (np. loginów/haseł).

2.Zasady korzystania z poczty elektronicznej

Organizacja przyjmuje następujące zasady przyznania służbowego konta poczty elektronicznej pracownikowi:

1. Każdemu pracownikowi lub współpracownikowi (ze względu na potrzeby biznesowe) może zostać udostępnione konto pocztowe;
2. Adres konta pocztowego tworzony jest wg stałego wzorca dla wszystkich pracowników (Imię „." Nazwisko @itelus.pl);
3. Założenie konta, w tym schemat zarządzania uprawnieniami i kontroli dostępu, odbywa się zgodnie z Procedurą opisaną w punkcie 9.2. niniejszej Polityki.
4. Konto pocztowe jest aktywne dla użytkownika na czas trwania zatrudnienia.

Zasady korzystania z służbowego konta poczty elektronicznej przez użytkowników są następujące:

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego do wszelkiej korespondencji z innymi pracownikami wewnątrz organizacji, klientami oraz innymi podmiotami w celach komunikacji służbowej,
2. Użytkownik nie może posługiwać się prywatną (spoza domeny) pocztą email w celach służbowych,
3. Użytkownik może posługiwać się pocztą email wyłącznie w celach zgodnych z prawem, przestrzegając między innymi prawa autorskiego, praw własności intelektualnej oraz wszelkich innych przepisów których złamanie mogłoby narazić pracodawcę na straty finansowe, wizerunkowe lub konsekwencje prawne.
4. Użytkownik nie może posługiwać się służbowym adresem email w celach prywatnych oraz rejestrować służbowego adresu poczty elektronicznej w serwisach internetowych niezwiązanych z wykonywaną pracą,
5. Użytkownik może uzyskiwać dostęp do służbowej poczty email za pomocą:
    - klienta pocztowego instalowanego na komputerach służbowych;
    - klienta pocztowego instalowanego na smartfonach służbowych;
    - przeglądarki internetowej, pod udostępnionym przez pracodawcę adresem.
6. W przypadku uzyskiwania dostępu do poczty email spoza siedziby Organizacji użytkownik zobowiązany jest do zachowania szczególnej ostrożności, w szczególności niedozwolone jest logowanie do systemów z:
    - sieci ogólnodostępnych typu hotspot;
    - komputerów ogólnodostępnych np. w hotelach, kawiarniach internetowych;
    - komputerów współużytkowanych przez inne osoby (np. dzieci);
    - komputerów co do których zachodzi podejrzenie że mogły zostać zainfekowane szkodliwym oprogramowaniem.
7. Podczas pracy z systemem pocztowym użytkownik zobowiązany jest do:
    - zapewniania poufności danych uwierzytelniających (loginu i hasła);
    - zapewnienia poufności korespondencji poprzez ograniczenie wglądu do danych osób postronnych;
    - nieotwierania i zapisywania załączników na komputerach niebędących własnością Organizacji.
8. Każda korespondencja wysyłana przez użytkownika musi zawierać:
    - imię i Nazwisko Nadawcy;
    - tytuł wiadomości;
    - zunifikowaną, firmową stopkę zawierającą dane identyfikujące osobę jak i organizację;
    - klauzulę dotyczącą zachowania poufności.
9. Użytkownik ponosi pełną odpowiedzialność za sposób wykorzystywania poczty email, treść przesyłanej korespondencji,
10. Użytkownik przyjmuje do wiadomości, że administrator poczty może uzyskiwać dostęp do przesyłanej poczty email,
11. Wszelkie nieprawidłowości w pracy systemu pocztowego należy zgłaszać Administratorowi Systemu Informatycznego (ASI),
12. Administrator w dowolnym momencie może zablokować użytkownikowi dostęp do konta pocztowego w przypadku
    - wielokrotnych prób błędnego uwierzytelnienia;
    - niestosowania się do zaleceń regulaminu;
    - blokada może być trwała lub obowiązywać do czasu wyjaśnienia nieprawidłowości.
13. W przypadku, gdy użytkownik, niezależnie od nadawcy, **NIE SPODZIEWA SIĘ** otrzymać wiadomości email zawierającej dodatkowe dokumenty w załączniku lub w postaci pliku do pobrania, powinien powstrzymać się od otwarcia takiej wiadomości na czas 48h od czasu jej otrzymania.

3. Korespondencja mailowa

Jeśli przedmiotem korespondencji są jakiekolwiek dane osobowe, które nie mogą być publicznie dostępne, nie należy ich umieszczać w treści wiadomości, a w załączniku do wiadomości, który należy zabezpieczyć hasłem. Hasło należy przekazać inną drogą niż mail (telefonicznie, smsem, osobiście).

3.1.Korespondencja z kontrahentami i podmiotami zewnętrznymi

Nie należy realizować wniosków o udostępnienie danych osobowych, które zostały dostarczone jako wiadomość e-mail, w ten sposób nie należy też udzielać odpowiedzi – udostępnianie wymaga zachowania formy pisemnej.

W przypadku stałej współpracy z kontrahentem, któremu przekazywane są dane osobowe (np. szkolenia bhp, kancelaria prawna, windykacyjna) można te dane przekazać mailem. Danych osobowych nie należy umieszczać w treści wiadomości, a w załączniku do wiadomości, który należy zabezpieczyć hasłem. Hasło należy przekazać inną drogą niż mail (telefonicznie, smsem, osobiście). Ze stałym kontrahentem można umówić się na stałe hasło.

3.2.Wysyłanie wiadomości do wielu odbiorców

W przypadku wysyłania wiadomości do wielu odbiorów, którzy się nie znają (np. w przypadku wysyłania informacji do potencjalnych wykonawców w postępowaniu przetargowym) ich adresy mailowe należy umieścić w polu UDW: lub BCC: (ukryte do wiadomości). Nie używamy w takich wiadomościach pola DO: (TO:).

4. Udzielanie informacji przez telefon

Nie należy udzielać telefonicznie informacji o danych osobowych instytucjom, podmiotom zewnętrznym (np. bankom) oraz osobom trzecim.

5. Zasady ochrony fizycznej

1. Wszystkie dane osobowe w formie papierowej po zakończonej pracy muszą być przechowywane w zamykanych szafkach, klucze do szaf należy zabezpieczyć przed dostępem osób nieupoważnionych.
2. Ekrany monitorów stanowisk dostępu do danych osobowych muszą zostać wyłączone po 10 minutach nieaktywności pracownika. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych muszą zostać ustawione w sposób uniemożliwiający tym osobom wgląd do danych.
3. Po opuszczeniu pomieszczenia przez ostatnią osobę upoważnioną należy zamknąć je na klucz i zabrać klucz ze sobą.
4. Dokumenty zawierające dane osobowe po ustaniu przydatności muszą być niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

6. Praca w systemie informatycznym

Każda osoba posiada swój login i hasło do komputera i jest zobowiązana do tego, aby nie ujawniać haseł innym osobom. Pracownik odpowiada za zachowanie poufności swojego hasła, zatem nieuprawnione jest:

- zapisywanie haseł;
- korzystanie z funkcji zapamiętywania haseł;
- przekazywanie haseł innym osobom.

Jeśli do uwierzytelnienia wymagane jest hasło, musi się ono składać min. z 8 znaków oraz zawierać małą i dużą literę oraz cyfrę lub znak specjalny. Odchodząc od komputera za każdym razem należy się wylogować poprzez naciśnięcie kombinacji klawiszy **Ctrl + Alt + Del** lub **Windows + L**. Po zakończeniu pracy należy wylogować się z wszystkich programów i aplikacji oraz wyłączyć komputer.

7. Zasady korzystania z oprogramowania

Organizacja przyjmuje następujące zasady korzystania z oprogramowania:

1. Pracownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi i nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę / Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich;
2. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną. Pracownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę / Zleceniodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe;
3. Pracownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną;
4. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

8. Zasady korzystania z Internetu

Organizacja przyjmuje następujące zasady korzystania z Internetu:

1. Pracownicy mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych.

2. Przy korzystaniu z Internetu, Pracownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich. Pracownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym Pracodawcy / Zleceniodawcy, ściągać z Internetu jakichkolwiek plików muzycznych lub wideo.
3. W zakresie dozwolonym przepisami prawa, Pracodawca/Zleceniodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Pracownika z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, Pracodawca/Zleceniodawca zastrzega sobie prawo kontroli czasu spędzanego przez Pracownika w Internecie.
4. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

9. Obowiązki pracownika

1. Każdy pracownik zobowiązany jest zachować w poufności dane osobowe, z którymi styka się w związku z pełnieniem obowiązków oraz sposoby ich zabezpieczenia;
2. Pracownik jest zobowiązany przetwarzać dane tylko w zakresie niezbędnym do realizacji zadań służbowych – zgodnie z nadanym upoważnieniem. Zabronione jest np. pozyskiwanie szerszego zakresu danych niż wynika to z wewnętrznych przepisów Organizacji, przekazywanie danych służbowych osobom (także innym pracownikom), które nie posiadają analogicznego upoważnienia;
3. Obowiązkiem pracownika jest informowanie Inspektora Ochrony Danych o dostrzeżonych naruszeniach bezpieczeństwa przetwarzanych danych lub wystąpieniu sytuacji, które mogą do takiego naruszenia doprowadzić;
4. Obowiązkiem pracownika jest zgłaszanie Informatykowi incydentów związanych z naruszeniem bezpieczeństwa, bądź też niewłaściwym funkcjonowaniem systemu informatycznego zgodnie z punktem 10 niniejszej Polityki.

10. Postępowanie w przypadku przyjęcia nowego pracownika

W momencie rozpoczęcia współpracy z nową osobą (pracownikiem, zleceniobiorcą, praktykantem, stażystą) osoba odpowiedzialna za przygotowanie umowy jest zobowiązana przedstawić osobie do podpisu oświadczenie o zachowaniu poufności oraz zadbać o nadanie upoważnienia zgodnie ze wzorem stanowiącym **Załącznik** do niniejszej Polityki**.** Następnie stosuje się zasady opisane w punkcie 9.2.1.ninijeszej Polityki.

11. Przepisy karne

Pracownik Organizacji odpowiedzialny jest za wywiązywanie się z zakresu obowiązków oraz ponosi odpowiedzialność za potencjalne szkody wyrządzone pracodawcy. Pracownik przyjmuje do wiadomości następujące kary (wynikające z przepisów prawa):

- **Art. 266 Kodeksu karnego –** *Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*
- **Art. 267 Kodeksu karnego –** *Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Tej samej karze podlega, kto informację uzyskaną w sposób określony powyżej ujawnia innej osobie.*
- **Art. 268 Kodeksu karnego –** *Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. Kto, dopuszczając się czynu, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
- **Art. 269a Kodeksu karnego –** *Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
- **Art. 269b Kodeksu karnego –** *Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.*

10 INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

W instrukcji przyjęto następujące zasady:

1. Każdy pracownik Organizacji, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować o tym fakcie bezpośredniego przełożonego lub AD.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   - niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   - niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   - nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   - zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   - zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
   - umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia zagrożenia, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:
   - ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
   - inicjuje ewentualne działania dyscyplinarne;
   - rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
   - dokumentuje prowadzone postępowania na druku **„Raport z incydentu”** oraz w **„Rejestrze incydentów”** stanowiącymi **Załączniki** do niniejszej Polityki.
5. W przypadku stwierdzenia incydentu (naruszenia), Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:
   - ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
   - zabezpiecza ewentualne dowody;
   - ustala osoby odpowiedzialne za naruszenie;
   - podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
   - inicjuje działania dyscyplinarne;
   - wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
   - dokumentuje prowadzone postępowania.
6. Jeśli doszło do naruszenia ochrony danych osobowych zgodnie z art. 4 pkt 12 RODO, oraz to naruszenie powoduje ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych zgłasza taki fakt do Organu Nadzorczego w terminie 72 h od powzięcia informacji o naruszeniu.
7. Podmioty, którym Administrator Danych powierzył przetwarzanie danych są zobowiązane, poprzez odpowiednie klauzule w umowach, do zgłoszenia naruszenia powierzonych danych, do którego doszło u tych podmiotów – w terminie 24 h.
8. Punktem kontaktowym w związku z naruszeniem jest Inspektor Ochrony Danych.
9. Jeśli naruszenie powoduje wysokie ryzyko naruszenia praw lub wolności osoby, Administrator Danych bez zbędnej zwłoki zawiadamia tą osobę, lub jeśli jest to niemożliwe – wydaje publiczny komunikat o naruszeniu.
10. **Ewidencja zagrożeń** wraz ze sposobami postępowania stanowi **Załącznik** do niniejszej Polityki.

11 ANALIZA RYZYKA I OCENA SKUTKÓW DLA DANYCH OSOBOWYCH

W oparciu o przepisy art. 35 RODO oraz o wytyczne grupy roboczej Art. 29 przyjęte dnia 4 kwietnia 2017 roku, zmienione 5 października 2017 roku, ADO dokonał oceny kryteriów operacji przetwarzania w jednostce celem dokonania szacowania, czy mogą one powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

W toku dokonanej oceny stwierdzono, że w jednostce nie jest dokonywane:

- ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą”

- automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujące „skutki prawne wobec osoby fizycznej” lub decyzji, które „w podobny sposób istotnie na nią wpływają”

- systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub w ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie”

- dopasowywanie lub łączenie zbiorów danych np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą

- innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu itd.

- proces, w wyniku którego samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy”

Stwierdzono także, że w jednostce nie są przetwarzane dane :

- wrażliwe lub dane o charakterze wysoce osobistym: obejmują szczególne kategorie danych osobowych określone w art. 9 (np. informacje o poglądach politycznych obywateli) oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10

- na dużą skalę:

- dotyczące osób wymagających szczególnej opieki, których dane dotyczą

Mając na uwadze powyższe oszacowano, że nie jest prawdopodobne, aby operacje przetwarzania danych w jednostce mogły powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

Administrator Danych jest zobowiązywany do bieżącej, regularnej oceny ww. i innych kryteriów operacji przetwarzania w jednostce celem dokonania szacowania, czy okoliczności uległy zmianie i czy mogą one powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

12 POWIERZENIE PRZETWARZANIA

Administrator Danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej. Podmiot, któremu AD powierzył dane, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych oraz jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie, w jakim reguluje to zawarta umowa.

Zapisy w umowie z podmiotem, któremu powierzono przetwarzanie danych musi zawierać zapisy gwarantujące, co najmniej, że podmiot ten:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora Danych;
- nie będzie podzlecał czynności jakie wykonuje dla Administratora Danych bez jego pisemnej zgody;
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych po jego stronie zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- wspomaga Administratora Danych w wykonywaniu obowiązku informacyjnego;
- zabezpiecza powierzone dane osobowe w sposób adekwatny do zagrożeń, w tym zgodnie z instrukcjami przekazanymi przez Administratora Danych;
- zabezpiecza, zwraca lub niszczy dane i nośniki po ustaniu świadczenia usług – zależnie od wzajemnych ustaleń;
- umożliwia Administratorowi Danych przeprowadzenie kontroli zgodności przetwarzania danych z umową.

W każdym przypadku, kiedy AD lub IOD uzna to za konieczne, można dokonać oceny podwykonawcy w celu weryfikacji spełnienia obowiązków wynikających z RODO oraz należytego wykonania zobowiązań. Ocenę podwykonawcy można wykonać poprzez:

- żądanie wyjaśnień i przedstawienia dowodów realizacji wymagań RODO;
- autoocenę podwykonawcy w oparciu o ankiety przygotowane przez AD;
- audyt drugiej strony, wykonany przez IOD oraz osoby wskazane przez AD.

Ankieta oceny podwykonawcy stanowi **Załącznik** do niniejszej Polityki.

Administrator Danych prowadzi rejestr podmiotów, którym powierzono przetwarzanie danych na wzorze, który stanowi **Załącznik** do niniejszej Polityki – **Rejestr podmiotów przetwarzających**.

13 ZAŁĄCZNIKI

– Rejestr czynności przetwarzania
– Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniami
– Rejestr osób upoważnionych do przetwarzania danych osobowych
– Rejestr podmiotów przetwarzających
– Raport z incydentu
– Rejestr incydentów
– Ewidencja zagrożeń
– Rejestr udostępnień i realizacji zapytań
– Ankieta Oceny Podwykonawcy
– Prezentacja szkoleniowa z zakresu Ochrony Danych Osobowych