TRANZ-TEL SP. Z O.O.

Kobiór 43-210, ul. Centralna 37

NIP: 638-164-17-78

Tel.: +48 32 218 86 59, +48 32 218 86 39

Faks: +48 32 218 86 59 wew. 502

E-mail: biuro@tranztel.com.pl

Polityka Ochrony Danych Osobowych

Firmy Tranz-Tel Sp. Z o.o.

Obowiązuje od dnia 25.05.2018r.

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowanym przez firmę Tranz-Tel Sp. z o. o. w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

DEFINICJE:

- **Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
- **RODO** – rozporządzenie 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 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)
- **Dane osobowe** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.
- **Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
- **Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania
- **Anonimizacja**- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych
- **Zgoda osoby, której dane dotyczą** - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub

wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

- **Ocena skutków w ochronie danych -** to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.
- **Podmiotem danych** jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.
- **Odbiorca -** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
- **Podmiot przetwarzający** (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.
- **Inspektor Ochrony Danych (IOD) -** to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/ pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.
- **Pseudonimizacja -** oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- **Szczególne kategorie danych osobowych** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.
- **Profilowanie** – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy

tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

- **Naruszenie ochrony danych osobowych -** jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2 OCENA SKUTKÓW (ANALIZNA RYZYKA)

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Firma Tranz-Tel Sp. z o. o. nie jest zobowiązana do przeprowadzenia oceny skutków, mimo to zastosowała poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

Ocena skutków musi być wykonana ze współudziałem Inspektora Ochrony Danych Osobowych.

2.1 OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

W celu dokonania analizy ryzyka firma Tranz-Tel Sp. z o. o. zidentyfikowała dane osobowe, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku:

01a Wykaz zbiorów danych osobowych.

2.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) firma Tranz-Tel sp. z o. o. lub Podmiot przetwarzający dane osobowe zobowiązuje się do spełnienia wobec nich obowiązków prawnych:

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9)
2. dane te są adekwatne w stosunku do celów przetwarzania
3. dane te są przetwarzane przez określony czas (retencja danych)
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody)
5. opracowano klauzule informacyjne dla powyższych osób (patrz załącznik 01b Klauzule informacyjne).
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28) zgodnie z załącznikiem 01f Umowa powierzenia (wykaz podmiotów przetwarzających prowadzony jest w załączniku 01e Rejestr umów powierzenia.

7. potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w załączniku: 01a Wykaz zbiorów danych osobowych.

2.3 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów, dla procesu wysyłania informacji handlowej z bazy marketingowej banku)

2.3.1 DEFINICJE

- **Aktywa** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
- **Naruszenie (Incydent) ochrony danych osobowych** - to 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
- **Zagrożenie** - potencjalne naruszenie (potencjalny incydent)
- **Skutki** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
- **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

2.3.2 WYZNACZNIE ZAGROŻEŃ:

1. Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów
3. Wykaz przykładowych zagrożeń znajduje się w załączniku 02c Lista potencjalnych zagrożeń

2.3.3 WYLICZENIE RYZYKA DLA ZAGROŻEŃ:

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne

4. Proponowaną Skalę skutków prezentuje Tabela B
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.3.4 PORÓWNANIE WYLICZONYCH RYZYK ZE SKALĄ I OKREŚLENIE DALSZEGO POSTĘPOWANIA Z RYZUKIEM:

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

2.3.5 REAKCJA NA WARTOŚĆ RYZYKA

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:

a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
b. Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)
c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę)

3. Wykaz przykładowych zabezpieczeń do znajduje się w załączniku 02d Lista potencjalnych zabezpieczeń
4. Analizę ryzyka przeprowadza się w specjalnym szablonie (programie) 02e Arkusz analizy ryzyka RODO

2.3.6 PONOWNA ANALIZA RYZYKA

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

2.3.7 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

3 UPOWAŻNIENIA

3.1 Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych – patrz załącznik 03 Ewidencja osób upoważnionych.

3.2 Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

3.3 Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia nadawane są w formie udokumentowanego zakresu obowiązków.

3.4 Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia

4 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów

bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych)
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze –patrz załącznik 04 Formularz rejestracji incydentu
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie

później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik - 05 Regulamin Ochrony Danych Osobowych

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, patrz załącznik 03 ewidencja osób upoważnionych

6 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO
2. Za przeprowadzenie szkolenia odpowiada IOD
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą 06a Załącznik Plan szkolenia RODO
4. Materiały szkoleniowe dla uczestników szkolenia opracowano w formie załącznika 06b Szkolenie wewnętrzne RODO
5. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, patrz załącznik 03 Ewidencja osób upoważnionych

7 REJESTR CZYNNOŚCI PRZETWARZANIA

1. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, wypełnia załącznik 07a Rejestr czynności prowadzony przez Administratora
2. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Podmiot przetwarzający, wypełnia załącznik 07b Rejestr czynności prowadzony przez Podmiot przetwarzający

8 AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W tym celu Administrator stosuje procedurę audytów – patrz załącznik 08 Procedura audytu

9 PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO (BCP)

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w załączniku 09 Plan ciągłości działania

10 WYKAZ ZABEZPIECZEŃ

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz załącznik Instrukcja zarządzania systemami informatycznymi / Wykaz zabezpieczeń RODO
2. Wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne
3. Instrukcja / wykaz jest aktualizowana po każdej analizie ryzyka