POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH FIRMY

INTERLAND HANNA CZERNIAWSKA-SNOPEK

Zatwierdziła:	Hanna Czerniawska-Snopek		25.05.2018
	IMIĘ I NAZWISKO	**PODPIS**	**DATA**

1. TERMINOLOGIA

1.1. **Aktywa** – wszystko, co ma wartość dla organizacji (zasoby ludzkie, finansowe, informacyjne, organizacyjne, technologiczne i fizyczne);

1.2. **InterLand** - InterLand Hanna Czerniawska-Snopek

1.3. **ADO** - Administrator Danych Osobowych - InterLand Hanna Czerniawska-Snopek reprezentowana przez p. Hannę Czerniawską-Snopek.

Pojęcie administratora oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

1.4. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Katalog informacji stanowiących dane osobowe nie jest zamknięty. Przy rozstrzyganiu czy określone dane stanowią dane osobowe, w większości przypadków nieuniknione jest dokonanie zindywidualizowanej oceny przy uwzględnieniu konkretnych okoliczności.

1.5. **Dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia

1.6. **Dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne

1.7. **Naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

1.8. **Odbiorca** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

1.9. **PUODO** – Prezes Urzędu Ochrony Danych Osobowych.

1.10. **Polityka** - Polityka Bezpieczeństwa Danych Osobowych

1.11. **Przetwarzanie danych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie

1.12. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

1.13. **RODO** – Ogólne Rozporządzenie o Ochronie Danych Osobowych – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016

1.14. **System Informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

1.15. **Udostępnianie Danych** - stworzenie możliwości dostępu do danych osobowych innemu podmiotowi lub osobie.

1.16. **Usuwanie danych** - zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby.

1.17. **Zabezpieczenie danych osobowych** - środki techniczne i organizacyjne zapewniające ochronę danych osobowych.

1.18. **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

1.19. **Zgoda osoby, której dane dotyczą** - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

2. POLITYKA

2.1. Bezpieczeństwo danych osobowych jest nieodzownym elementem budowania zaufania i wiarygodności. Stanowi jedną z wartości, której utrata może mieć negatywne konsekwencje na relacje z klientami i innymi zainteresowanymi stronami.

2.2. Bezpieczeństwo danych osobowych jest procesem ciągłym obejmującym swym zasięgiem m.in. obszary informatyki, organizacji wewnętrznej, polityk i procedur, ochrony fizycznej, zgodności z prawem i obowiązującymi regulacjami, ciągłości działania. Jego istotą jest zrozumienie wymagań, szacowanie ryzyka, ustanowienie zasad przetwarzania danych osobowych, wdrożenie zabezpieczeń, monitorowanie ich skuteczności i ciągłe doskonalenie w oparciu o fakty.

2.3. Szacowanie ryzyka odbywa się przynajmniej raz na pół roku lub w przypadku istotnych zmian w firmie InterLand. Zmiany te mogą mieć różny charakter, np. organizacyjny, technologiczny, procesowy, prawny. Istotne zmiany mogą również dotyczyć kontekstu zewnętrznego firmy. Do udokumentowania oceny ryzyka wykorzystywane jest dedykowane narzędzie CNIL.

2.4. Naszym celem jest zapewnienie bezpieczeństwa informacji przy zachowaniu akceptowalnego poziomu ryzyka i efektywności procesów wewnętrznych.

2.5. Zasady postępowania określone w **Polityce** dotyczą wszystkich pracowników, współpracowników i zleceniobiorców firmy **InterLand**.

2.6. Właścicielka firmy będącą jednocześnie Administratorem Danych Osobowych (**ADO**) deklaruje pracę nad stałym doskonaleniem niżej przedstawionej **Polityki** i dokładanie wszelkich starań służących osiągnięciu celu w postaci zapewnienia bezpieczeństwa i zgodności przetwarzania danych osobowych z obowiązującymi wymaganiami prawnymi.

2.7. Dla osiągnięcia zamierzonego celu będą prowadzone sukcesywnie szkolenia obejmujące zagadnienia dotyczące zabezpieczenia przetwarzanych w systemach informatycznych i tradycyjnych („papierowych”) danych osobowych.

2.8. Przetwarzanie danych osobowych następuje przy poszanowaniu zasad wypływających w szczególności z następujących źródeł:

a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

b) Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r

c) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych

3. ZASADY OGÓLNE

3.1. Zasady przetwarzania danych osobowych

Podstawowe zasady, którymi **InterLand** oraz wszyscy jego pracownicy, współpracownicy i zleceniobiorcy kierują się podczas przetwarzania danych osobowych obejmują w szczególności:

- zasadę legalności, rzetelności i przejrzystości

  Przesłanką legalności przetwarzania przez **InterLand** danych osobowych zawartych w zbiorze **„Pośrednictwo pracy”** oraz **„Zatrudnienie”** jest art. 6, pkt. 1, podpunkt b **RODO**: „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy”
  Dodatkową przesłanką legalności przetwarzania przez **InterLand** danych osobowych w w/w zbiorach są zgody osób, których dane dotyczą (art. 6, pkt.1, podpunkt a), których wzór stanowi załącznik nr 1 i 1a do niniejszej Polityki.

- zasadę celowości i ograniczenia celu

  Jedynym celem przetwarzania danych osobowych w zbiorze **„Pośrednictwo pracy”** oraz **„Pracownicy”** przez **InterLand** jest odpowiednio:
  - zawieranie umów pośrednictwa pracy zgodnie z ustawą o promocji zatrudnienia i instytucjach rynku pracy (t.j. Dz. U. 2018 poz 1265) , oraz
  - zawieranie umów o pracę zgodnie z Kodeksem Pracy (t.j. Dz.U. 2018 poz 917)

- zasadę adekwatności i minimalizacji danych

  Zakres przetwarzanych danych osobowych nie wykracza poza te niezbędne do realizacji celu przetwarzania:

  W bazie **„Pośrednictwo pracy”** zakres przetwarzanych danych obejmuje:
  - dane kontaktowe (np. imię, nazwisko, adres, tlf, email)
  - dane kontaktowe rodziny (np. imię, nazwisko, adres, tlf)
  - dane pochodzące z dokumentów tożsamości (np. paszportów, książeczek żeglarskich, wiz)
  - dane związane z kwalifikacjami kandydata do pracy (np. dyplomy, certyfikaty, zaświadczenia, uprawnienia, wykształcenie, historia zatrudnienia)
  - inne dane osobowe (np. daty urodzenia, zdjęcia, świadectwa zdrowia, waga, wzrost, płeć, narodowość, dane kont bankowych, dane o szczepieniach, dane finansowe)

  W bazie **„Pracownicy”** zakres przetwarzanych danych obejmuje dane wyszczególnione w Kodeksie Pracy (t.j. Dz.U. 2018 poz 917) art 22.

- zasadę ograniczenia czasowego i ograniczenia przechowywania

  W bazie **„Pracownicy”** dane osobowe są przechowywane zgodnie z wymaganiami dotyczącymi przechowywania dokumentacji związanej z historią zatrudnienia.

  W bazie **„Pośrednictwo pracy”** dane osobowe są przechowywane tak długo, aż zgoda na ich przetwarzanie nie zostanie odwołana. Po odwołaniu zgody, przez okres czasu odpowiadający okresowi przedawnienia roszczeń, jakie może podnosić administrator danych i jakie mogą być podnoszone wobec administratora danych.
  Cykl życia danych osobowych rozpoczyna się od momentu ich zebrania poprzez analizę, przechowywanie, udostępnianie uprawnionym odbiorcom, uaktualnianie i usuwanie po osiągnięciu celu przetwarzania lub w momencie wycofania zgody podmiotu danych.

Część danych osobowych jest archiwizowana do celów udokumentowania historii pracy i działalności agencji przed urzędami administracji państwowej (np.: umowy agencyjne, kontrakty, umowy o pracę).

- zasadę merytorycznej poprawności, prawidłowości

  Dane są uaktualniane w zależności od potrzeb zatrudnienia (np. przed wyjazdem na kontrakt lub na podstawie informacji od podmiotu danych).
  Zidentyfikowane dane, które nie są aktualne są usuwane.

- zasadę poufności, integralności i dostepności

  Dane są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

4. PRZETWARZANIE DANYCH OSOBOWYCH

4.1. Obszar przetwarzania danych osobowych

Wykaz budynków, pomieszczeń i części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe przedstawiono w załączniku nr 2 do niniejszej Polityki.
Dostęp do pomieszczeń w godzinach pracy mają pracownicy tam zatrudnieni. Osoby postronne (np. interesanci) mogą przebywać w pomieszczeniach, w których przetwarzane są dane osobowe wyłącznie w obecności osób uprawnionych. Po godzinach pracy dostęp do pomieszczeń jest możliwy wyłącznie za zgodą **ADO**.

4.2. Wykaz zbiorów

Wykaz zbiorów danych osobowych oraz programów zastosowanych do przetwarzania tych danych stanowi załącznik nr 2 do niniejszej Polityki.

4.3. Zabezpieczenie danych osobowych

1. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, obejmują:
   a. zabezpieczenia fizyczne,
   b. zabezpieczenia proceduralne,
   c. zabezpieczenia techniczne,
2. Zabezpieczenia fizyczne obejmują:
   a. przetwarzanie danych osobowych w pomieszczeniu o ograniczonym i kontrolowanym dostępie,
   b. ustalenie zasad zarządzania kluczami do pomieszczeń i szaf,
   c. wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, w odpowiednio zabezpieczenia mebli (zamknięcia) i niezbędne zabezpieczenia alarmowe
   d. pomieszczenie zajmowane przez **InterLand** znajduje się w budynku z ochroną całodobową.

3. Zabezpieczenia proceduralne obejmują:
    a. dopuszczanie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienia nadane przez **ADO**,
    b. zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemu informatycznego służącego do ich przetwarzania,
    c. odebranie stosownych zobowiązań i oświadczeń; tj. zobowiązania do zachowania tajemnicy danych osobowych i sposobów ich zabezpieczenia oraz oświadczenia o zapoznaniu z treścią przepisów określających zasady postepowania przy przetwarzaniu danych osobowych, a także z dokumentacją przetwarzania i ochrony danych osobowych.
4. Zabezpieczenia techniczne obejmują:
    a. mechanizmy kontroli dostępu do systemów i zasobów,
    b. zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (programy antywirusowe, FW, automatyczna aktualizacja systemu operacyjnego),
    c. regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych,
    d. zastosowanie ochrony zasilania.

4.4. Powierzenie przetwarzania Danych Osobowych

a. Co do zasady **InterLand** nie powierza innym podmiotom przetwarzania danych osobowych.

4.5. Udostępnianie Danych Osobowych

a. Dane Osobowe udostępniane są pracodawcom krajowym i zagranicznym z obszaru EOG oraz Szwajcarii, w tym armatorom na podstawie umów zawartych między ADO a danym pracodawcą.
b. W przypadku pracodawców zagranicznych niemających siedziby na terenie Unii Europejskiej podpisywane są standardowe klauzule umowne zatwierdzone przez Komisję Europejską (załączniki nr 5).
c. W przypadku pracodawców krajowych i zagranicznych mających siedzibę w UE podpisywane są klauzule umowne o zachowaniu poufności oraz określane są bezpieczne warunki przekazywania danych osobowych.

4.6. Nadawanie i odbieranie upoważnienia do przetwarzania danych osobowych

a. Upoważnienia do przetwarzania danych osobowych nadaje ADO, po wcześniejszym przeszkoleniu i podpisaniu oświadczenia pracownika o zapoznaniu się z przepisami – wzór oświadczenia i upoważnienia stanowi załączniki nr 3 do niniejszej Polityki.
b. Upoważnienia są dołączane do teczki personalnej pracownika.
c. Utworzenie konta w systemie informatycznym i nadawanie uprawnień realizowane jest zgodnie z „Zasadami bezpieczeństwa informacji dla użytkowników”.
d. ADO odbiera upoważnienie do przetwarzania danych osobowych w następujących przypadkach:
    a. rozwiązania z pracownikiem umowy o pracę,
    b. zmiany zakresu obowiązków pracownika,
e. Odbiór praw dostępu i wyrejestrowanie z Systemu realizowane jest zgodnie z „Instrukcją Zarządzania Systemem IT”.

5. OBOWIĄZKI I ODPOWIEDZIALNOŚĆ PRACOWNIKÓW

5. Pracownicy **InterLand**, przeszkoleni i upoważnieni przez **ADO** do przetwarzania danych osobowych odpowiadają za:
    a. zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych,
    b. zapoznanie się z Polityką Bezpieczeństwa Danych Osobowych i jej stosowanie.
    c. podpisanie oświadczenia o zapoznaniu się z tymi przepisami, a także o zachowaniu w tajemnicy powierzonych im do przetwarzania danych i sposobach ich zabezpieczenia;
    d. przetwarzanie danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach,
    e. zabezpieczanie stanowiska pracy przed dostępem osób nieupoważnionych,
    f. bezzwłoczne zawiadomienie bezpośredniego przełożonego o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych oraz powstrzymania się od wszelkich działań mogących spowodować zatarcie śladów bądź dowodów naruszenia
    g. zachowanie szczególnej ostrożności w przypadku korzystania z komputera przenośnego na którym znajdują się dane osobowe, a w szczególności:
        • zabezpieczenie dostępu do komputera,
        • nieudostępnianie komputera osobom nieupoważnionym,
        • stosowanie środków ochrony kryptograficznej podczas użytkowania poza **InterLand**
    h. informowanie osób, których dane osobowe zamierzają przetwarzać (przyjęcie wniosku/umowy) o celu zbierania danych osobowych, adresie siedziby **InterLand** oraz przysługujących uprawnieniach (klauzula informacyjna stanowi załącznik nr 1 i 1a do niniejszej Polityki) lub dokonanie odpowiednich zapisów w umowie

6. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

6.1 W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

6.2 Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (załącznik nr 4). Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

7. LISTA ZAŁĄCZNIKÓW

- Nr 1 – Klauzula informacyjna i zgoda na przetwarzanie danych osobowych
- Nr 1a – Klauzula informacyjna i zgoda na przetwarzanie danych osobowych (NoK)
- Nr 2 – a) wykaz budynków, pomieszczeń i części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
  b) wykaz zbiorów danych osobowych oraz programów zastosowanych do ich przetwarzania
  c) opis struktury zbioru danych i przepływu danych osobowych
- Nr 3 – Upoważnienie do przetwarzania danych osobowych
- Nr 4 – Zgłoszenie i raport z incydentu/zdarzenia
- Nr 5 – Standardowe klauzule umowne zatwierdzone przez Komisję Europejską

8. HISTORIA ZMIAN DOKUMENTU

Wersja 1 z 01/06/2015 Utworzenie Polityki Bezpieczeństwa Danych Osobowych (POL_BI_ver 1)
Wersja 2 z 25/05/2018 Zmiany związane z wdrożeniem RODO (POL_BI_ver 2)