

**POLITYKA BEZPIECZEŃSTWA  
PRZETWARZANIA DANYCH OSOBOWYCH  
W **Union Jack Sp.z.o.o****

## Spis treści

1. CEL POLITYKI .....	3
2. ŹRÓDŁA WYMAGAŃ .....	3
3. DOKUMENTY POWIĄZANE .....	3
4. ZAKRES STOSOWANIA .....	3
5. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH .....	3
6. POZIOM BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH .....	4
7. DEFINICJE .....	4
8. ODPOWIEDZIALNOŚĆ .....	5
8.1. Kierownictwo .....	5
8.2. Inspektor Danych Osobowych i .....	5
8.3. Osoby upoważnione do przetwarzania danych .....	6
9. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH .....	6
10. ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI .....	8
11. BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA .....	9
12. OCENA RYZYKA I PRZEGLĄDY .....	11
13. ZARZĄDZANIE INCYDENTAMI .....	12
14. ZBIORY DANYCH OSOBOWYCH .....	12
15. POSTANOWIENIA KOŃCOWE .....	13
<b>Załącznik nr 1 .....</b>	<b>14</b>
<b>Załącznik nr 2 .....</b>	<b>15</b>
<b>Załącznik nr 3 .....</b>	<b>16</b>
<b>Załącznik nr 4 .....</b>	<b>17</b>
<b>Załącznik nr 5 .....</b>	<b>18</b>

## 1. CEL POLITYKI

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w Union Jack Sp.z.o.o przez pracowników i współpracowników, którzy przetwarzają dane osobowe.

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Union Jack Sp.z.o.o rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniami przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

## 2. ŹRÓDŁA WYMAGAŃ

Polityka bezpieczeństwa przetwarzania danych osobowych w Union Jack Sp.z.o.o, 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.)

Wytycznymi w zakresie opracowania i wdrożenia polityki bezpieczeństwa - Generalny Inspektor Ochrony Danych Osobowych

## 3. DOKUMENTY POWIĄZANE

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Union Jack Sp.z.o.o.

## 4. ZAKRES STOSOWANIA

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.

W zakresie podmiotowym, Polityka obowiązuje wszystkich pracowników Union Jack Sp.z.o.o oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło.

## 5. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

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.

## 6. 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.

## 7. DEFINICJE

7.1.1. Administrator danych – Union Jack Sp.z.o.o, podmiot, który decyduje o środkach i celach przetwarzania danych osobowych, zwany dalej Union Jack Sp.z.o.o.

7.1.2. Inspektora Danych Osobowych – osoba wyznaczona przez Kierownictwo, odpowiedzialna 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.

7.1.3. 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.

7.1.4. Kierownictwo – Zarząd, organ zarządzający i reprezentujący Inspektor Danych Osobowych.

7.1.5. Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Inspektora Danych Osobowych lub przez osobę wyznaczoną, uprawniona do przetwarzania danych osobowych.

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

7.1.7. 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).

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

7.1.9. 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.

7.1.10. 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.

## 8. ODPOWIEDZIALNOŚĆ

### 8.1. 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 Inspektora Danych Osobowych.

wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;

egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych;

poddawanie przeglądów 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.

### 8.2. Inspektor Danych Osobowych

Do obowiązków Inspektora Danych Osobowych, 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.

### 8.3. 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 Inspektora Danych Osobowych.

## 9. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

### 9.1. Podstawowe zasady

9.1.1. 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.

9.1.2. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

9.1.3. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

9.1.4. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

### 9.2. Procedury postępowania z danymi osobowymi

9.2.1. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.

9.2.2. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.

9.2.3. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

### 9.3. Upoważnienie do przetwarzania danych osobowych

9.3.1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy.

9.3.2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Inspektora Danych Osobowych.

9.3.3. W celu upoważnienia do przetwarzania danych osobowych należy dostarczyć do Inspektora Danych Osobowych podpisane oświadczenie, którego wzór stanowi załącznik nr 1 niniejszej Polityki.

9.3.4. Na podstawie otrzymanego oświadczenia Inspektor Danych Osobowych upoważnia formalnie wnioskującego do przetwarzania danych osobowych i wydaje upoważnienie sporządzone wg wzoru stanowiącego załącznik nr 2 niniejszej Polityki.

9.3.5. 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.

### 9.4. Ewidencja osób upoważnionych

9.4.1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Inspektora Danych Osobowych 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.

9.4.2. Przełożeni osób upoważnionych odpowiadają za natychmiastowe zgłoszenie do Inspektora Danych Osobowych osób, które utraciły uprawnienia dostępu do danych osobowych.

### 9.5. Zachowanie danych osobowych w tajemnicy

9.5.1. 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.

### 9.6. Znajomości regulacji wewnętrznych

9.6.1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w Union Jack Sp.z.o.o, w szczególności Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

## 9.7. Zgodność

9.7.1. Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Union Jack Sp.z.o.o, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

9.7.2. Okresowy przegląd Polityki powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Union Jack Sp.z.o.o oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

9.7.3. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w Union Jack Sp.z.o.o.

## 10. ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI

### 10.1. Bezpieczeństwo usług zewnętrznych

10.1.1. Należy zapewnić aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w Union Jack Sp.z.o.o, wymaganiami umowy oraz wymaganiami prawa.

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

10.1.3. Należy zapewnić aby użytkownicy nie będący pracownikami Union Jack Sp.z.o.o stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

### 10.2. Powierzenie przetwarzania danych osobowych

10.2.1. 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.

10.2.2. 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.

10.2.3. 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.

10.2.4. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Union Jack Sp.z.o.o za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w



umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia Union Jack Sp.z.o.o do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

### 10.3. Udostępnianie danych osobowych

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

10.3.2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Inspektora Danych Osobowych .

10.3.3. 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.

10.3.4. 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.

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

### 10.4. 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

## 11. BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

### 11.1. Obszar przetwarzania

11.1.1. Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Union Jack Sp.z.o.o 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.

11.1.2. 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.

11.1.3. 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 wynosić ww. kluczy po zakończeniu pracy poza miejsca przeznaczone do ich przechowywania.

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

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

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

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

## 11.2. Bezpieczeństwo środowiskowe

11.2.1. 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.

11.2.2. 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.

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

## 11.3. Bezpieczeństwo urządzeń

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

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

## 11.4. Fizyczna kontrola dostępu

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

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

11.4.3. Klucze dostępowe, 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.

11.4.4. 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.

11.4.5. 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.

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

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

11.4.8. Monitory należy ustawić w taki sposób aby uniemożliwić 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.

## 12. OCENA RYZYKA I PRZEGLĄDY

### 12.1. Ocena ryzyka

12.1.1. 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.

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

### 12.2. Przeglądy bezpieczeństwa

12.2.1. 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.

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

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

## 13. ZARZĄDZANIE INCYDENTAMI

### 13.1. Monitorowanie incydentów

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

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

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

### 13.2. Zgłaszanie incydentów

13.2.1. 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 Inspektora Danych Osobowych.

## 14. ZBIORY DANYCH OSOBOWYCH

### 14.1. Wykaz zbiorów danych osobowych

14.1.1. Dokumentacja zbiorów danych osobowych jest prowadzona przez Inspektora Danych Osobowych i stanowi załącznik nr 4 niniejszej Polityki.

14.1.2. 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.

### 14.2 Opis struktury zbiorów osobowych

14.2.1. Dokumentacja zbiorów danych osobowych jest prowadzona przez Inspektora Danych Osobowych i stanowi załącznik nr 4 niniejszej Polityki.

14.2.2. 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.

14.2.3. Zawartość pól informacyjnych, występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają Inspektora Danych Osobowych do przetwarzania danych osobowych.

14.3. Sposób przepływu danych pomiędzy poszczególnymi systemami

14.3.1. 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.

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

14.4. Określenie środków technicznych i organizacyjnych

14.4.1. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych znajduje się w załączniku numer 5 niniejszej Polityki.

## 15. POSTANOWIENIA KOŃCOWE

15.1.1. 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.

15.1.2. 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.

15.1.3. Pracownicy Union Jack Sp.z.o.o 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 Union Jack Sp.z.o.o, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

## Załącznik nr 1

### Oświadczenie

.....  
(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 niepożądanym 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

## Załącznik nr 2

### Upoważnienie

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

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j.Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

– udziela się Panu/Pani<sup>1</sup>:

.....  
(imię i nazwisko)

.....  
(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych w rozumieniu Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (t.j.Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

Jest Pan/Pani\* upoważniony/upoważniona\* do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani\* zadań służbowych oraz poleceń przełożonego.

Upoważnienie traci ważność z chwilą ustania stosunku pracy.

.....  
(data i podpis osoby upoważniającej)

---

<sup>1</sup> niepotrzebne skreślić

### Załącznik nr 3

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe.

NAZWA FIRMY

Ulica, numer

Kod pocztowy, Miejscowość



## Załącznik nr 4

Wykaz zbiorów danych osobowych oraz opis struktury zbiorów:

Zbiór .....

Zbiór .....

Zbiór .....

Wykaz powierzonych zbiorów danych osobowych:

Zbiór .....

## Załącznik nr 5

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Dane osobowe są chronione przy zastosowaniu następujących zabezpieczeń niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych:

1. Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:

- 1) budynek i wszystkie pomieszczenia, w których zlokalizowano przetwarzanie danych osobowych zabezpieczone są przed dostępem osób nieuprawnionych;
- 2) dokumentacja papierowa po godzinach pracy jest przechowywana w zamkniętych biurkach lub szafach;
- 3) przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą wyznaczonej osoby.

2. Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:

- 1) dla zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych stosuje się w nich sprzęt oraz oprogramowanie wyprodukowane przez renomowanych producentów oraz zabezpiecza się sprzęt przed awarią zasilania lub zakłóceniami w sieci zasilającej;
- 2) zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii zapasowych;
- 3) kopie zapasowe są usuwane niezwłocznie po ustaniu ich użyteczności.

3. Przedsięwzięcia w zakresie ochrony transmisji danych:

- 1) w celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosuje się zabezpieczenia chroniące przed nieuprawnionym dostępem;
- 2) transmisja danych osobowych przez publiczną sieć telekomunikacyjną jest zabezpieczona środkami kryptograficznej ochrony danych;

4. Przedsięwzięcia w zakresie środków ochrony w ramach oprogramowania systemów:

- 1) w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło;
- 2) w przypadku, gdy do uwierzytelnienia użytkowników używa się identyfikatora i hasła, składa się ono z co najmniej 8 znaków, i jest skonstruowane w sposób nie trywialny, w szczególności zawiera małe i duże litery, cyfry oraz znaki specjalne;
- 3) hasła służące do uwierzytelniania w systemach informatycznych służących do przetwarzania danych osobowych są zmieniane co najmniej raz na 30 dni;
- 4) system informatyczny powinien wymuszać zmianę haseł, informując po upływie ich ważności;
- 5) w przypadku gdy system informatyczny służący do przetwarzania danych osobowych nie wymusza zmiany haseł, użytkownik jest zobowiązany do samodzielnej zmiany hasła po upływie 30 dni.

5. Przedsięwzięcia w zakresie środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

- 1) w celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych;

2) system zapewnia automatyczne odnotowywanie w systemie informacji o identyfikatorze użytkownika, który wprowadził dane osobowe oraz dacie pierwszego wprowadzenia danych do systemu;

3) system zapewnia przygotowania i wydruk raportu, który zawiera informacje, o których mowa w § 7 Rozporządzenia;

4) stosuje się oprogramowanie umożliwiające trwałe usunięcie danych osobowych z urządzeń, dysków lub innych elektronicznych nośników informacji, które przeznaczone są do naprawy, przekazania lub likwidacji przez osobę nieuprawnioną;

#### 6. Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:

1) w celu ochrony danych osobowych przetwarzanych na stacjach roboczych na czas krótkotrwałego opuszczenia stanowiska pracy przez użytkownika systemu, stosuje się mechanizm blokady stacji roboczej zabezpieczony hasłem;

2) stosuje się mechanizmy kontroli dostępu użytkowników do systemów – ogranicza się dostępu do katalogów, ogranicza się wykonywanie poleceń;

3) na stacjach roboczych użytkownicy nie posiadają uprawnień do instalowania nieautoryzowanego oprogramowania;

4) stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

5) kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.

#### 7. Przedsięwzięcia w zakresie środków organizacyjnych.

1) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;

2) dostęp do danych osobowych możliwy jest po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych wydane przez upoważnione osoby;

3) wprowadzono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

4) monitoruje się wdrożone zabezpieczenia systemu informatycznego.