

**Roma Investments**

ul. Rejtana 12

62-030 Luboń

tel.: +48 618 139 050

fax: +48 618 102 821

NIP: 777 295 10 93

Regon: 300469443

---

## POLITYKA BEZPIECZEŃSTWA

---

ROMA INVESTMENTS PIĄTKIEWICZ SP. J.

UL. REJTANA 12A

62-030 LUBOŃ

|                                        |                   |
|----------------------------------------|-------------------|
| Data i miejsce sporządzenia dokumentu: | LUBOŃ, 25/05/2018 |
| Ilość stron:                           | 23                |

## SPIS TREŚCI

---

|                                                                                      |  |
|--------------------------------------------------------------------------------------|--|
| 1. Wstęp.....                                                                        |  |
| 1.1 Informacje ogólne.....                                                           |  |
| 1.2 Zakres informacji objętych polityką bezpieczeństwa oraz zakres zastosowania..... |  |
| 1.3 Wyjaśnienie terminów używanych w dokumencie polityki bezpieczeństwa.....         |  |
| 2. Osoby odpowiedzialne za ochronę danych osobowych.....                             |  |
| 2.1 Informacje ogólne.....                                                           |  |
| 3. Zarządzanie ochroną danych osobowych.....                                         |  |
| 3.1 Podstawowe zasady.....                                                           |  |
| 3.2 Procedury postępowania z danymi osobowymi.....                                   |  |
| 3.3 Upoważnienie do przetwarzania danych osobowych.....                              |  |
| 3.4 Ewidencja osób upoważnionych.....                                                |  |
| 3.5 Zachowanie danych osobowych w tajemnicy.....                                     |  |
| 3.6 Zarządzanie usługami zewnętrznymi.....                                           |  |
| 3.7 Bezpieczeństwo fizyczne obszarów przetwarzania.....                              |  |
| 3.8 Ocena ryzyka i przeglądy.....                                                    |  |
| 3.9 Zarządzanie incydentami.....                                                     |  |
| 3.10 Zbiory danych osobowych.....                                                    |  |
| 4. Postanowienia końcowe.....                                                        |  |
| 5. Załączniki.....                                                                   |  |

# WSTĘP

---

## 1.1 INFORMACJE OGÓLNE

---

1. Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w Roma Investments Piątkiewicz Sp. J. przez pracowników i współpracowników, którzy przetwarzają dane osobowe.
2. Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Roma Investments Piątkiewicz Sp. J. rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabránieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
3. Polityka bezpieczeństwa przetwarzania danych osobowych w Roma Investments Piątkiewicz Sp. J., zwana dalej Polityką została wydana w związku z § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz zgodnie z:
  - Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
  - Wytocznymi w zakresie opracowania i wdrożenia polityki bezpieczeństwa - Generalny Inspektor Ochrony Danych Osobowych

## 1.2 ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

---

1. Politykę stosuje się do danych osobowych przetwarzanych w systemie informatycznym, danych osobowych zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
2. W zakresie podmiotowym, Polityka obowiązuje wszystkich pracowników Roma Investments Piątkiewicz Sp.j. oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, osoby zatrudnione na umowę zlecenia, umowę o dzieło lub praktykantów.

## 1.3 WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

---

1. Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:
  - poufności — właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
  - integralności — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
  - rozliczalności — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi. Polityka Bezpieczeństwa posługuje się wieloma specjalistycznymi terminami z zakresu ochrony danych osobowych, które mogą być niewłaściwie rozumiane przez pracowników Administratora Danych – osoby obowiązane do przetwarzanie danych osobowych zgodnie z wymogami ustawowym.

### 2. Poziom bezpieczeństwa przetwarzania danych osobowych

Przy przetwarzaniu danych osobowych należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia, ponieważ urządzenia systemu służącego do przetwarzania danych osobowych połączone są z siecią publiczną.

### 3. Definicje

3.1. Administrator danych – Roma Investments Piątkiewicz Sp.J., podmiot, który decyduje o środkach i celach przetwarzania danych osobowych, zwany dalej Roma Investments Piątkiewicz Sp J.

3.2. Administrator Bezpieczeństwa Informacji –Kierownictwo, odpowiedzialne za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

3.3. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez 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.

3.4. Kierownictwo – Zarząd, organ zarządzający.

3.5. Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora danych lub przez osobę wyznaczoną, uprawnioną do przetwarzania danych osobowych.

3.6. Przetwarzanie danych osobowych - jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

3.7. Rozporządzenie - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

3.8. Ustawa – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

3.9. Zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

3.10. Zbiór nieinformatyczny - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

## **2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH**

---

### **2.1 INFORMACJE OGÓLNE**

---

#### **1. Kierownictwo**

Do obowiązków Kierownictwa należy zrozumienie oraz zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych, jego problematyki oraz wymagań. Do obowiązków należy również:

- podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych;
- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie Administratora Bezpieczeństwa Informacji.
- wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;
- egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych;
- poddawanie przeglądowi skuteczność polityki bezpieczeństwa przetwarzania danych osobowych;
- zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;

- zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
- zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych.

## 2. Administrator Bezpieczeństwa Informacji – w firmie Roma Investments Piątkiewicz Sp. J. Kierownictwo

Do obowiązków Administratora Bezpieczeństwa Informacji, należy nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej. Do obowiązków należy również:

- określenie wymagań bezpieczeństwa przetwarzania danych osobowych;
- nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych;
- prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury);
- analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie oraz przedstawienie Zarządowi zaleceń i rekomendacji dotyczących eliminacji ryzyk ich ponownego wystąpienia.

## 3. Osoby upoważnione do przetwarzania danych

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej. Do obowiązków należy również:

- przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;
- postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;
- zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia;
- ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

- informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do przełożonego, który ma obowiązek poinformować Administratora Bezpieczeństwa Informacji.

### **3. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH**

---

#### **3.1 PODSTAWOWE ZASADY**

---

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych.
2. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
3. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
4. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

#### **3.2 PROCEDURY POSTĘPOWANIA Z DANYMI OSOBOWYMI**

---

1. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
2. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
3. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

#### **3.3 UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH**

---

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy.
2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Kierownictwo.

3. W celu upoważnienia do przetwarzania danych osobowych należy dostarczyć do Administratora Bezpieczeństwa Informacji podpisane oświadczenie, którego wzór stanowi **załącznik nr 1** niniejszej Polityki.

4. Na podstawie otrzymanego oświadczenia Administrator Bezpieczeństwa Informacji upoważnia formalnie wnioskującego do przetwarzania danych osobowych i wydaje upoważnienie sporządzane wg wzoru stanowiącego **załącznik nr 2** niniejszej Polityki.

5. Upoważnienia, o których mowa powyżej przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.

6. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

### 3.4 EWIDENCJA OSÓB UPOWAŻNIONYCH

---

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji i zawiera w szczególności:

- imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych;
- zakres upoważnienia do przetwarzania danych osobowych;
- identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych;
- datę nadania i odebrania uprawnień.

2. Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia dostępu do danych osobowych.

### 3.5 ZACHOWANIE DANYCH OSOBOWYCH W TAJEMNICY

---

1. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

2. Znajomości regulacji wewnętrznych

2.1 Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w Roma Investments Piątkiewicz Sp.J., w

szczegółności Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

### 3.6 ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI

---

#### 1. Bezpieczeństwo usług zewnętrznych

1.1. Należy zapewnić aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w Roma Investments Piątkiewicz Sp. j, wymaganiami umowy oraz wymaganiami prawa.

1.2. Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług.

1.3. Należy zapewnić aby użytkownicy nie będący pracownikami Roma Investments Piątkiewicz Sp. j. stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

#### 2. Powierzenie przetwarzania danych osobowych

2.1. Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.

2.2. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 31 i nast. Ustawy. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39a Ustawy.

2.3. W umowach stanowiących podstawę powierzenia przetwarzania danych albo eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego do przestrzegania niniejszej Polityki oraz zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych.

2.4. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Roma Investments Piątkiewicz Sp.j. za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Roma Investments Piątkiewicz Sp. J. do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

#### 3. Udostępnianie danych osobowych

3.1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.

3.2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.

3.3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.

3.4. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.

3.5. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

#### 4. Monitorowanie i przegląd usług strony trzeciej

Monitorowanie usług strony trzeciej powinno być udokumentowane i powinno zawierać informacje o: poziomie wykonania usługi, incydentach bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych, śladach audytowych, problemach operacyjnych, awariach, błędach i zakłóceniach.

### 3.7 BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

---

#### 1. Obszar przetwarzania

1.1. Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Roma Investments Piątkiewicz Sp. J. prowadzi działalność. Do takich pomieszczeń, zalicza się w szczególności:

- pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
- pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe;
- pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

1.2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.

1.3. Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku drzwi. Nie można wnosić ww. kluczy po zakończeniu pracy poza miejsca przeznaczone do ich przechowywania.

1.4. Wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

1.5. Niepotrzebne wydruki lub inne dokumenty należy niszczyć za pomocą niszczarek.

1.6. Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.

1.7. Szczegółowy wykaz obszarów przetwarzania danych osobowych znajduje się w **załączniku nr 3** niniejszej Polityki.

## 2. Bezpieczeństwo środowiskowe

2.1. Lokalizację i umiejscowienie danych osobowych należy starannie dobierać z uwzględnieniem wymaganych aspektów bezpieczeństwa przetwarzania danych osobowych. W szczególności należy rozważyć aspekty dotyczące:

- zasilania energią elektryczną;
- klimatyzacji oraz wentylacji;
- wykrywania oraz ochrony przed pożarem i powodzią;
- fizycznej kontroli dostępu.

2.2. Pomieszczenia wchodzące w skład obszaru przetwarzania danych osobowych należy wyposażyć w odpowiednie środki ochrony fizycznej i organizacyjnej chroniące przed nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami pracy.

2.3. Kopie zapasowe zawierające dane osobowe należy przechowywać w drugiej fizycznej lokalizacji w bezpiecznej odległości od lokalizacji podstawowej.

## 3. Bezpieczeństwo urządzeń

3.1. Urządzenia służące do przetwarzania danych osobowych należy przechowywać w bezpieczny i nadzorowany sposób.

3.2. Urządzenia mobilne takie jak np. komputery przenośne, urządzenia PDA, telefony komórkowe nie powinny być pozostawiane bez opieki jeżeli nie są zastosowane odpowiednie środki ochrony.

## 4. Fizyczna kontrola dostępu

4.1. Należy wdrożyć procedury eksploatacyjne w celu ochrony danych osobowych oraz dokumentacji systemowej przed nieautoryzowanym lub nieuprawnionym ujawnieniem, modyfikacją, usunięciem i zniszczeniem.

4.2. Należy wdrożyć politykę czystego biurka i czystego ekranu w celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia danych osobowych.

4.3. Karty, hasła itd. służące do uzyskania dostępu do systemów informatycznych służących do przetwarzania danych osobowych należy zabezpieczać a sposób ich uzyskiwania należy szczegółowo zdefiniować w procedurach.

4.4. Dostęp do serwerowni lub innych pomieszczeń, w których znajdują się systemy informatyczne służące do przetwarzania danych osobowych lub zbiory nieinformatyczne należy rejestrować oraz okresowo przeglądać.

4.5. Dostęp dla gości do serwerowni lub innych pomieszczeń, w których znajdują się systemy informatyczne służące do przetwarzania danych osobowych należy nadzorować przez cały czas ich pobytu.

4.6. Przyznawanie dostępu gościom należy wykonywać wyłącznie w określonych i autoryzowanych celach.

4.7. Kończąc pracę, należy zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację, wydruki, elektroniczne nośniki informacji i umieścić je w zamykanych szafkach.

4.8. Monitory należy ustawić w taki sposób aby uniemożliwiać podgląd wyświetlanych danych osobowych przez osoby nieuprawnione.

11.4.9. W przypadku korzystania z usług zewnętrznych podmiotów oferujących zbieranie i niszczenie papierów, urządzeń lub nośników zawierających dane osobowe, należy wybrać wykonawcę z odpowiednimi zabezpieczeniami i doświadczeniem.

### **3.8 OCENA RYZYKA I PRZEGLĄDY**

---

#### **1. Ocena ryzyka**

1.1. Systemy informatyczne i aplikacje powinny być poddawane ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzania danych osobowych co najmniej raz na dwa lata. Ocena ryzyka powinna być również przeprowadzana przy dużych zmianach procesów biznesowych, systemów informatycznych i aplikacji.

1.2. Narzędzia informatyczne służące do oceny ryzyka bezpieczeństwa przetwarzania danych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

#### **2. Przeglądy bezpieczeństwa**

2.1. Przeglądy bezpieczeństwa przetwarzania danych osobowych powinny być przeprowadzane okresowo, co najmniej raz na 2 lata w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.

2.2. Przeglądy zgodności z zasadami bezpieczeństwa przetwarzania danych osobowych urządzeń informatycznych oraz sieci teleinformatycznych należy przeprowadzać okresowo, co najmniej raz na rok.

2.3. Narzędzia informatyczne służące do przeprowadzania przeglądów bezpieczeństwa przetwarzania danych osobowych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

### **3.9 ZARZĄDZANIE INCYDENTAMI**

---

#### **1. Monitorowanie incydentów**

1.1. Incydenty związane z bezpieczeństwem przetwarzania danych osobowych powinny być wykrywane, rejestrowane i monitorowane w celu ich zidentyfikowania i zapobiegania ich wystąpieniu w przyszłości.

1.2. Zdarzenia systemowe powinny być przechowywane jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.

1.3. Użytkownicy systemów powinni znać i przestrzegać zasad zgłaszania incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.

## 2. Zgłaszanie incydentów

2.1. Zaistniałe zdarzenia związane z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych takie jak np. utrata integralności, niedostępność, awarie, uszkodzenia, ostrzeżenia i alarmy bezpieczeństwa systemów informatycznych, urządzeń teleinformatycznych oraz danych powinny być niezwłocznie zgłaszane do Administratora Bezpieczeństwa Informacji.

### 3.10 ZBIORY DANYCH OSOBOWYCH

---

#### 1. Wykaz zbiorów danych osobowych

1.1. Dokumentacja zbiorów danych osobowych jest prowadzona przez Administratora Bezpieczeństwa Informacji i stanowi **załącznik nr 4** niniejszej Polityki.

1.2. Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń należących do obszaru przetwarzania danych osobowych.

#### 2. Opis struktury zbiorów danych osobowych

2.1. Wskazane w **załączniku nr 4** zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach.

2.2. Zawartość pól informacyjnych, występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają Administratora danych do przetwarzania danych osobowych.

#### 3. Sposób przepływu danych pomiędzy poszczególnymi systemami

3.1. Dokumentacja systemów informatycznych służących do przetwarzania danych osobowych powinna zawierać opis współpracy z innymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami z którymi współpracuje.

3.2. Administrator systemów informatycznych jest zobowiązany do poprowadzenia aktualnej dokumentacji opisującej sposób przepływu danych osobowych pomiędzy systemami.

## 4. POSTANOWIENIA KOŃCOWE

---

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
3. Pracownicy Roma Investments Piątkiewicz Sp.J. zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Roma Investments Piątkiewicz Sp j. , użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

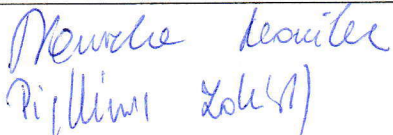
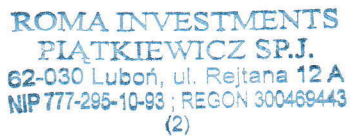
## 5 ZAŁĄCZNIKI

Załącznik nr 1 – Oświadczenie

Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 3 – Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Załącznik nr 4 – Wzór wykazu struktury zbiorów danych

| Dokument sporządzono:                                     | Pełen podpis Administratora                                                                           | Pieczęć                                                                                                                                                                                                        |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                           | Danych:                                                                                               |                                                                                                                                                                                                                |
| Data: 25/05/2018 (dd/mm/rrrr)<br>Miejsce: .....Lubon..... | <br>Piklini Lok(1) | <br>ROMA INVESTMENTS<br>PIATKIEWICZ SP.J.<br>62-030 Lubon, ul. Rejtana 12 A<br>NIP 777-295-10-93 ; REGON 300469443<br>(2) |

.....  
(data)

## OŚWIADCZENIE

Oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), aktów wykonawczych wydanych na jej podstawie oraz dokumentów w związku z przetwarzaniem danych osobowych, w szczególności:

- Polityki bezpieczeństwa przetwarzania danych osobowych;
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zobowiązuję się do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia do których uzyskam dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

Jednocześnie przyjmuje do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

.....  
Imię i nazwisko pracownika

.....  
Pracodawca

Potwierdzam odbiór 1 egz. oświadczenia.

..... Czytelny podpis pracownika

## UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.), **upoważniam:**

|                                          |  |
|------------------------------------------|--|
| Imię i nazwisko upoważnionego pracownika |  |
|------------------------------------------|--|

Osoba upoważniona obowiązana jest przetwarzać dane osobowe w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Roma Investments Piątkiewicz Sp.J wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

\_\_\_\_\_  
Data i podpis upoważniającego

\_\_\_\_\_  
Data i podpis osoby upoważnionej

### Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Roma Investments Piątkiewicz Sp.J (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

\_\_\_\_\_  
Data i podpis osoby upoważnionej

Załącznik nr 3 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe.

---

1. Roma Investments Piątkiewicz Sp.J ul. Rejtana 12A, 62-030 Luboń
  2. Platinum Palace Hotel ul. Powstaków Śląskich 204, Wrocław
  3. Platinum Palace Residence ul.Rejmonta 19, Poznań
-

Załącznik nr 4 – Wzór wykazu struktury zbiorów danych

| Nr | Stanowisko | Imię i nazwisko | Zakres przetwarzanych danych | Uwagi |
|----|------------|-----------------|------------------------------|-------|
| 1. |            |                 |                              |       |
| 2. |            |                 |                              |       |
| 2. |            |                 |                              |       |
| 3. |            |                 |                              |       |
| 4. |            |                 |                              |       |
| 5. |            |                 |                              |       |
| 6. |            |                 |                              |       |
| 7. |            |                 |                              |       |
| 8. |            |                 |                              |       |
| 9. |            |                 |                              |       |