# POLITYKA BEZPIECZEŃSTWA INFORMACJI

w

**Przewóz Osób i Towarów Duńczyk Tomasz Polesiński**

[nazwa firmy]

07.05.2018 r.
[data sporządzenia]

Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).
Defnicje:
1. Administrator Danych: Tomasz Polesiński
2. Dane osobowe – wszelkie informacje dotyczące zidentyfkowanej lub możliwej do zidentyfkowania osoby fzycznej
3. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych
4. Użytkownik – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych
5. Zbiór danych – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów
6. Przetwarzanie danych – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych
7. Identyfkator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfkujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
8. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie
9. Uwierzytelnianie – działanie, którego celem jest weryfkacja deklarowanej tożsamości podmiotu (Użytkownika).

## I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w

. . . . . [nazwa firmy],
niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać

nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
c) monitorowanie zastosowanych środków ochrony.
5. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
6. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

## II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 1 do niniejszej polityki.

## III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych

w . . . . . [nazwa firmy].

2. Wszystkie dane osobowe w firmie są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
a) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.
b) Dane są przetwarzane są rzetelnie i w sposób przejrzysty.
c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.
e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.
f) Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.
g) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.

h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Administrator danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust 5 pkt d RODO).
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nie uprawnione kopiowanie Danych osobowych;
g) naruszenie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych,
6. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" – wzór Upoważnienia stanowi Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa,
c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w kancelarii w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy" stanowi element „Upoważnienia do przetwarzania danych osobowych".
7. Pracownicy zobowiązani są do:
a) ścisłego przestrzegania zakresu nadanego upoważnienia;
b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabez
pieczenia;
d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
IV. Obszar przetwarzania danych osobowych
1. Obszar, w którym przetwarzane są Dane osobowe na terenie

. . . . . [nazwa firmy],
obejmuje pomieszczenie biurowe zlokalizowane w

. . . . . [adres firmy].
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

## V. Określenie środków technicznych i organizacyjnych

niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych, Środki obejmują:
a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.
b) Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
c) Wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów.
d) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
e) Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci frewall.
f) Ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem.
g) Zabezpieczenie dostępu do urządzeń Kancelarii przy pomocy haseł dostępu.
h) Wykorzystanie szyfrowania danych przy ich transmisji.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fzycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fzycznych, Administrator zgłasza fakt na ruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 3 do niniejszej polityki.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

## VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

## VIII. Przekazywanie danych do państwa trzeciego

1. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wnisek osoby, której dane dotyczą.

## IX. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące
Złączniki:

Załącznik nr 1
Rejestr czynności przetwarzania danych osobowych

Załącznik nr 2
Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 3
Wzór Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe

Załącznik nr 4
Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego

Załącznik 1. Rejestr czynności przetwarzania danych osobowych

Nazwa oraz dane
kontaktowe Administratora Danych .....

Imię i nazwisko lub
nazwa oraz dane kontaktowe .....
Inspektora Ochrony Danych Osobowych

Opis kategorii osób, których
dane dotyczą, .....
oraz kategorii danych osobowych

Cele przetwarzania
danych osobowych .....

Kategorie odbiorców,
którym dane .....
osobowe zostały lub
zostaną ujawnione,
w tym odbiorców w państwach
trzecich .....
lub w organizacjach
międzynarodowych

Informacja o przetwarzaniu
danych osobowych .....
do państwa trzeciego

Planowane terminy
usunięcia poszczególnych .....
kategorii danych

Ogólny opis technicznych
i organizacyjnych .....
środków bezpieczeństwa

Załącznik 2. Wzór upoważnienia do przetwarzania danych osobowych

. . . . . , dn. . . . . r.
[data sporządzenia]

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
nr . . . . . [jeżeli jest nadawany]

Działając w imieniu … . . . . . niniejszym upoważniam:
Panią/Pana
… . . . . . .
Stanowisko … . . . . . .
do przetwarzania danych osobowych w … . . . . . .
. . . . . [nazwa firmy]
w następującym zakresie*:

A. Okres upoważnienia:
- na okres zatrudnienia / współpracy z . . . . . .
do dnia . . . . . włącznie

B. Zakres upoważnienia:
- dane przetwarzane na nośnikach papierowych,
- system informatyczny,
- dane osobowe objęte zbiorem:
a) . . . . . .
b) . . . . . .
c) . . . . . [należy pozostawić właściwe]

* bez ograniczeń, podgląd danych, wprowadzanie danych, opracowywanie danych, zmienianie danych, usuwanie danych, na komputerach przenośnych) [należy pozostawić właściwe]

. . . . . .
[administrator danych]

Załącznik 3. Wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe

. . . . . , dn. . . . . r.
[data sporządzenia]

. . . . . .
imię i nazwisko osoby upoważnionej

. . . . . .
stanowisko

. . . . . .
miejsce pracy

OŚWIADCZENIE

Oświadczam, że – w związku z wykonywaniem przeze mnie prac na rzecz

. . . . . [nazwa firmy]
i upoważnieniem mnie do Przetwarzania danych osobowych – zostałem/łam za poznany/a ze stosownymi przepisami i standardami ochrony danych osobowych, zobowiązuję się do przestrzegania:

- Przepisów o ochronie adwokackiej tajemnicy zawodowej,
- Przepisów o ochronie danych osobowych, w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fzycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
- Polityki Bezpieczeństwa informacji w
. . . . . .
. . . . . [nazwa firmy],
- Instrukcji zarządzania systemem Informatycznym w
. . . . . .
. . . . . [nazwa firmy].

W związku z powyższym zobowiązuję się do:

a. zapewnienia ochrony danych osobowych przetwarzanych w zbiorach administratora, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfkacją lub zniszczeniem,

b. zachowania w tajemnicy, także po zaprzestaniu wykonywania prac, wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarza nia danych osobowych w zbiorach . . . . . .

c. natychmiastowego zgłaszania do Administratora Danych zaobserwowania próby lub faktu naruszenia zabezpieczenia fzycznego pomieszczenia, bez pieczeństwa zbioru/zbiorów lub systemów informatycznych.

. . . . . .
[podpis pracownika/współpracownika]

Załącznik 4. Wzór zgłoszenia incydentu naruszenia ochrony danych osobowych

. . . . . , dn. . . . . r.
[data sporządzenia]

Prezes Urzędu Ochrony Danych Osobowych

. . . . . .

# ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fzycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przeływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora .....

Miejsce i dzień naruszenia .....

Kategoria i przybliżona liczba osób, których dane dotyczą .....

Kategoria i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

.....

Opis charakteru naruszenia ochrony danych

.....

Możliwe konsekwencje naruszenia ochrony danych

.....

Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych.

.....

. . . . . .
podpis osoby uprawnionej do reprezentowania Administratora Danych

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM** w

. . . . . .
[nazwa firmy]

. . . . . .
[data sporządzenia]

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych

. . . . . [nazwa firmy]
przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).
Defnicje:
1. Administrator Danych . . . . . .
. . . . . [nazwa firmy]
2. Dane osobowe – wszelkie informacje, w tym o stanie zdrowia, dotyczące zi dentyfkowanej lub możliwej do zidentyfkowania osoby fzycznej
3. System informatyczny – zespół współpracujących ze sobą urządzeń, progra mów, procedur przetwarzania informacji narzędzi programowych zastosowa nych w celu Przetwarzania danych
4. Użytkownik – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych w . . . . . .
. . . . . [nazwa firmy]
5. Sieć lokalna – połączenie Systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych
6. Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie
7. Przetwarzanie danych – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w Systemach informatycznych
8. Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem
9. Identyfkator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfkujący osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
10. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi)

## I. Procedury nadawania uprawnień do Przetwarzania danych i rejestrowania tych uprawnień w Systemie informatycznym

1. Za bezpieczeństwo Danych osobowych w Systemie informatycznym . . . . . [nazwa systemu] i za właściwy nadzór odpowiedzialny jest Administrator Danych.
2. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych,
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfkator użytkownika.
Z chwilą nadania Identyfkatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfkator i Hasło.
5. Identyfkator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.
6. Identyfkator osoby, która utraciła uprawnienia do dostępu do Danych oso bowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zo stają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

### II. Metody i środki Uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W Systemie informatycznym stosuje się Uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do Uwierzytelnienia Użytkownika na poziomie dostępu do systemu operacyjnego stosuje się Hasło oraz Identyfkator użytkownika.
2. Hasła użytkowników umożliwiające dostęp do Systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.
3. Minimalna długość Hasła przydzielonego Użytkownikowi wynosi . . . . . znaków alfanumerycznych i znaków specjalnych.
4. Zabrania się używania identyfkatora lub Hasła drugiej osoby.
5. Dla każdej osoby, której Dane osobowe są przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:
a) daty pierwszego wprowadzenia danych do systemu,
b) identyfkatora Użytkownika wprowadzającego Dane osobowe do systemu,
c) informacji o odbiorcach, którym Dane osobowe zostały udostępnione.

### III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez Użytkowników systemu

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfkowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfkatora Użytkownika oraz hasła do systemu informatycznego.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowe go należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.
5. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 min braku aktywności).

### IV. Tworzenie kopii zapasowych Zbiorów danych

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach

firmy.
2. Do archiwizacji służy . . . . . .
[opisać, np. „do archiwizowania służą płyty DVD z zapisem danych z systemu”].
3. Wszystkie dane archiwizowane winny być identyfkowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfkator zapisanych w kopii danych.

**V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających Dane osobowe oraz kopii zapasowych**

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fzycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

**VI. Sposób zabezpieczenia Systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania**

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:

| Obszar chroniony | Rodzaj ochrony | Typ | |
|---|---|---|---|
| 1.<br>2.<br>3. | Stacje robocze | System antywirusowy | … |
| Firewall | … | | |
| Szyfrowanie nośników danych | … | | |
| 4.<br>5. | Sieć wewnętrzna | System antywirusowy | … |
| Firewall | … | | |
| 6.<br>7. | Poczta e-mail | Szyfrowanie danych | … |
| System antiwirusowy i antyspamowy | … | | |

2.Użytkowany system jest automatycznie skanowany z częstotliwością ….
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy:
a) uruchomić program antywirusowy i skontrolować użytkowany system,
b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.
Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
a) zakończyć pracę w systemie komputerowym,
b) odłączyć zainfekowany komputer od sieci,
c) powiadomić o zaistniałej sytuacji Administratora Danych lub ABI.
5. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar,

w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

**VII. Poczta elektroniczna**

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing e-mail). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

## VIII. Sposoby realizacji w systemie wymogów dotyczących Przetwarzania danych

(sposób realizacji wymogu zapisania w Systemie informatycznym informacji o odbiorcach danych)

1. Informacje o odbiorcach danych zapisywane są w Systemie informatycznym, z którego nastąpiło udostępnienie.
2. Informacja o odbiorcy danych zapisana jest w Systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

## IX. Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez frmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:

a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych,

b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,

c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,

d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.